CYTOMIC

Advanced EPDR Administration Guide_

Legal notice.

Registered trademarks.

Contact information.

Corporate Headquarters:

Cytomic (Business Unit of Panda Security)

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 Spain.

https://www.pandasecurity.com/uk/about/contact/

Version: 4.50.00

Author: Cytomic

Date: 4/1/2025

About the Advanced EPDR Administration Guide

To get the latest version of the documentation in PDF format, go to:

https://info.cytomicmodel.com/resources/guides/EPDR/latest/en/EPDR-guide-EN.pdf

For more information about a specific topic, see the product's online help, available at:

https://info.cytomicmodel.com/resources/help/EPDR/latest/en/index.htm

Release notes

To find out what's new in the latest version of Advanced EPDR, go to the following URL:

https://info.cytomicmodel.com/releasenotes/?product=EPDR&lang=en

Technical documentation not included in this Administration Guide for modules and services compatible with Advanced EPDR

To access the Cytomic Insights User's Guide, go to the following URL:

https://info.cytomicmodel.com/resources/guides/Insights/en/INSIGHTS-guide-EN.pdf

To access the Cytomic Data Watch User's Guide, go to the following URL:

https://info.cytomicmodel.com/resources/guides/DataWatch/en/DATAWATCH-guide-EN.pdf

To access the Cytomic SIEMConnect guides, go to the following URLs:

https://info.cytomicmodel.com/resources/guides/SIEMConnect/en/SIEMCONNECT- Manual-EN.pdf

https://info.cytomicmodel.com/resources/guides/SIEMConnect/en/SIEMCONNECT-EventDescriptionGuide-EN.pdf

Technical support

Cytomic provides global support services aimed at responding to specific questions regarding the operation of the company's products. The technical support team also generates documentation covering technical aspects of our products. This documentation is available in the eKnowledge Base portal.

To access specific information about the product, go to the following URL:

https://www.cytomic.ai/support/epdr/

To access the eKnowledge Base portal, go to the following URL:

https://www.cytomic.ai/support/

Advanced EPDR Administration Guide survey

Rate this Administration Guide and send us suggestions and requests for future versions of our documentation at:

https://es.surveymonkey.com/r/feedbackEPDRGuideEN

Table of contents

Chapter 1

Preface

This Administration Guide contains basic information and procedures for making the most out of your Advanced EPDR product.

Chapter contents

Who is this Administration Guide for?

This guide is intended for network administrators who are responsible for managing corporate IT security.

To correctly interpret the information provided by the product and draw conclusions that help to bolster corporate security, certain technical knowledge of the Windows environment is required with respect to processes, the file system, and the registry, as well as understanding the most commonly-used network protocols.

What is Advanced EPDR?

Advanced EPDR is a managed service that enables organizations to protect their IT assets, find out the extent of the security problems detected, and develop prevention and response plans against unknown and advanced persistent threats (APTs).

Advanced EPDR is divided into two clearly defined functional areas:

- Advanced EPDR
- Cytomic platform

Advanced EPDR

This is the product that implements the features aimed at ensuring the security of all workstations and servers in the organization, without the need for network administrators to intervene.

Cytomic platform

This is the ecosystem where the Cytomic products are run. Cytomic delivers all the information generated by Advanced EPDR about processes, the programs run by users, and the IT devices in the organization in real time and in an organized and highly detailed manner.

Cytomic is a scalable and efficient platform perfectly suited to address the needs of key accounts and MSPs.

Icons

The following icons are used in this Administration Guide:

Clarification or additional information, such as an alternative way of performing a certain task.

Suggestions and recommendations.

Additional information available in other sections of the Administration Guide.

Chapter 2

Advanced EPDR overview

Advanced EPDR is a comprehensive security solution for workstations and servers. Based on multiple technologies, it provides customers with a complete anti-malware security service without the need to install, manage, or maintain new hardware resources in the organization's infrastructure.

Chapter contents

Advanced EPDR benefits

Advanced EPDR is a solution based on multiple protection technologies that enables organizations to replace the traditional antivirus solution installed on their networks with a complete, managed security service.

Only legitimate software is allowed to run

Advanced EPDR monitors and classifies all processes run on the Windows computers on the network based on their behavior and characteristics. The service protects workstations and servers by allowing only programs classified as trusted to run.

Adapts to an organization environment

Unlike traditional antivirus solutions, Advanced EPDR leverages a new security approach that enables it to adapt precisely to each company particular environment. To achieve this, it monitors the execution of all applications, constantly learning from the actions triggered by the processes launched on workstations and servers.

After a brief learning period, Advanced EPDR is able to provide a far greater level of security than traditional antivirus solutions.

Assessment and remediation of security problems

The solution security offering is completed with monitoring, forensic analysis, and remediation tools that enable administrators to determine the scope of security incidents and resolve them.

Continuous monitoring provides valuable information about the context in which security problems take place. This information enables administrators to assess the impact of incidents and take the necessary measures to prevent them from occurring again.

Cross-platform service

Advanced EPDR is a cloud-based, cross-platform service compatible with Windows, macOS, Linux, and Android, as well as with persistent and non-persistent Virtual Desktop Infrastructure (VDI) environments.

Advanced EPDR does not require the installation of new management infrastructure, thereby reducing the total cost of ownership (TCO) to the lowest possible level.

Advanced EPDR features

Advanced EPDR provides guaranteed security for companies against advanced threats and targeted attacks. It is based on four strategic pillars:

- **Visibility**: It tracks every action taken by running applications.

Figure 2.1: The four pillars of Advanced EPDR advanced protection

- **Detection**: Constant monitoring of running processes and real-time blocking of zero-day and targeted attacks, as well as other advanced threats designed to bypass traditional antivirus solutions.
- **Remediation and response**: Forensic information for in-depth analysis of every attempted attack, as well as remediation tools.
- **Prevention**: Future attacks are prevented by editing the settings of the different protection modules and patching the vulnerabilities found on installed operating systems and applications.

Cytomic platform features

Cytomic is the new management, communication, and data processing platform developed by Cytomic and designed to centralize the services common to all of the company's products.

The Cytomic platform manages communications with the agents deployed across the network. Its management console presents the data gathered by Advanced EPDR in a structured and easy to understand way for later analysis by the network administrator.

The solution's modular design eliminates the need for organizations to install new agents or products on customers' computers for any new module that is purchased. All Cytomic products that run on the Cytomic platform share the same agent on customers' endpoints as well as the same web management console, facilitating product management and minimizing resource consumption.

Key benefits of Cytomic

The following are the main services that Cytomic provides for all Cytomic products compatible with the platform:

Cloud management platform

Cytomic is a platform hosted on the Cytomic cloud, with a series of significant benefits in terms of usage, functionality, and accessibility.

It does not require management servers to host the management console on the customer's premises: As it operates from the cloud, it can be accessed directly by all devices subscribed to the service, from anywhere and at any time, regardless of whether they are office-based or on-the-road.

Network administrators can access the management console at any moment and from anywhere, using any compatible Internet browser from a laptop, desktop, or even mobile devices such as tablets or smartphones.

It is a high-availability platform, operating 99.99% of the time. Network administrators do not need to design and deploy expensive systems with redundancy to host the management tools.

Real-time communication with the platform

The pushing out of settings profiles and scheduled tasks to and from network devices is performed in real time, the moment that administrators apply the new settings profiles to the selected devices. Administrators can adjust the security parameters almost immediately to resolve security breaches or to adapt the security service to the dynamic nature of corporate IT infrastructures.

Multi-product and cross-platform

The integration of Cytomic products in a single platform offers administrators a series of benefits:

- **Minimizes the learning curve**: All products share the same platform, thereby reducing the time that administrators require to learn how to use the new tool, which in turn reduces the TCO.
- **Single deployment for multiple products**: Only one software program is required on each device to deliver the functionality of all products compatible with Cytomic Platform. This minimizes the resource consumption on users' devices in comparison with separate products.
- **Greater synergy among products**: All products report through the same console. Administrators have a single dashboard from which they can see all the generated data, reducing the time and effort invested in maintaining several independent information repositories and in consolidating the information received from different sources.
- **Compatible with multiple platforms**: It is no longer necessary to invest in a range of products to cover the whole spectrum of devices used by a company. Cytomic Platform supports Windows, Linux, macOS, and Android, as well as persistent and non-persistent virtual and VDI environments.

Flexible, granular settings

The new configuration model speeds up the management of devices by reusing settings profiles, taking advantage of specific mechanisms such as inheritance and the assignment of settings profiles to individual devices. Network administrators can assign more detailed and specific settings profiles with less effort.

Complete, customized information

Cytomic Platform implements mechanisms that enable the configuration of the amount of data shown across a wide range of reports, depending on the needs of the administrator or the user of the information.

This information is completed with data about the network devices and installed hardware and software, as well as a log of changes, which helps administrators accurately determine the security status of the network.

Cytomic architecture

Cytomic architecture is designed to be scalable in order to provide a flexible, efficient service. Information is sent and received in real time to and from numerous sources and destinations simultaneously. These can be endpoints linked to the service, external data consumers such as SIEM systems or mail servers, or web instances for requests for settings changes and the presentation of information to network administrators.

Moreover, Cytomic implements a backend and a storage layer that implements a wide range of technologies that enable it to efficiently handle numerous types of data.

Figure 2.2: shows a high-level diagram of Cytomic Platform.

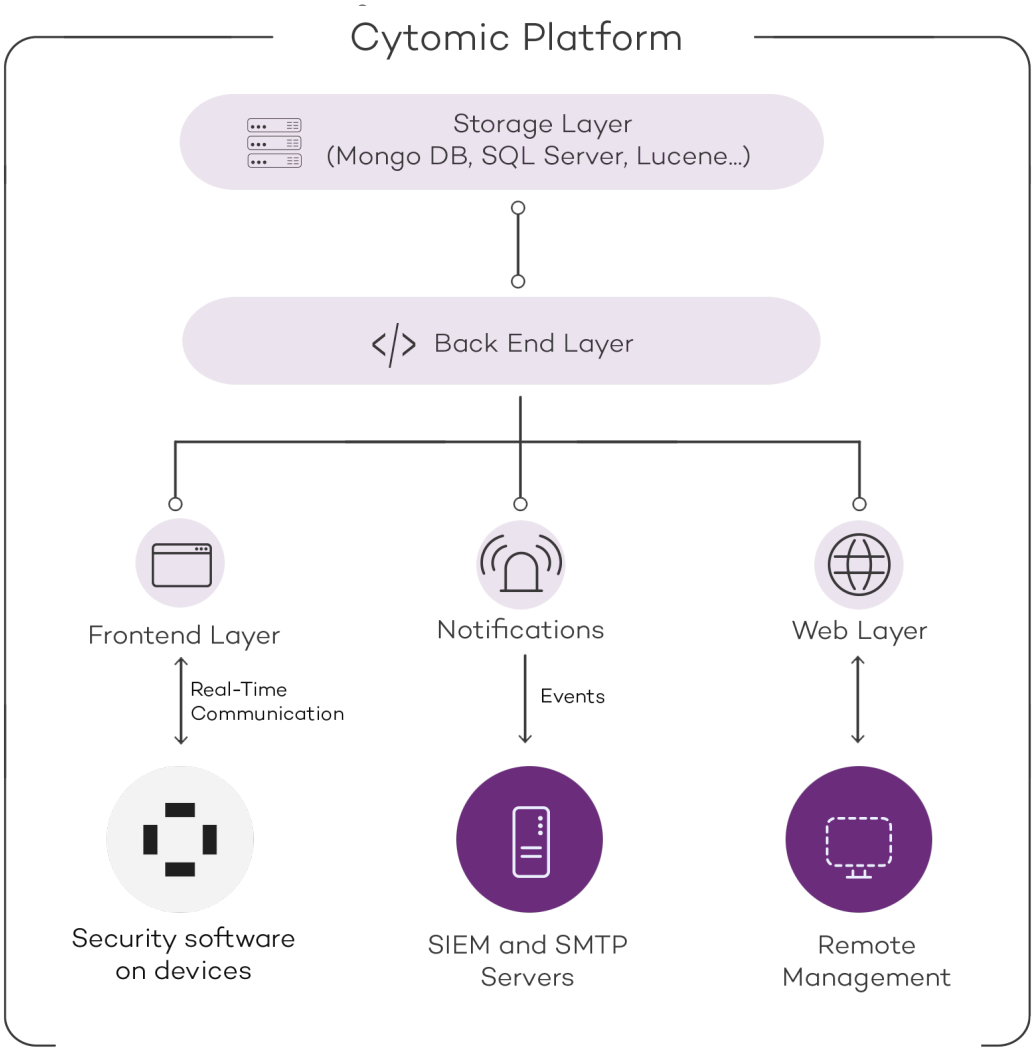


Figure 2.2: Logical structure of Cytomic

Cytomic on users' computers

Network computers protected by Advanced EPDR have a software program installed, consisting of two independent yet related modules which provide all the protection and management

functionality:

- **Cytomic communications agent module (Cytomic agent)**: This acts as a bridge between the protection module and the cloud, managing communications, events, and the security settings profiles implemented by the administrator from the management console.
- **Advanced EPDR protection module**: This is responsible for providing effective protection for users' computers. To do this, it uses the communications agent to receive the security settings profiles and sends statistics and detection information as well as details of the items scanned.

Cytomic real-time communications agent

The Cytomic agent handles communications between managed computers and the Advanced EPDR server. It also establishes a dialog among the computers that belong to the same network in the customer's infrastructure.

This module manages the security solution processes and gathers the configuration changes made by the administrator through the web console, applying them to the protection module.

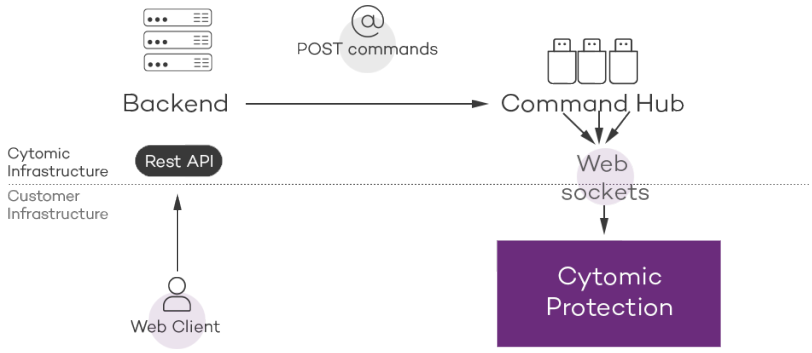


Figure 2.3: Flowchart of the commands entered through the management console

The communication between the devices and the Command Hub takes place through real-time persistent WebSocket connections. A connection is established for each computer for sending and receiving data. To prevent intermediate devices from closing the connections, a steady flow of keep-alive packets is generated.

The settings profiles configured by the network administrator through the Advanced EPDR management console are sent to the backend through a REST API. The backend, in turn, forwards them to the Command Hub, generating a POST command which pushes the information to all managed devices. This information is transmitted instantly provided the communication lines are not congested and every intermediate element is working correctly.

Key components

Advanced EPDR is a security service based on the analysis of the behavior of the processes run on the computers in each customer's IT infrastructure. This analysis is performed using machine learning techniques in Big Data environments hosted in the cloud.

Figure 2.4: shows the general structure of Advanced EPDR and its components:

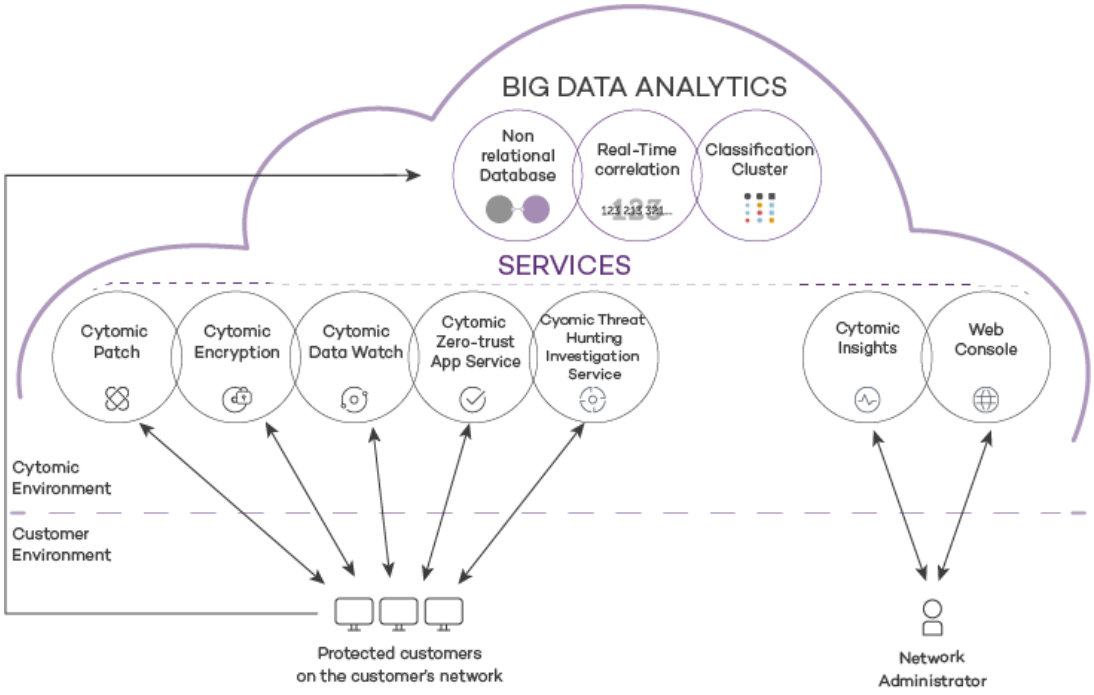


Figure 2.4: Advanced EPDR general structure

- **Big Data analytics infrastructure**: Made up of non-relational databases, services that correlate the events monitored in real time, and a classification cluster for the monitored processes.
- **Zero-Trust Application Service**: Classifies all processes run on Windows computers without ambiguity or false positives/negatives.
- **Threat Hunting Investigation Service (THIS)**: Cross-investigation service included in the product's basic license. It detects unknown threats and 'Living off the Land' attacks. These targeted attacks are designed to evade the protections installed on computers.
- **Cytomic SIEMConnect (optional)**: Integrates Advanced EPDR with third-party SIEM tools.
- **Cytomic Data Watch service (optional)**: A service for finding, listing, and monitoring the personal information stored in PII files.
- **Vulnerability assessment service**: Finds software with vulnerabilities and provides information about available patches.
- **Cytomic Insights service (optional)**: Reporting service for generating advanced security intelligence.
- **Cytomic Patch service (optional)**: A service for patching Windows operating systems and third-party applications.

- **Cytomic Encryption service (optional)**: Encrypts the internal storage devices of Windows computers to minimize data exposure in the event of loss or theft, as well as when storage devices are removed without having deleted their content.
- **Web console**: Management console server.
- Computers protected with the installed software (Advanced EPDR).
- The computer of the network administrator who accesses the web console.

Big Data analytics infrastructure

This is the cloud-based server cluster that receives the telemetry generated on the computers on the customer's network. This telemetry consists of the actions performed by the user programs monitored by the protection module, their static attributes, and execution context information. All this provides a constant flow of information which is scanned in the cloud using artificial intelligence techniques to evaluate the programs' behavior and issue a classification for each running process. This classification is returned to the protection module installed on each computer and is taken as the basis to perform the actions required to keep the computer protected.

The benefits provided by this cloud-based model in comparison to the methodology used by traditional antiviruses, which send samples to the antivirus vendor for manual analysis, include:

- Every process run on protected computers is monitored and analyzed: This eliminates the uncertainty that characterizes traditional antivirus solutions, which can recognize malware items but cannot identify any other application.
- The delay in classifying processes seen for the first time (the malware window of opportunity) is minimal, as Advanced EPDR sends the actions triggered by each process in real time to our servers. Our cloud servers are constantly working on the actions collected by our sensors, significantly reducing any delay in issuing a classification and the time that computers are exposed to threats.
- The continuous monitoring of every process enables Advanced EPDR to classify as malware items which initially behaved as goodware. This is typical of targeted attacks and other advanced threats designed to operate under the radar.
- Cloud-based scanning frees customers from having to install and maintain a dedicated hardware and software infrastructure, or stay up to date with license payments and manage warranties, notably reducing the TCO.

Web management console server

The web console is compatible with the most popular Internet browsers, and is accessible anytime, anywhere, from any device with a supported browser.

To check whether your Internet browser is compatible with the service, see ***Access to the web console*** *on page* ***953****.*

The web console is responsive, that is, it can be used on smartphones and tablets without any problems.

Computers protected with Advanced EPDR

Advanced EPDR requires the installation of a small software component on all computers on the network susceptible of having security problems. This component is made up of two modules: the Cytomic communications agent and the Advanced EPDR protection module.

Advanced EPDR can be installed without problems on computers with competitors' security products installed.

The Advanced EPDR protection module contains the technologies designed to protect customers' computers. Advanced EPDR provides, in a single product, everything necessary to detect targeted and next-generation malware (APTs), as well as productivity management and remediation tools to disinfect compromised computers and assess the impact of intrusion attempts.

Advanced EPDR services

Cytomic provides other services, some of which are optional, which enable customers to integrate the solution into their current IT infrastructures and benefit directly from the security intelligence generated at Cytomic labs.

Zero-Trust Application Service

This service, included in the product by default for Windows computers, is designed to allow only Cytomic certified programs to run. To do this, it uses a combination of local technologies on the user's computer and cloud-hosted technologies in a Big Data infrastructure. These technologies are capable of automatically classifying 99.98 percent of all running processes. The remaining percentage is manually classified by malware experts. This approach enables us to classify 100 percent of all binaries run on customers' computers without creating false positives or false negatives.

All executable files found on users' computers that are unknown to the platform are sent to the Big Data analytics infrastructure for analysis.

> *Unknown files are sent only once for all customers using Advanced EPDR, which reduces the impact on customers' networks virtually to zero. Additionally, bandwidth management mechanisms are implemented, as well as per-computer and per-hour bandwidth limits.*

Threat Hunting Investigation Service (THIS)

A service that detects living-off-the-land attacks and threats designed to bypass the protections installed on computers. This service leverages the Cytomic Orion product, the advanced threat hunting platform developed by Cytomic.

Thanks to the telemetry sent from computers, Cytomic Orion performs cross-analytics of the processes run in customers' IT infrastructures to detect new threats and create advanced hunting rules. When an indicator of attack is detected, it is validated by the Cytomic team of cybersecurity experts. After it is validated, Advanced EPDR shows the associated indicator of attack (IOA) in the console, along with a description of its characteristics and recommendations for the administrator to resolve the situation.

This service is included in all the Advanced EDR and Advanced EPDR licenses

> *For more information about how to configure the indicators of attack module, see "**Configuring indicators of attack (IOA)** on page **621**".*

MDR (Managed Detection and Response) service

A 24/7 cybersecurity service that enables partners to provide a managed detection and response service to customers with minimum investment in a SOC (Security Operations Center). The service monitors the security of computers in the organization, searching for threats, detecting attacks, investigating, and providing guided recommendations about how to restore affected assets and improve customer security.

The MDR service leverages innovative technologies that use artificial intelligence algorithms. Additionally, the service is fully managed by a team of cybersecurity experts, which improves customer security and cyber resilience overall and minimizes detection and response times.

> *For more information about the MDR service, see **MDR service settings** on page **657**.*

Cytomic Insights service (optional)

Advanced EPDR automatically and transparently sends all the information collected from user computers to Cytomic Insights, a knowledge storage and leverage system.

All actions triggered by the processes run across the IT network are sent to Cytomic Insights, where they are correlated and analyzed in order to extract security intelligence. This provides administrators with additional information on threats and the way users use corporate computers. This information is delivered in the most flexible and visual way to make it easier to understand.

The Cytomic Insights service is directly accessible from the Advanced EPDR web console dashboard.

See the Cytomic Insights User Guide (accessible from the product web page) for information about how to configure and take advantage of the knowledge analytics and advanced search service.

Cytomic SIEMConnect service (optional)

Advanced EPDR integrates seamlessly with the third-party SIEM solutions installed by customers on their IT infrastructures. The activities performed by the applications run on the network are delivered to the SIEM server, ready to use and enriched with the knowledge provided by Advanced EPDR.

The SIEM systems compatible with Advanced EPDR are:

- QRadar
- AlienVault
- ArcSight
- LookWise
- Bitacora

See the Cytomic SIEMConnect User Guide for a detailed description of the information collected by Advanced EPDR and sent to the customer SIEM system.

Cytomic Data Watch service (optional)

This is a security module integrated in the Advanced EPDR platform and designed to help organizations comply with the applicable data protection regulations that govern the storage and processing of personally identifiable information (PII).

Cytomic Data Watch discovers, audits, and monitors in real time the full lifecycle of the PII files stored on Windows computers: from data at rest to data in use (the operations taken on personal data) and data in motion (data exfiltration). With this information, Cytomic Data Watch generates an inventory showing the evolution of the number of files with personal data found on each computer on the network.

For more information about this service, see ***Cytomic Data Watch (Personal data monitoring)*** *on page* ***371****.*

Cytomic Patch service (optional)

This service reduces the attack surface of the Windows workstations and servers in the organization by updating the vulnerable software found (operating systems and third-party applications) with the patches released by the relevant vendors.

Additionally, it finds all programs on the network that have reached their EOL (End-Of-Life) stage. These programs pose a threat as they are no longer supported by the relevant vendor and are a primary target for hackers looking to exploit known unpatched vulnerabilities. Administrators can easily find all EOL programs in the organization and design a strategy for the controlled removal of this type of software.

Also, in the event of compatibility conflicts or malfunction of the patched applications, Cytomic Patch enables organizations to roll back/uninstall those patches that support this feature, or exclude them from installation tasks, preventing them from being installed.

Vulnerability Assessment service

This free service searches for software with vulnerabilities on computers. To prevent malware from exploiting security holes to damage and infect workstations and servers, it informs about the availability of patches that can mitigate those vulnerabilities.

To centrally install available patches, you must have a Cytomic Patch license.

Cytomic Encryption service (optional)

The ability to encrypt the information held in the internal storage devices of the computers on your network is key to protecting the stored data in the event of loss or theft or when the organization recycles storage devices without having deleted their contents completely. Advanced EPDR uses Windows BitLocker and macOS FileVault technologies to encrypt hard disk contents at sector level, centrally managing recovery keys in the event of loss or hardware configuration changes.

The Cytomic Encryption module enables you to use the Trusted Platform Module (TPM), if available, and provides multiple authentication options, adding flexibility to computer data protection.

Product user profile

Even though Advanced EPDR is a managed service that offers security without administrator intervention, it also provides clear and detailed information about the activity of the processes run by all users on the organization's network. This data can be used by administrators to clearly assess the impact of security problems and adapt the company's protocols to prevent similar situations in the future.

Supported devices and languages

For a detailed description of the platforms and requirements, see ***Product features and requirements*** *on page* ***932****.*

Supported operating systems

- Windows Workstation
- Windows Server
- Persistent and non-persistent VDI systems
- macOS
- Linux
- Android smartphones and tablets

Supported web browsers

The management console supports the latest versions of the following web browsers:

- Chrome
- Microsoft Edge
- Firefox
- Opera

Languages supported in the web console

- Spanish
- English
- Swedish
- French
- Italian
- German
- Portuguese
- Hungarian
- Russian
- Japanese
- Finnish (local console only)

Chapter 3

The management console

Advanced EPDR leverages the latest web development techniques to provide a cloud-based management console that enables organizations to interact with the security service simply and centrally. Its main characteristics are as follows:

- **It is adaptive**: Its responsive design allows the console to adapt to the size of the screen or web browser you are viewing it with.
- **It is user friendly**: The console uses Ajax technologies to avoid full page reloads.
- **It is flexible**: Its interface adapts easily to your needs, enabling you to save settings for future use.
- **It is homogeneous**: It follows well-defined usability patterns to minimize your learning curve.
- **It is interoperable**: The data shown can be exported to `CSV` format with extended fields for later consultation.

Chapter contents

Benefits of the web console

The web console is the main tool with which administrators manage security. Because it is a centralized web service, it brings together a series of features that benefit the way the IT department operates.

A single tool for complete security management

Through the web console, administrators can deploy the Advanced EPDR installation package to all computers on the network, configure their security settings, monitor the protection status of the network, and benefit from remediation tools as well as forensic analysis tools to resolve security incidents. All these features are provided from a single web-based console, facilitating the integration of the different tools and minimizing the complexity of using products from different vendors.

Centralized security management for remote offices and mobile users

The web console is hosted in the cloud so it is not necessary to configure VPNs or change router settings to access it from outside the company network. Neither is it necessary to invest in IT infrastructures such as servers, operating system licenses, or databases, nor to manage maintenance and warranties to ensure the operation of the service.

Security management from anywhere at anytime

The web console is responsive, adapting to any device used to manage security. This means administrators can manage protection anywhere and at any time, using a smartphone, a notebook, a desktop PC, etc.

Access to the web console and requirements

Requirements for accessing the web console

- Valid credentials (user account and password) and a second authentication factor (optional). See **Accessing, controlling, and monitoring the management console** on page **61**.
- Latest version of a supported web browser:

- Google Chrome
- Internet Explorer
- Firefox
- Opera

- Internet connection and communication through port 443 allowed.

Access to the web console

To access the Advanced EPDR web console, go to:

https://central.cytomic.ai

- Open your web browser and go to **https://central.cytomic.ai**
- Type the credentials for your user account.
- If your user account has access to multiple different customer accounts, the **Select an account** page opens. Choose the customer whose console you want to access.
- The **Security** dashboard of the Advanced EPDR console opens.

General structure of the web console

The web console has resources that ensure a straightforward and smooth management experience, both with respect to security management as well as remediation and forensic analysis tasks.

The aim is to deliver a simple yet flexible and powerful tool that enables administrators to begin to productively manage network security as soon as possible.

Following is a description of the items available in the console and how to use them.

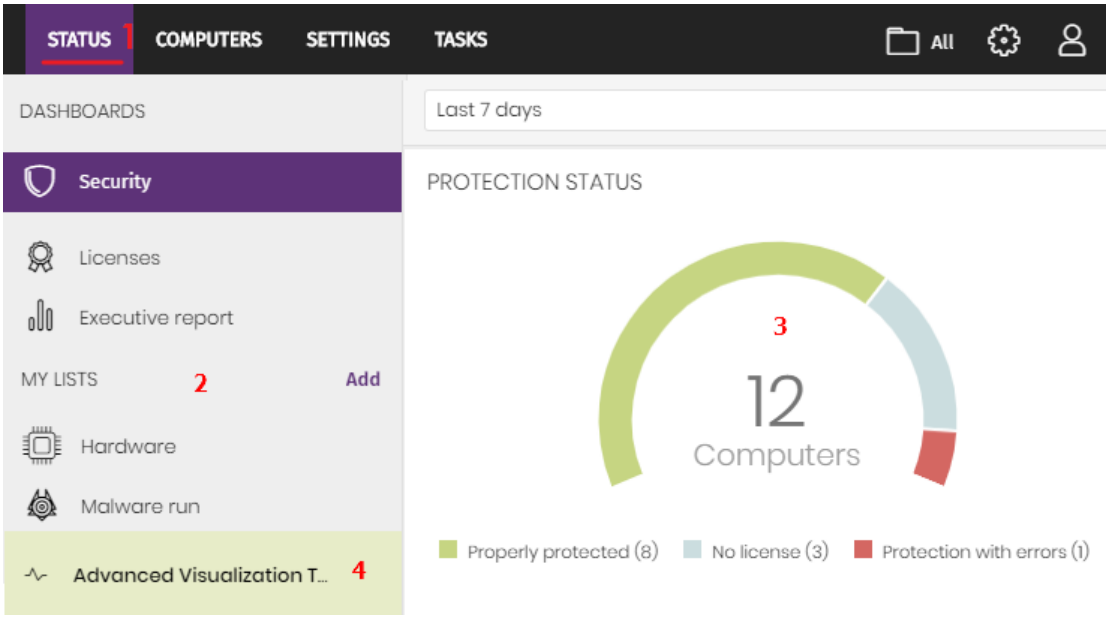


Figure 3.1: Advanced EPDR management console overview

Top menu (1)

The top menu enables you to access each of the main areas that the console is divided into:

- Cytomic Central button
- Status
- Computers
- Settings
- Tasks
- Filter by group
- Web notifications
- General options
- User account

Cytomic Central button

Click the ▦ button located in the left corner of the top menu. A page opens from which you can access and manage every security product you have contracted, as well as editing your Cytomic Account settings.

Status menu

Shows dashboards that provide administrators with an overview of the security status of the network through widgets and a number of lists accessible through the side menu. See **Status area overview**

for more information.

Computers menu

Provides the basic tools for network administrators to define the computer structure that best fits the security needs of their IT network. Choosing the right device structure is essential in order to assign security settings profiles quickly and easily. See **The Computers area** on page **212** for more information.

Settings menu

Define the behavior of Advanced EPDR on the workstations and servers where it is installed. Settings profiles can be assigned globally to all computers on the network or to some specific computers only through templates, depending on the type of settings profile to apply. Settings templates are very useful for computers with similar security requirements and help reduce the time needed to manage the security of the computers on your IT network.

*See **Managing settings** on page **287** for more information about how to create settings profiles in Advanced EPDR.*

Tasks menu

Schedule security tasks to be run on the day and time you specify. See **Tasks** on page **909**.

Filter by group icon 

Limits the information displayed in the console to the data collected from the computers belonging to the selected group(s). See **Filtering results by groups** on page **227** for more information.

Web notifications icon 

Click the icon to show a drop-down menu with the general communications that Cytomic makes available to all console users, sorted by importance:

- Planned maintenance tasks
- Alerts regarding critical vulnerabilities
- Security tips
- Messages to start console upgrade processes. See **Management console upgrades** on page **207**.

Each communication has a priority level associated with it:

-  Important
-  Notice
-  Information

The number on the icon indicates the number of new (unread) web notifications.

To delete a web notification, click the X icon. Deleted notifications are not shown again, and the number on the icon changes to show the total number of available notifications.

General options icon 

Displays a drop-down menu that enables you to access product documentation, change the console language, and access other resources.

Option	Description
Online Help	Enables you to access the product's web help.
Cytomic Insights Administration Guide	Provides access to the Cytomic Insights Administration Guide (if the module has been purchased).
Advanced EPDRAdministration Guide	Provides access to the Advanced EPDRAdministration Guide.
Cytomic Data Watch Administration Guide	Provides access to the Cytomic Data Watch Administration Guide (if the module has been purchased).
Technical Support	Takes you to the technical support website for Advanced EPDR.
Suggestion Box	Launches the mail client installed on the computer to send an email to the Cytomic technical support department.
License Agreement	Shows the product's EULA (End User License Agreement).
Data Processing Agreement	Shows the data processing agreement for the platform in compliance with European regulations.
Advanced EPDR Release Notes	Takes you to a support page detailing the changes and new features incorporated into the new version.
Language	Select the language of the management console.

Option	Description
About...	Shows the version of the different elements that make up Advanced EPDR. • **Version**: product version. • **Protection version**: internal version of the protection module installed on computers. • **Agent version**: internal version of the communications module installed on computers.

Table 3.1: General options menu

User account icon

Displays a drop-down menu with the following options:

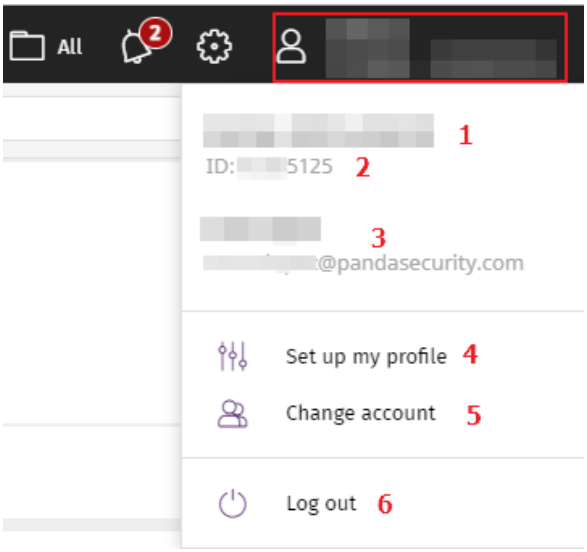


Figure 3.2: User account drop-down menu

Option	Description
Account	Name of the account used to access the console.
Customer ID	This is the number used by Cytomic to identify the customer. It is sent in the welcome email and requested in all communications with support.
Email address	Email address used to access the console.

Option	Description
Set up my profile	Modify the user account information. See **Editing the personal details for a user account** on page **65**.
Change account	Lists all the accounts that are accessible to the administrator and enables you to select an account to work with.
Log out	Logs you out of the management console and takes you back to the IDP page.

Table 3.2: User account menu

Side menu (2)

The side menu gives you access to different subareas within the selected area. It acts as a second-level selector with respect to the top menu.

The side menu changes depending on the area you are in, adapting its contents to the information required.

To maximize the display area of the center panel, reduce the size of the side menu by clicking the panel splitter. Reducing it too much causes the side menu to be hidden. To restore the menu to its original size, click the icon.

Center panel (3)

Shows all relevant information for the area and subarea selected by the administrator. **Figure 3.1:** shows the **Status** area, **Security** subarea, with widgets that enable you to interpret the security information collected from the network. For more information about the widgets, see **Security module panels/widgets** on page **661**.

Shortcut to Cytomic Insights (4)

Cytomic Insights gives access to the management console for the Cytomic Data Watch and Cytomic Insights modules. Both modules share a console specifically designed to generate advanced charts and tables with relevant information about the activity of all processes run on the organization's workstations and servers.

Basic elements of the web console

Tab menu

The most complex areas of the console provide a third-level selector in the form of tabs that show the information in an organized way.

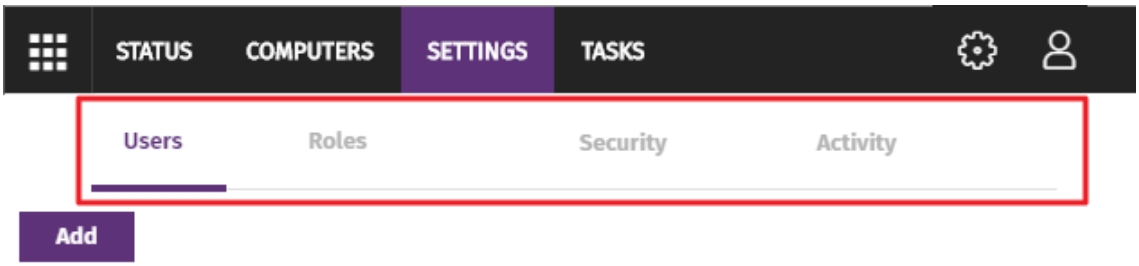


Figure 3.3: Tab menu

Action bar

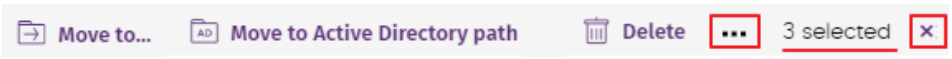


Figure 3.4: Action bar

To make it easier to navigate the console and perform some common operations on workstations and servers, an action bar appears at the top of certain pages in the console. The number of buttons on the action bar adapts to the size of the page. Click the ••• icon at the right end of the action bar to view the buttons that do not fit within the allocated space.

Finally, the right corner of the action bar shows the total number of selected computers. Click the cross icon to undo your selection.

Filter and search tools

The filter and search tools enable you to filter and show information of special interest. Some filter tools are generic and apply to an entire page, for example, those shown at the top of the **Status** and **Computers** pages.

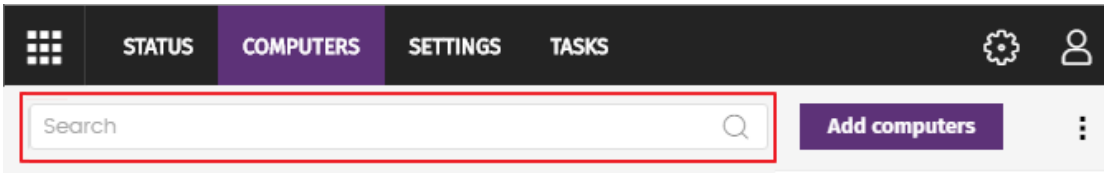


Figure 3.5: Filter tool

Some filter tools are hidden under the **Filters** button and enable you to refine your searches according to categories, ranges, and other parameters based on the information shown.

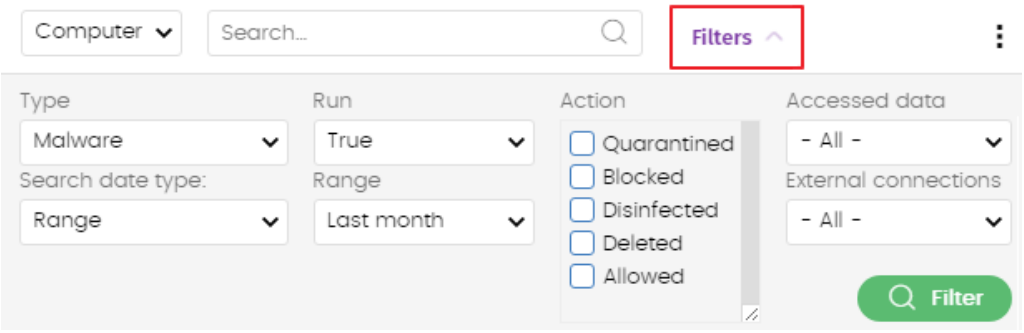


Figure 3.6: Data filter tool in lists

Other interface elements

The Advanced EPDR web console uses standard interface elements for configuring settings, such as:

- Buttons. **(1)**
- Links. **(2)**
- Checkboxes. **(3)**
- Drop-down menus. **(4)**
- Combo boxes. **(5)**
- Text fields. **(6)**

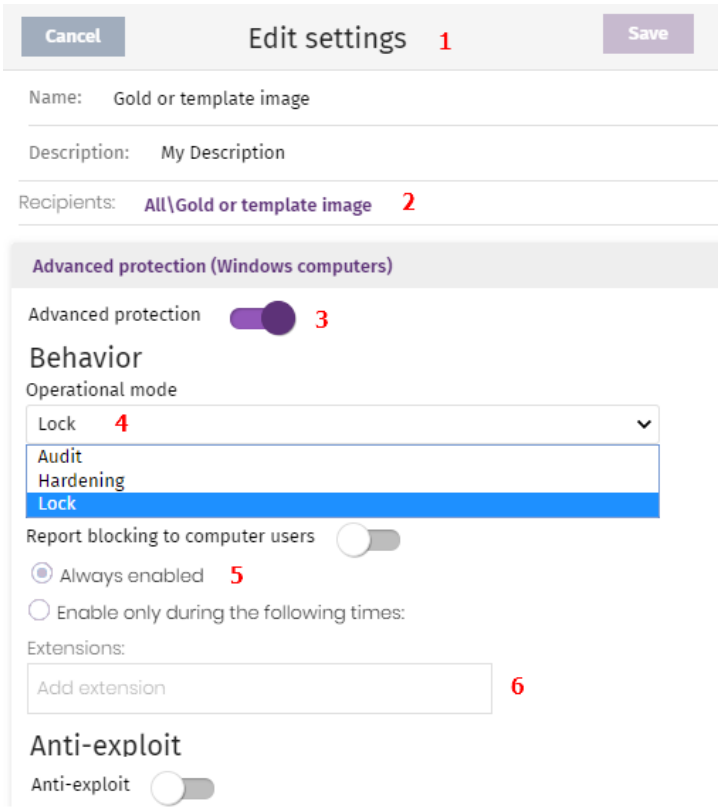


Figure 3.7: Controls for using the management console

Sort by button

Some lists of items, such as those displayed on the **Tasks** page (top menu **Tasks**) or on the **Settings** page (top menu **Settings**), show a sort by button in the upper-right or lower-right corner of the list. This button enables you to sort the items in the list according to different criteria:

- **By creation date**: Items are sorted based on when they were added to the list.
- **By name**: Items are sorted based on their name.
- **Ascending**
- **Descending**

Context menus

These are drop-down menus that open when you click the icon. They show options related to the area they are in.

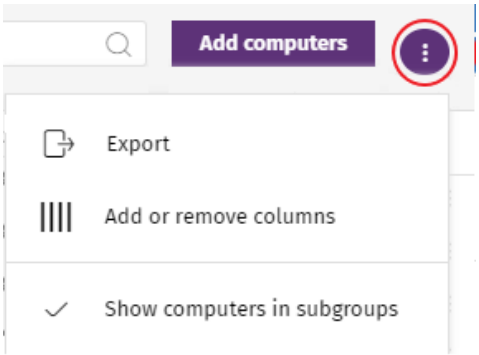


Figure 3.8: Context menus

Copy contents and Delete contents buttons

If you point the mouse to a text box that enables you to enter multiple values separated by spaces, two buttons appear for copying and deleting contents.

- **Copy button (1)**: Copies the items in the text box to the clipboard, separated by carriage returns. A message appears in the console when the operation is complete.
- **Delete button (2)**: Clears the contents of the text box.

Figure 3.9: Copy and Delete buttons

- Click on a text box and press Control+v to insert the contents of the clipboard, provided it contains text lines separated by line breaks.

Status area overview

The **Status** menu includes the main visualization tools. It is divided into several sections:

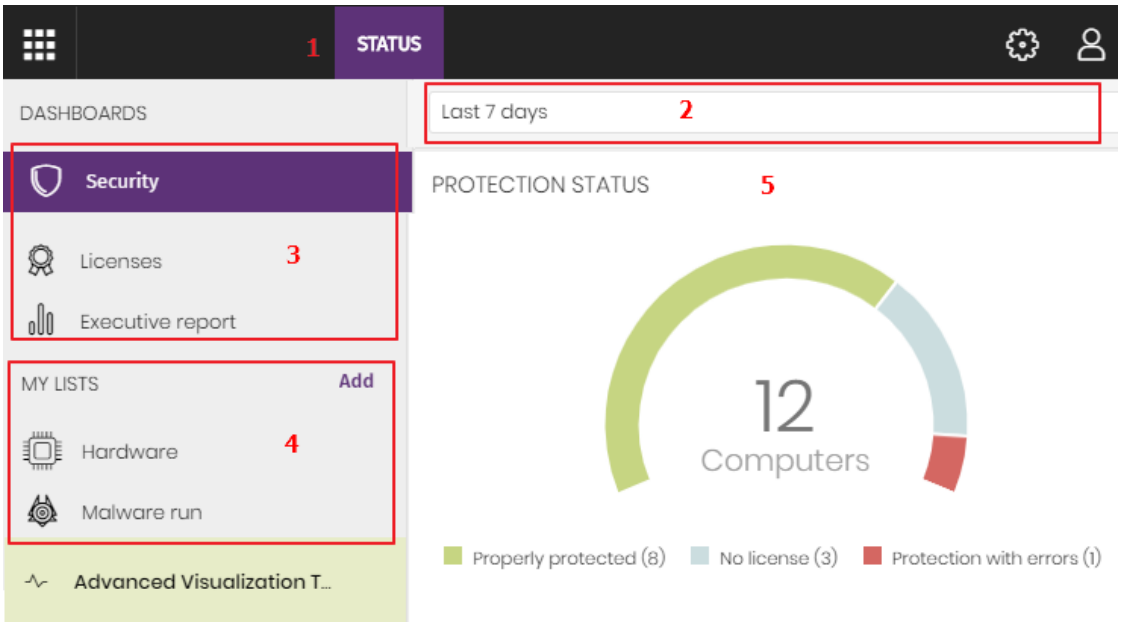


Figure 3.10: Status page (dashboards and access to lists)

Access to dashboards (1)

The **Status** top menu provides access to various types of dashboards. From here, you can also access different widgets and lists.

Widgets represent specific aspects of the managed network, while more detailed information is available through the lists.

Time period selector (2)

Dashboards show information for the time period you select from the drop-down menu at the top of the **Status** page. You can select these time periods:

- Last 24 hours
- Last 7 days.
- Last month.
- Last year.

> *Some widgets do not show information for the last year. If information from the last year is not available for a specific widget, a notification appears.*

Dashboard selector (3)

- **Security**: Information about the security status of the IT network. For more information about the available widgets, see **Security module panels/widgets** on page **661**.
- **Web access**: Web browsing filtering. For more information about the available widgets, see **Security module panels/widgets** on page **661**.
- **Cytomic Patch**: Information about updates for the operating system and third-party software installed on computers. For more information about the available widgets, see **Security module panels/widgets** on page **661**.
- **Cytomic Data Watch**: Information about the monitoring of the personal data stored on the computers on your network. For more information about the available widgets, see **Introduction to Cytomic Data Watch operation** on page **372**.
- **Cytomic Encryption**: Information about the encryption status of computers internal storage devices. For more information about the available widgets, see **Security module panels/widgets** on page **661**.
- **Licenses**: Information about the status of the Advanced EPDR licenses assigned to the computers on your network. For more information about license management, see **Licenses** on page **189**.
- **Scheduled reports**: For more information about how to configure and generate reports, see **Scheduled sending of reports and lists** on page **865**

My lists (4)

Lists are data tables with the information presented in widgets. They include highly detailed information and have search and filter tools to help you locate the information you need.

Information panels/widgets (5)

Each dashboard has a series of widgets related to specific aspects of network security.

The information in the widgets is generated in real time and is interactive: Point the mouse to an item in a widget to display a tooltip with more detailed information.

All the graphs include a legend explaining the meaning of the data displayed and have hotspots that can be clicked on to show lists with predefined filters.

Advanced EPDR uses several types of graphs to show information in the most practical way according to the type of data displayed:

- Pie charts.
- Histograms.
- Line charts.

Managing lists

Advanced EPDR structures the information collected at two levels: a first level that presents the data graphically through dashboards and widgets, and a second, more detailed level, where the data is presented in tables. Most widgets have an associated list, so you can quickly see information graphically in the widget and then get more detail from the list.

Advanced EPDR enables you to schedule and email a report of the list results. This eliminates the need to access the web console to view the details of the events that have taken place across the network. Additionally, this feature makes it easier to share information among departments and enables organizations to build an external repository containing a history of all the events that have occurred, outside the boundaries of the web console. With this repository, the management team can keep track of the generated information free from third-party interference.

Templates, settings, and views

A list consists of two items: a template and a filter.

A template can be thought of as a source of data about a specific area covered by Advanced EPDR.

A filter is a specific configuration of the filter tools associated with each template.

A filter applied to a template results in a 'list view' or, simply, a 'list'. Administrators can create and save new lists for later consultation simply by editing the filters associated with a template, saving management time.

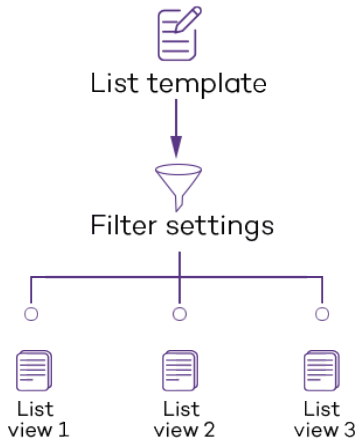


Figure 3.11: Generating three lists from a single template/data source

List templates

Click the **Status** menu at the top of the console. From the left panel, in the **My lists** section, click **Add**. A window opens with all available templates grouped by type:

Group	List	Description
General	Licenses	Shows details of the license status of the computers on your network. See **Licenses module lists** on page **196** for more information.
	Unmanaged computers discovered	Shows all Windows computers on your network that do not have the Advanced EPDR software installed. See **Unmanaged computers discovered list** on page **126** for more information.
	Computers with duplicate name	Shows computers with the same name and belonging to the same domain. See **Computers with duplicate name** on page **249**for more information.
	Software	Shows the software installed on the computers on your network. See **Software** on page **246** for more information.
	Hardware	Shows the hardware installed on the computers on your network. See **Hardware** on page **243**for more information.
Security	Computer protection status	Shows details of the protection status of the computers on your network. See **Computer protection status** on page **683**for more information.
	Malware and PUP activity	Shows a list of the threats detected on the computers protected by Advanced EPDR. See **Malware/PUP activity** on page **691**for more information.
	Exploit activity	Shows the number of vulnerability exploit attacks suffered by the Windows computers on your network. See **Exploit activity** on page **694**for more information.

Group	List	Description
	Currently blocked programs being classified	Shows a table with files which, although they have not finished being classified, Advanced EPDR has initially detected represent a potential risk. See **Malware/PUP activity** on page **691** for more information.
	Threats detected by the antivirus	Provides complete, consolidated information about all detections made on all supported platforms and in all the infection vectors scanned by the solution. See **Threats detected by the antivirus** on page **701** for more information.
	Intrusion attempts blocked	Shows the intrusion attempts blocked by the computer's firewall. See **Intrusion attempts blocked** on page **711** for more information.
	Blocked devices	Shows details of all computers on your network with limitations regarding access to peripherals. See **Blocked devices** on page **707** for more information.
	Blocks by advanced security policies	Shows detected scripts and unknown programs that use advanced infection techniques. See **Blocks by advanced security policies** on page **698**
	Blocks by advanced security policies	Shows a list of the advanced threats detected on the computers protected by Advanced EPDR. See **Security module lists** on page **682** for more information.
	Blocked connections	Shows the connections blocked by the local firewall. See **Intrusion attempts blocked** on page **711** for more information.
	Detected IOCs	Shows the indicators of compromise found on the customer's computers.

Group	List	Description
		See **Security module lists** on page **682** for more information.
	Indicators of attack (IOA)	Shows confirmed indicators of advanced attacks on the network. See **Indicators of attack (IOA)** on page **624**.
Cytomic Patch	Patch management status	Shows details of all computers on the network compatible with Cytomic Patch. See **Patch management status** on page **478** for more information.
	Available patches	Shows a list of all missing patches on the computers on your network and published by Cytomic. See **Available patches** on page **467**for more information.
	Installation history	Shows the patches that Advanced EPDR tried to install and the computers that received them during the selected time period. See **Installation history** on page **498**for more information.
	End-of-Life programs	Shows information about the end of life of the programs installed on your network, grouped by the end-of-life date. See **End-of-Life programs** on page **506**for more information.
	Excluded patches	Shows the computer-patch pairs excluded from installation tasks. See **Excluded patches** on page **509**for more information.
Activity control	Web access by category	Shows the web pages visited by users on your network, grouped by category. See **Top 10 most accessed categories** on page **678**for

Group	List	Description
		more information.
	Web access by computer	Shows the web pages visited by users on your network, grouped by device. See **Top 10 most accessed categories by computer** on page **679**for more information.
Activity control	Programs blocked by the administrator	Shows all attempts to run programs blocked by the administrator on the computers on your network. See **Programs blocked by the administrator** on page **575**for more information.
Data protection	Encryption status	Shows information about the computers on your network compatible with the encryption feature. See **Encryption status** on page **563**for more information.
	Cytomic Data Watch status	Shows the status of the Cytomic Data Watch module included in Advanced EPDR. See **Cytomic Data Watch status** on page **409**for more information.
	Files with personal data	Shows all PII files found on your network, along with their type, location, and other relevant information. See **Files with personal data** on page **417**for more information.
	Computers with personal data	Shows the number of PII files found on each computer on your network. See **Computers with personal data** on page **421**for more information.

Group	List	Description
	Files deleted by the administrator	Shows the status of the files deleted by the administrator using the Cytomic Data Watch module. See **Files deleted by the administrator** on page **426**for more information.

Table 3.3: Templates available in Advanced EPDR

Additionally, there are other templates you can directly access from the context menu of certain lists or from certain widgets on the dashboards. See the chapter dealing with the relevant widget.

List sections

Lists have a number of tools in common to make interpretation easier. Following is a description of the main elements in a sample list.

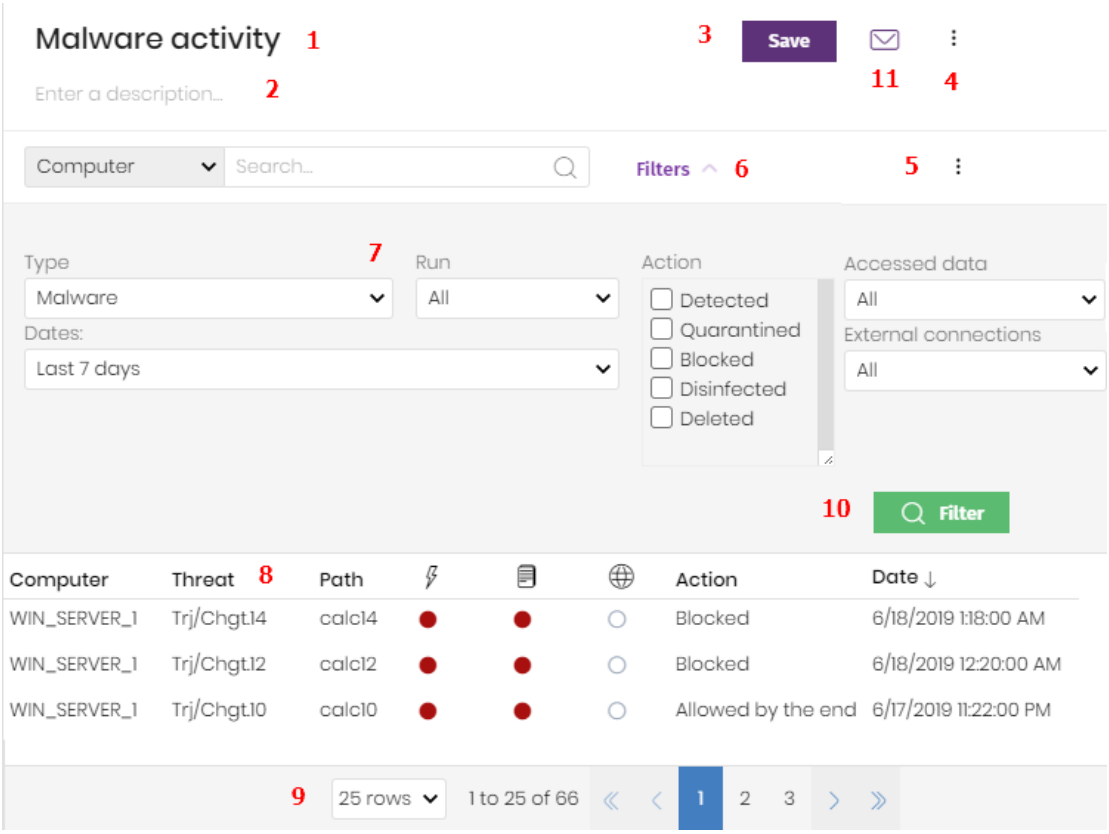


Figure 3.12: List page elements

- **List name (1)**: Identifies the information in the list.
- **Description (2)**: A free text box for specifying the purpose of the list.
- **Save (3)**: A button for saving the current view and creating a new list in the My lists tree.

- **Context menu (4)**: Drop-down menu with the actions you can take on the list (copy and delete). See **Operations with lists** for more information.
- **Context menu (5)**: Drop-down menu with the list export options.
- **Link to filter and search tools (6)**: Click it to display a panel with the available filter tools. After you configure your search, click the **Filter (10)** button.
- **Filtering and search parameters (7)**: Enable you to filter the data shown in the list.
- **Sorting order (8)**: Click a column header to sort the list by that column. Click the same header a second time to switch between ascending and descending order. This is indicated with arrows (a ↑ arrow or a ↓ arrow). If you are accessing the management console from a small mobile device, click the  icon in the lower-right corner of the list to display a menu with the names of the columns included in the table.
- **Pagination (9)**: At the bottom of the table there are pagination controls to help you quickly move from page to page.

Icon	Description
	Rows per page selector.
	Range of rows displayed out of the total number of rows.
	First page link.
	Previous page link.
	Numbered links to access pages directly.
	Next page link.
	Last page link.

Table 3.4: Pagination controls

- **Scheduled report (11)**: Advanced EPDR enables you to send a CSV file with the contents of the list by email. See **Scheduled sending of reports and lists** on page **865** for more information.

Operations with lists

From the top menu, select **Status**. In the side menu, go to **My lists** to view all lists created by the administrator as well as a number of predefined lists that Advanced EPDR includes by default. For more information, see **Predefined lists**.

Creating a custom list

You can create a new custom list/view in multiple ways:

- **From the My lists side panel**
  - From the left panel, in the **My lists** section, click **Add**. A window opens with all available templates.
  - Choose a template, configure the filter tools, edit the name and description of the list, and click the **Save (3)** button.
- **From a dashboard widget**
  - Click a widget on the dashboard to open its associated template.
  - Click its context menu **(4)** and select **Copy**. A new list is created.
  - Edit the filters, name, and description of the list. Click the **Save** button **(3)**.
- **From an existing list**
  - You can make a copy of an existing list by clicking its context menu **(4)**. Then, click **Copy**. A new list is immediately generated with the name "Copy of...".
  - Edit the filters, name, and description of the list. Click the **Save** button **(3)**.
- **From the context menu of the My lists panel**
  - Click the context menu for the list you want to copy.
  - Click **Make a copy**. A new template view is created with the name "Copy of...".
  - Edit the filters, name, and description of the list. Click the **Save** button **(3)**.

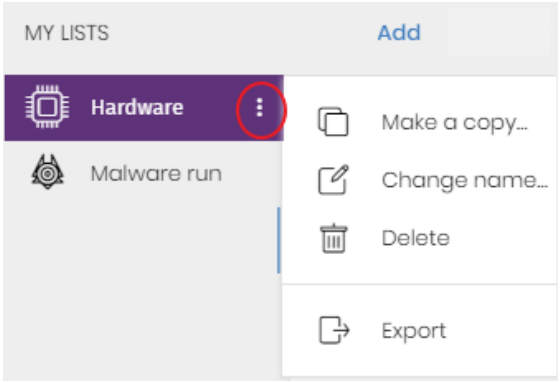


Figure 3.13: Context menu for the lists accessible from the My lists panel

Deleting a list

You can delete a list in multiple ways:

- **From the My lists panel**
  - From the **My lists** panel, click the context menu for the relevant list.
  - Click the icon.
- **From the list**
  - Click the list context menu **(4)**.
  - From the drop-down menu that opens, click the icon.

Copying a list

You can copy a list in multiple ways:

- **From the My lists panel**
  - From the **My lists** panel, click the context menu for the relevant list.
  - Click the icon.
- **From the list**
  - Click the list context menu **(4)**.
  - From the drop-down menu that opens, click the icon.

Exporting a list

You can export lists to CSV format to get more information than is shown in the web console. For information about the fields in each exported file, see the relevant chapter of this Administration Guide. You can export a list in multiple ways:

- **From the My lists panel**
  - If the list does not support export of details, click the icon. A CSV file is downloaded with the list data.
  - If the list supports export of details, click the icon **(5)**. A drop-down menu appears.
  - Click **Export**. A CSV file is downloaded with the list data.
- **From the list**
  - Click the list context menu **(4)**.
  - From the drop-down menu that opens, click the **Export** icon. A CSV file is downloaded with the list data.

Depending on the module or feature, some lists can provide more details in the exported file than others.

Exporting a list details

You can export a list details to get more information than is shown in the exported CSV file. For more information about the fields in each exported file, see the relevant chapter of this Administration Guide. You can export a list in multiple ways:

- **From the My lists panel**
  - Click the icon **(5)**. A drop-down menu opens.
  - Click **Export list and details**. A CSV file is downloaded with the list details.
- **From the list**
  - Click the list context menu **(4)**. A drop-down menu opens.
  - Click the **Export list and details** icon . A CSV file is downloaded with the list details.

Depending on the module or feature, some lists can provide more details in the exported file than others.

Configuring a custom list

- Assign a new name to the list **(1)**. By default, the console creates new names for lists by adding the text "New" to the type of list, or "Copy of" if the list is a copy of a previous one.
- Assign a description **(2)**: This step is optional.
- Click the **Filters** link **(6)** to display the filter and search options.
- Click **Filter (10)** to apply the configured filter and check if it meets your needs. The list shows the search results.
- Click **Save (3)**. The new list appears in the **My lists** section in the left panel. You can access it by clicking its name.

Scheduling a list to be sent by email

- **From the context menu of the My lists panel**
  - Click the context menu for the list you want to send. Select the **Schedule report** option.

- A dialog box opens where you can enter the necessary information to automatically send the list.

- **From the list**
  - Click the **(11)** icon. A dialog box opens where you can enter the necessary information to automatically send the list.

For more information, see ***Scheduled sending of reports and lists*** *on page* ***865****.*

Available actions for computers in lists

Some lists include checkboxes that enable you to select computers. When you select one or more computers, an action bar appears at the top of the page. This bar makes it easier to manage the selected workstations and servers. See **Action bar (10)** on page **284**.

Each list page shows information about 25 computers. To take action on all computers on a page, select the checkbox in the upper-left corner of the list **(1)**:

With the **Computers** and **Unmanaged computers discovered** lists, after you select this checkbox, you can take action on all computers on all of the list pages **(2)**.

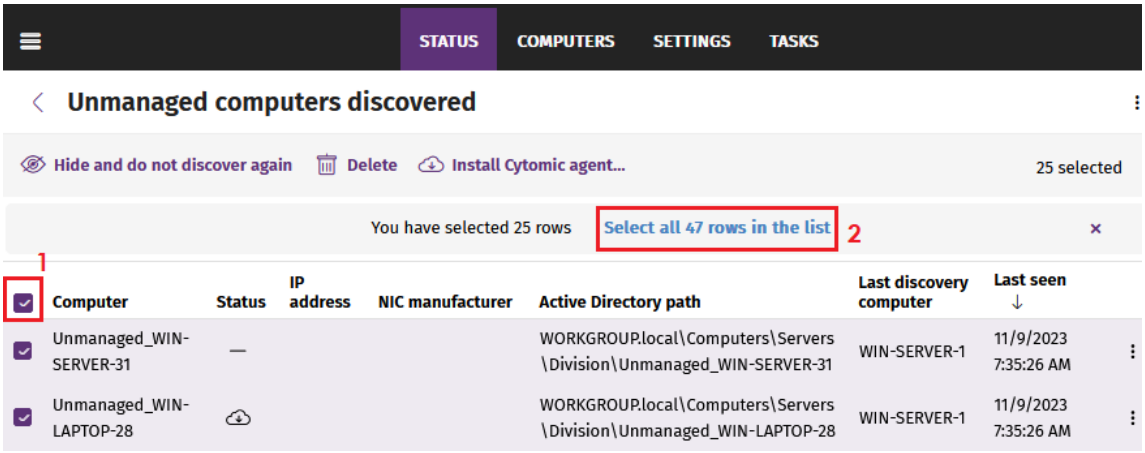


Figure 3.14: Select computers on a list

Predefined lists

The management console includes various predefined lists:

- Unprotected workstations and laptops.
- Unprotected servers.
- Hardware
- Software

Unprotected workstations and laptops

Shows all desktop and laptop computers, regardless of the operating system installed, which could be vulnerable to threats due to a problem with the protection:

- Computers on which the Advanced EPDR software is currently being installed or the installation failed.
- Computers on which the protection is disabled or has errors.
- Computers without a license assigned or with an expired license.
- See **Computer protection status** on page **683** for more information.

Unprotected servers

Shows all servers, regardless of the operating system installed, which could be vulnerable to threats due to a problem with the protection:

- Servers on which the Advanced EPDR software is currently being installed or the installation failed.
- Servers on which the protection is disabled or has errors.
- Servers without a license assigned or with an expired license. See **Computer protection status** on page **683** for more information.

Software

Shows a list of the programs installed across your network. See **Software** on page **246** for more information.

Hardware

Shows a list of the hardware components installed across your network. See **Hardware** on page **243** for more information.

Chapter 4

Accessing, controlling, and monitoring the management console

Advanced EDR implements multiple resources for limiting, controlling, and monitoring access to the web management console and the actions that network administrator can take through it:

- User account.
- Roles assigned to user accounts.
- User account activity log.

Chapter contents

General concepts

User account

A user account is a resource consisting of a set of data that Advanced EPDR uses to allow administrator to access the web console and set the actions that administrators can take on user computers.

User accounts are used only by the IT administrators who access the Advanced EPDR console. Each administrator can have one or more user accounts assigned.

The main characteristics of user accounts are:

- They are accounts managed by the administrator. The administrator can create or delete accounts, change their passwords, add or remove permissions, or enable two-factor authentication.
- A user account provides access to all products purchased from Cytomic through Cytomic Central.
- A user account can provide access to multiple customers. The administrator can choose the product they want to access in Cytomic Central, and then select the console they want to access on the **Select account** page.

Cytomic Central

This is a portal that centralizes access to all the products included in the Cytomic portfolio. A user account created in a Cytomic product provides access to the portal, from which the administrator can access the consoles of the purchased products.

For more information, see ***https://info.cytomic.ai/central/index.htm#t=001.htm****.*

Customer account

This is a resource consisting of confidential data associated with a customer that has purchased a Cytomic product. The customer's fiscal address, full name, tax identification number, and other data are part of the customer account.

Managing user accounts

A user account consists of multiple pieces of information that are generated when the account is created:

- **Account login email address**: Identifies the users accessing the console.
- **Account password**: Allows or prevents access to the management console.
- **Assigned role**: Determines which computers the account user can manage and the actions they can take.

Creating the first user account

The procedure to create the first user account is different from the steps to create subsequent accounts. The first user account always has the Full Control role assigned. This role enables you to perform any action through the console. You cannot remove or modify this account.

Receive the welcome email

- After you purchase Advanced EPDR, you receive an email message from Cytomic.
- Click the **Click here** link in the message to access the website from which you can create the first user account.

Complete the Create your Cytomic account form

- Enter your email address and click **Create**. You will receive a new email message at the email address you specified in the form to activate the account you created.

Activate the user account

- Click the activation button in the message you received to verify the email address you provided when you created the user account. If the button does not work, copy and paste the link included in the message into your browser. The **Cytomic Account** page opens.
- Enter the password for the account. The password length must be at least 8 characters. The password must contain at least one number and at least one letter.
- Choose the country. Click **Activate account**. The **One second and you are done** page opens.
- Enter your first and last name, date of birth, phone number, and address. Click **Save**. You can skip this step by clicking **Not now**. The Cytomic Central end-user license agreement opens.
- Click **Accept and continue**. The Cytomic Central page opens, from which you can access all services purchased from Cytomic.

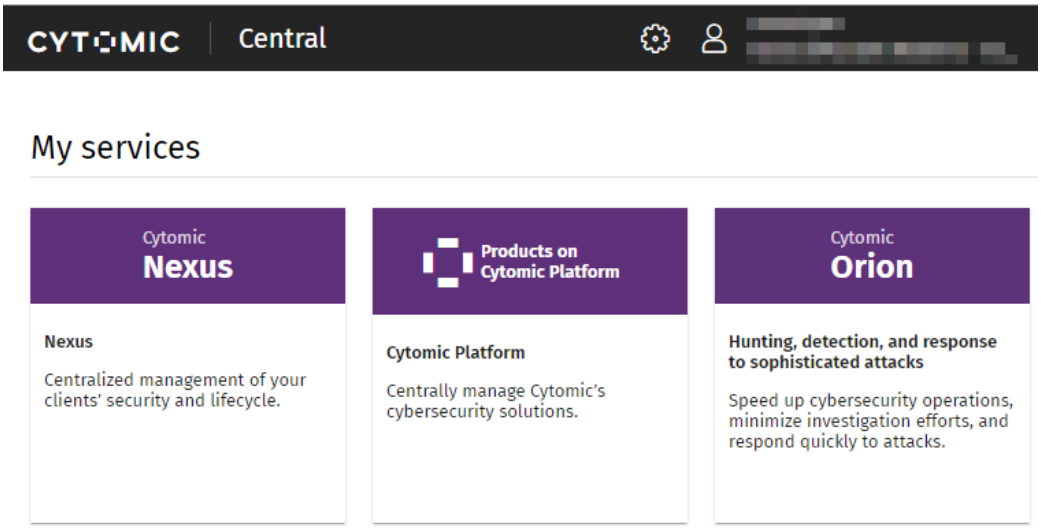


Figure 4.1: Cytomic Central page

- To access the Advanced EPDR console, click the Advanced EPDR tile in **My services**. The first time you access the console, a wizard opens that prompts you to accept the license and data processing agreements.
    - On the **License agreement** page, click the **Accept and continue** button.
    - On the **Data processing agreement** page, click **Go to data processing agreement**.
    - On the **Data processing agreement** page, click **Accept**. The Advanced EPDR console opens.

After the process is complete, the WatchGuard user account can access the Advanced EPDR console. See **Access to the web console** on page **37**.

Creating subsequent user accounts

After you have created the first user account, you can access the Advanced EPDR management console, from which you can create all other user accounts you may need.

- Make sure the user has the **Manage users and roles** permission assigned. See **Understanding permissions**.
- From the top menu, select **Settings**. From the side menu, select **Users.**
- Select the **Users** tab. A page opens that shows a list of all users created in the management console.
- Click **Add**. The **Add user** page opens.
- In the **Login email** field, enter the console user email address. Enter a description if needed.
- Choose a role for the user account. See **Understanding permissions**.

- Click **Save**. Advanced EPDR sends an email to the specified email address so that the user can generate an access password and accept the terms of the license and data processing agreements.

> *Before you begin this procedure, make sure you have logged out of the WatchGuard Portal and the Advanced EPDR console and you have closed your web browser.*

Editing the personal details for a user account

- In the management console, click the icon in the upper-right corner of the page. A drop-down menu appears.
- Select **Set up my profile**.

Cytomic Central

- The **Cytomic Account** page opens.
- In the left menu, select **Profile**. Fill the form with the personal details for the account.
- Click **Save**. The changes are stored on the Cytomic server.

Editing the email address or password for a user account

- In the management console, click the icon in the upper-right corner of the page. A drop-down menu appears.
- Select **Set up my profile**.

Cytomic Central

- The **Cytomic Account** page opens.
- In the left menu, select **Login**. Click the **Change email address** or **Change password** links. A page opens that prompts you to validate the old data and enter the new one.
- Click **Change**.

Removing or blocking user accounts

- Make sure the user has the **Manage users and roles** permission assigned. See **Understanding permissions**.
- From the top menu, select **Settings**. From the side menu, select **Users.**
- Select the **Users** tab. A page opens that shows a list of all users created in the management console.
- Click the icon for the user account you want to remove.

- To temporarily disable access from a user account to the web console, click the account and enable the **Block this user** toggle. Access from the account to the management console is denied. If the account user is currently logged in, they are logged out immediately. Also, email alerts are no longer sent to the email addresses configured in the account settings.

Enabling two-factor authentication

Advanced EPDR supports the two-factor authentication (2FA) standard to add an additional layer of security beyond that provided by the 'user-password' basic pair. This way, when you try to access the web console, you are prompted to enter an additional authentication item: a code that only the account owner has. This is a random code that is generated on a specific device, typically the Advanced EPDR administrator personal smartphone or tablet.

Requirements for enabling 2FA

- Access to a personal smartphone or tablet with a built-in camera.
- Download the WatchGuard AuthPoint free app (or similar) from:
  - **iOS**: **https://apps.apple.com/app/watchguard-authpoint/id1335115425**
  - **Android**: **https://play.google.com/store/apps/details?id=com.watchguard.authpoint**

Enabling 2FA

- In the management console, click the icon in the upper-right corner of the page. A drop-down menu appears.
- Select **Set up my profile**.

Cytomic Central

- The **Cytomic Account** page opens.
- From the side menu, select **Login**. In the **Two-factor authentication** section, click the **Enable** link. The **Synchronization using an authentication app** dialog box opens.
- The first time that you use the WatchGuard AuthPoint app on your mobile device, tap **Activate**. If you have used it before, tap the QR code icon in the upper-right corner of the dialog box. The mobile device camera opens.

Figure 4.2: Scanning the QR code with WatchGuard AuthPoint

- Point the camera at the QR code in the Advanced EPDR console. A new entry is added to WatchGuard AuthPoint and a token is generated every 30 seconds.
- Enter the code generated by WatchGuard AuthPoint in the Advanced EPDR console to link the device to the user account. Click **Verify**. A dialog box opens that shows the message **Two-factor authentication is enabled**.
- Click **OK**.

Accessing the web console from Cytomic Central using an account with 2FA enabled

- Go to **https://www.pandacloudsecurity.com/PandaLogin/**. Enter your user name and password. Click **Log in**.
- Enter the verification code generated by WatchGuard AuthPoint on your mobile device. Click **Verify**. The **Cytomic Central** page opens.

Forcing all console users to use 2FA

The user account with which you enforce the use of 2FA must have the **Manage users and roles** permission assigned and full visibility into the IT network. See **Managing roles and permissions**

- From the top menu, select **Settings**. Select the **Security** tab.
- Select the option **Require users to have two-factor authentication enabled to access this account**.
- If the user account with which you force all console users to use 2FA does not have two-factor authentication enabled, a warning message appears and prompts you to access your **Cytomic Account** and enable the feature. See **Enabling 2FA**.

User list

Required permissions

All console users can view the user list.

Accessing the list

- Select the **Settings** menu at the top of the console. Select **Users** in the side menu.
- Select the **Users** tab. A list appears that shows all user accounts created in Advanced EPDR, along with the following information:

Field	Description
Account name	User account name.

Field	Description
Role	Role assigned to the user account.
Email account	Email account assigned to the user.
Padlock	Indicates whether the account has two-factor authentication (2FA) enabled.
Status	Indicates whether the user account is active or blocked.

Table 4.1: Fields in the user list

Sorting and searching in the user list: Click the  icon to sort the user list in ascending/descending order, by name, or by creation date. To search for a user, type the text in the search box and click the  icon.

Fields displayed in the exported file

Field	Definition	Values
Client	Customer account the service belongs to.	Character string
Name	Name of user profile.	Character string
Login email	Email address used to access the console	Character string
Role	Role assigned to the user.	Character string
Description	Description added to the user profile.	Character string
Two-factor authentication	Indicates whether the account has two-factor authentication enabled or disabled.	Boolean
Blocked	Indicates whether the user account is active or blocked.	Boolean

Table 4.2: Fields in the User list exported file

Filter tools

Field	Comment	Values
Search user	Enables you to search by user name and email address. You can type only a partial string.	Character string
Blocked	Finds blocked user accounts in the list.	• All • Yes • No
Two-factor authentication	Finds user accounts that have two-factor authentication enabled.	• All • Enabled • Disabled

Table 4.3: Filters available in the user list

Sorting tools

To display the available sorting criteria, click the  icon.

Managing roles and permissions

Basic concepts

Roles

A role is a specific configuration of permissions that is applied to one or more user accounts. A user account is authorized to view or modify certain resources in the console depending on the role assigned to it.

A user account can have only one role assigned. However, a role can be assigned to more than one user account.

A role consists of the following:

- **Role name**: This is purely for identification and is assigned when the role is created.
- **Visibility**: Restricts access to certain computers on the network.
- **Permission set**: Determines the specific actions that the user account can take on computers belonging to groups defined as accessible.

Predefined roles

A Advanced EPDR license always has two predefined roles. These roles cannot be edited or deleted. Any user account can be assigned these roles through the web console.

Full Control role

The first user account that is created always has the Full Control role assigned. This account enables you to take all the actions available in the console on the computers added to Advanced EPDR.

Read-Only role

This role provides access to all sections of the console, but does not enable you to create, modify, or delete settings profiles, tasks, etc. That is, it provides total visibility of the environment but does not allow you to make any changes. This role is particularly suited for network administrators responsible for monitoring the network, but who do not have enough permissions to take actions such as editing settings profiles or launching on-demand scans.

Permission

A permission controls access to a specific section of the management console. There are different types of permissions that provide access to many sections of the Advanced EPDR console. A specific configuration of all available permissions makes up a role, which can be assigned to one or more user accounts.

Visibility

Each user account enables you to configure the security of a subset of computers from all the computers added to the Advanced EPDR console. This is determined by the account visibility.

Creating a role

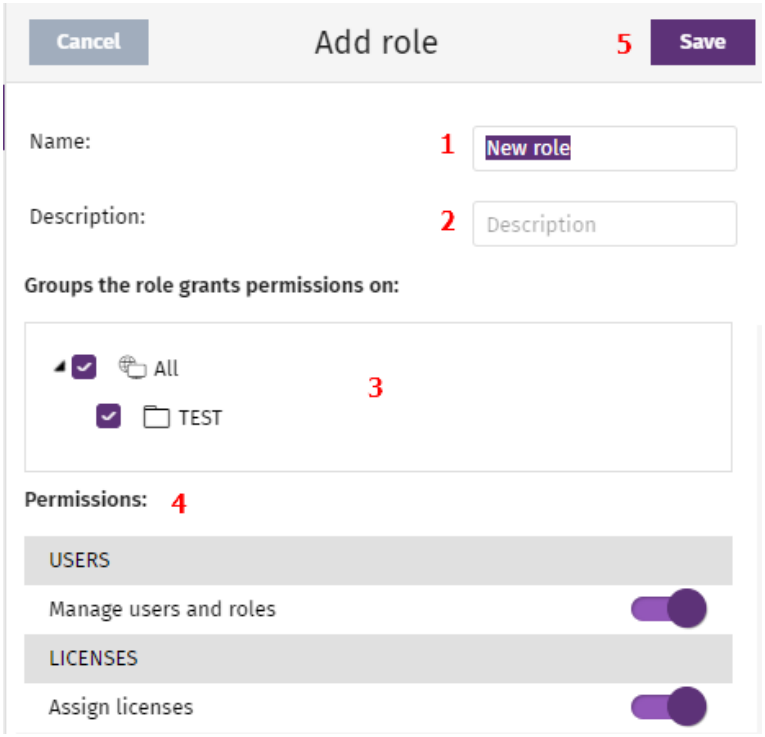


Figure 4.3: Add role page

- Select the **Settings** menu at the top of the console. Select **Users** from the side menu. A page opens that shows a list of all created users.
- Select the **Roles** tab. Select **Add**. The **Add roles** page opens.
- Enter a name for the role **(1)** and, optionally, a description **(2)**.
- Specify the visibility for the role **(3)**.
- Enable or disable permissions **(4)**.
- Click **Save (5)**.

Limitations when creating users and roles

To prevent privilege escalation problems, users with the **Manage users and roles** permission assigned have the following limitations when it comes to creating new roles or assigning roles to existing users:

- A user account can create only new roles with the same or lower permissions than its own.
- A user account can edit only the same permissions as its own in existing roles. All other permissions remain disabled.
- A user account can assign only roles with the same or lower permissions than its own.
- A user account can copy only roles with the same or lower permissions than its own.

Deleting a role

- Select the **Settings** menu at the top of the console. Select **Users** from the side menu.
- Select the **Roles** tab. A list appears that shows all created roles.
- Click the  icon of a role to delete it. If the role you are trying to delete has user accounts assigned, the delete operation is canceled.

Copying a role

- Select the **Settings** menu at the top of the console. Select **Users** from the side menu.
- Select the **Roles** tab. A list appears that shows all created roles.
- Click the icon of a role to copy it. The **Copy role** page opens. This page shows the settings of the copied role.
- Modify the role settings. Click **Save**.

Modifying a role

- Select the **Settings** menu at the top of the console. Select **Users** in the side menu.
- Select the **Roles** tab. A list appears that shows all created roles.
- Click the role you want to edit. The **Edit role** page opens.
- Modify the role settings. Click **Save**.

Understanding permissions

Manage users and roles

- **Enabled**: The account user can create, delete, and edit user accounts and roles.
- **Disabled**: The account user cannot create, delete, or edit user accounts or roles. The user can view registered users and account details, but not the list of roles created.

Assign licenses

- **Enabled**: The account user can assign and remove licenses for the managed computers.
- **Disabled**: The account user cannot assign or remove licenses, but can see whether computers have licenses assigned.

Modify computer tree

- **Enabled**: The account user has full access to the group tree, and can create and delete groups, as well as moving computers to groups already created.
- **Enabled with permission conflict**: Because of the inheritance mechanism that applies to the computer tree, any changes made to the tree structure can result in a change to the settings profiles assigned to the affected devices. For example, in cases where the administrator does not have permission to assign settings profiles, if they move a computer from one group to another, the web console will show a warning indicating that, because of the computer move operation and the inheritance mechanism applied, the settings profiles assigned to the computer that was moved might have changed (even if the administrator does not have permission to assign settings profiles). See section **Manual and automatic assignment of settings profiles** on page **296**
- **Disabled**: The account user can view the group tree and the settings profiles assigned to each group, but cannot create new groups or move computers.

Add, discover, and delete computers

- **Enabled**: The account user can deploy the installer to computers on the network and add them to the console. They can also delete computers from the console and configure all aspects related to the discovery of unmanaged computers: assign and revoke the discovery computer role, edit discovery settings, launch an immediate discovery task, and install the Cytomic agent remotely from the list of discovered computers.
- **Disabled**: The account user cannot download the installer, nor deploy it to computers on the network. Neither can the user delete computers from the console or access the computer discovery feature.

Modify network settings (proxies and cache)

- **Enabled**: The account user can create new **network settings profiles**, edit or delete existing ones, and assign them to computers in the console.
- **Disabled**: The account user cannot create new **network settings profiles**, nor delete existing ones. Neither can the user change the computers these settings profiles are assigned to.

Configure per-computer settings (updates, passwords, etc.)

- **Enabled**: The account user can create new **per-computer settings profiles**, edit or delete existing ones, and assign them to computers in the console.
- **Disabled**: The account user cannot create new **per-computer settings profiles**, nor edit or delete existing ones. Neither can the user change the computers these settings profiles are assigned to.

Configure remote control

- **Enabled**: The account user can configure remote access to Windows devices. This permission is assigned from the Cytomic console and is executed from Cytomic Orion.
- **Disabled**: The Windows computers on the network cannot be remotely managed from the Cytomic Orion web console.

Remote computer control

- **Enabled**: The account user can remotely access the Windows computers on the network they have permissions on.
- **Disabled**: The account user cannot remotely access computers on the network.

Restart and repair computers

- **Enabled**: The account user can restart workstations and servers from computer lists. They can also remotely reinstall the Advanced EPDR software on Windows computers.
- **Disabled**: The account user cannot restart computers or remotely reinstall the Advanced EPDR software.

Isolate computers

- **Enabled**: The account user can isolate and deisolate Windows and macOS computers.
- **Disabled**: The account user cannot isolate computers.

Configure security for workstations and servers

- **Enabled**: The account user can create, edit, delete, and assign security settings profiles for workstations and servers.
- **Disabled**: The account user cannot create, edit, delete, or assign security settings profiles for workstations and servers.

If you disable this permission, the **View security settings for workstations and servers** permission appears.

View security settings for workstations and servers

*This permission is accessible only if you disable the **Configure security settings for workstations and servers** permission.*

- **Enabled**: The account user can only view the security settings profiles created, as well as the settings profiles assigned to a computer or group.
- **Disabled**: The account user cannot view the security settings profiles created nor access the settings profiles assigned to computers.

Configure security for mobile devices

- **Enabled**: The account user can create, edit, delete, and assign settings profiles for mobile devices.
- **Disabled**: The account user cannot create, edit, delete, or assign settings profiles for mobile devices.

If you disable this permission, the **View security settings for mobile devices** permission appears. This permission is explained next.

View security settings for mobile devices

*This permission is accessible only if you disable the **Configure security for mobile devices** permission.*

- **Enabled**: The account user can only view the settings profiles created for mobile devices, as well as the settings profiles assigned to a specific mobile device or group of mobile devices.
- **Disabled**: The account user cannot view the settings profiles created for mobile devices nor the settings profiles assigned to mobile devices.

Use the anti-theft protection for mobile devices (locate, wipe, lock, etc.)

- **Enabled**: The account user can view the geolocation map and use the action panel to send anti-theft tasks to mobile devices.
- **Disabled**: The account user cannot view the geolocation map nor use the action panel to send anti-theft tasks to mobile devices.

View detections and threats

- **Enabled**: The account user can access the widgets and lists available on the **Security** dashboard accessible from the **Status** top menu, as well as creating new lists with custom filters.
- **Disabled**: The account user cannot access the widgets and lists available on the **Security** dashboard accessible from the **Status** top menu, nor create new lists with custom filters.

*Access to the features related to the exclusion and unblocking of threats and unknown items is governed by the **Exclude threats temporarily (malware, PUPs, and blocked items)** permission.*

View access to web pages

- **Enabled**: The account user can access the widgets and lists available on the **Web access** dashboard accessible from the **Status** top menu.
- **Disabled**: The account user cannot access the widgets and lists available on the **Web access** dashboard accessible from the **Status** top menu.

Launch scans and disinfect

- **Enabled**: The account user can create, edit, and delete scan and disinfection tasks.
- **Disabled**: The account user cannot create new scan and disinfection tasks, nor edit or delete existing ones. The user can only view those tasks and their settings.

Search for and manage IOCs

- **Enabled**: The account user can access the import, export, delete, and search options of the IOC gallery section.
- **Disabled**: The account user cannot access the import, export, delete, or search options of the IOC gallery section.

Exclude threats temporarily (malware, PUPs, and blocked items)

- **Enabled**: The account user can block/unblock and exclude/allow all types of items in the process of classification (malware, PUPs, and unknown items).
- **Disabled**: The account user cannot block/unblock or exclude/allow malware, PUPs, or unknown items in the process of classification.

*To enable a user to **Exclude threats temporarily (malware, PUPs, and blocked items)**, the **View detections and threats** permission must be enabled.*

Configure patch management

- **Enabled**: The account user can create, edit, delete, and assign patch management settings profiles to Windows, macOS, and Linux computers.

- **Disabled**: The account user cannot create, edit, delete, or assign patch management settings profiles to Windows, macOS, or Linux computers.

If you disable this permission, the **View patch management settings** permission appears.

View patch management settings

*This permission is accessible only if you disable the **Configure patch management** permission.*

- **Enabled**: The account user can only view the patch management settings profiles created as well as the settings profiles assigned to a computer or group.
- **Disabled**: The account user cannot view the patch management settings profiles created or assigned to a computer or group.

Install, uninstall, and exclude patches

- **Enabled**: The account user can create patch installation, uninstallation, and exclusion tasks, and access these lists: **Available patches**, **End-of-Life programs**, **Installation history**, and **Excluded patches**.
- **Disabled**: The account user cannot create patch installation, uninstallation, or exclusion tasks.

View available patches

*This permission is accessible only if you disable the **Install, uninstall, and exclude patches** permission.*

- **Enabled**: The account user can access the following lists: **Patch management status**, **Available patches**, **End-Of-Life programs**, and **Installation history**.
- **Disabled**: The account user cannot access these lists: **Patch management status**, **Available patches**, **End-Of-Life programs**, or **Installation history**.

Configure vulnerability assessment

- **Enabled**: The account user can create, edit, delete, and assign vulnerability assessment settings profiles to Windows, macOS, and Linux computers.

- **Disabled**: The account user cannot create, edit, delete, or assign vulnerability assessment settings profiles to Windows, macOS, or Linux computers.

If you disable this permission, the **View vulnerability assessment settings** permission appears.

View vulnerability assessment settings

*This permission is accessible only if you disable the **Configure vulnerability assessment** permission.*

- **Enabled**: The account user can only view the vulnerability assessment settings profiles created as well as the settings profiles assigned to computers or groups.
- **Disabled**: The account user cannot view the vulnerability assessment settings profiles created, nor access the settings profiles assigned to computers.

View available patches

*This permission is accessible only if you disable the **Configure patch management** permission.*

- **Enabled**: The account user can access the following lists: **Vulnerability assessment status**, **Available patchesby computers**, and **End-of-Life programs**.
- **Disabled**: The account user cannot access these lists: **Vulnerability assessment status**, **Available patches by computers**, or **End-of-Life programs**.

Configure program blocking

- **Enabled**: The account user can create, edit, delete, and assign program blocking settings profiles to Windows workstations and servers.
- **Disabled**: The account user cannot create, edit, delete, or assign program blocking settings profiles to Windows workstations and servers.

If you disable this permission, the **View program blocking settings** permission appears.

View program blocking settings

*This permission is accessible only if you disable the **Configure program blocking** permission.*

- **Enabled:** The account user can only view the program blocking settings profiles created, as well as the settings profiles assigned to computers or groups.
- **Disabled**: The account user cannot view the program blocking settings profiles created nor access the settings profiles assigned to computers.

Configure authorized software

- **Enabled**: The account user can create, edit, delete, and assign authorized software settings profiles to Windows workstations and servers.
- **Disabled**: The account user cannot create, edit, delete, or assign authorized software settings profiles to Windows workstations and servers.

If you disable this permission, the **View authorized software settings** permission appears.

View authorized software settings

*This permission is accessible only if you disable the **Configure authorized software** permission.*

- **Enabled:** The account user can only view the authorized software settings profiles created, as well as the settings profiles assigned to a computer or group.
- **Disabled**: The account user cannot view the authorized software settings profiles created, nor access the settings profiles assigned to computers on the network.

Configure indicators of attack (IOA)

Enabled: The account user can create, edit, delete, and assign indicators of attack (IOA) settings profiles.

- **Disabled**: The account user cannot create, edit, delete, or assign indicators of attack (IOA) settings profiles.
- If you disable this permission, the **View indicators of attack (IOA) settings** permission appears.

View indicators of attack (IOA) settings

*This permission is accessible only if you disable the **Configure indicators of attack (IOA)** permission.*

- **Enabled:** The account user can only view the indicators of attack (IOA) settings profiles created, as well as the settings profiles assigned to computers or groups.
- **Disabled**: The account user cannot view the indicators of attack (IOA) settings profiles created nor access the settings profiles assigned to computers.

Configure Cytomic Data Watch

- **Enabled**: The account user can create, edit, delete, and assign Cytomic Data Watch settings profiles to Windows computers.
- **Disabled**: The account user cannot create, edit, delete, or assign Cytomic Data Watch settings profiles to Windows computers.

View Cytomic Data Watch settings

*This permission is accessible only if you disable the **Configure sensitive data search, inventory, and monitoring** permission.*

- **Enabled**: The account user can only view the Cytomic Data Watch settings profiles created, as well as the settings profiles assigned to computers or groups.
- **Disabled**: The account user cannot view the Cytomic Data Watch settings profiles created, nor access the settings profiles assigned to computers on the network.

Search for data on computers

- **Enabled:** The account user can access the **Searches** widget to search for files by their name and content across the corporate network.
- **Disabled**: The account user cannot access the **Searches** widget.

View personal data inventory

- **Enabled**: The account user can access these lists: **Files with personal data** and **Computers with personal data**, and these widgets: **Files with personal data**, **Computers with personal data**, and **Files by personal data type**.

- **Disabled**: The account user cannot access these lists: **Files with personal data** or **Computers with personal data**, or these widgets: **Files with personal data**, **Computers with personal data**, or **Files by personal data type**.

Delete and restore files

- **Enabled**: The account user can access the **Delete** option from the context menu available on the **Files with personal data** list to delete and restore files.
- **Disabled**: The account user cannot access the **Delete** option from the context menu available on the **Files with personal data** list. The user cannot delete or restore files.

Configure computer encryption

- **Enabled**: The account user can create, edit, delete, and assign encryption settings profiles.
- **Disabled**: The account user cannot create, edit, delete, or assign encryption settings profiles.

View computer encryption settings

*This permission is available only if you disable the **Configure computer encryption** permission.*

- **Enabled**: The account user can only view the computer encryption settings profiles created, as well as the encryption settings profiles assigned to computers or groups.
- **Disabled**: The account user cannot view the encryption settings profiles created, nor access the encryption settings profiles assigned to computers.

Access recovery keys for encrypted drives

- **Enabled**: The account user can view the recovery keys for computers that have storage devices encrypted and managed by Advanced EPDR.
- **Disabled**: The account user cannot view the recovery keys for computers that have encrypted storage devices.

Access advanced security information

- **Enabled**: The account user can access the Cytomic Insights (from the top menu **Status**, left panel Cytomic Insights). However, the Data Access Control application included in the tool is not visible with this permission.
- **Disabled**: Access to the Cytomic Insights is prevented.

Access file access information

- **Enabled**: The account user can access the Cytomic Insights (from the top menu **Status**, left panel **Cytomic Insights**). The Data Access Control application is also accessible with this permission.
- **Disabled**: Access to the Cytomic Insights is prevented.

Access advanced Cytomic Data Watch information

- **Enabled**: The account user can access the Cytomic Data Watch extended console (from the top menu **Status**, left panel **Cytomic Insights**).
- **Disabled**: The account user cannot access the Cytomic Data Watch extended console (from the top menu **Status**, left panel **Cytomic Insights**).

Configure MDR

- **Enabled**: The account user can create, edit, and delete MDR settings profiles for all computers on the network.
- **Disabled**: The account user cannot create, edit, or delete MDR settings profiles for all computers on the network.

If you disable this permission, the **View MDR settings** permission appears.

View MDR settings

*This permission is accessible only if you disable the **Configure MDR** permission.*

- **Enabled**: The account user can only view MDR settings profiles.
- **Disabled**: The account user cannot view MDR settings profiles.

User account activity log

Advanced EPDR logs every action taken by network administrators in the web management console. This makes it very easy to find out who made a certain change, when, and on which object.

To access the activity log, click the **Settings** menu at the top of the console. Select the **Activity** tab.

Session log

The Sessions section shows a list of all accesses to the management console. It also enables you to export the information to a CSV file and filter the data.

Fields displayed in the Sessions list

Field	Description	Values
Date	Date and time that the access took place.	Date
User	User account that accessed the console.	Character string
Activity	Action performed by the user account.	• Log in • Log out
IP address	IP address from which the console was accessed.	Character string

Table 4.4: Fields in the Sessions list

Fields displayed in the exported file

Field	Description	Values
Date	Date and time that the access took place.	Date
User	User account that accessed the console.	Character string
Activity	Action taken by the account	• Log in • Log out
IP address	IP address from which the console was accessed.	Character string

Table 4.5: Fields in the Sessions exported file

Filter tool

Field	Description	Values
From	Set the start point of the search range.	Date
To	Set the end point of the	Date

Field	Description	Values
	search range.	
Users	User name.	List of all user accounts created in the management console.

Table 4.6: Filters available in the Sessions list

User actions log

The **User actions** section lists all the actions taken by the user accounts and enables you to export the information to a CSV file and filter the data.

Fields displayed in the User Actions list

Field	Description	Values
Date	The date and time when the action occurred.	Date
User	The name of the user who completed the action.	Character string.
Action	The user action completed.	See table **Item types and actions**.
Item type	The type of console object the action was performed on.	See table **Item types and actions**.
Item	The name of the console object that the action occurred on.	See table **Item types and actions**.

Table 4.7: Fields in the User Actions log

Fields displayed in the exported file

Field	Description	Values
Date	The date and time when the action occurred.	Date
User	The name of the user who completed the action.	Character string
Action	The user action completed.	See table **Item types and actions**.

Field	Description	Values
Item type	The type of console object the action was performed on.	See table **Item types and actions**.
Item	The name of the console object that the action occurred on.	See table **Item types and actions**.

Table 4.8: Fields in the User Actions exported file

Filter tool

Field	Description	Values
From	Specify the start point of the search range.	Date
To	Specify the end point of the search range.	Date
Users	User name.	List of all user accounts created in the management console.

Table 4.9: Filters available in the User Actions log

Item types and actions

Item type	Action	Item
License agreement	Accept	Version number of the accepted End User License Agreement.
Threat	Allow	Name of the threat the action was performed on.
	Stop allowing	Name of the threat the action was performed on.
Information search	Launch	Name of the search the action was performed on.
	Delete	Name of the search the action was performed on.

Item type	Action	Item
	Cancel	Name of the search the action was performed on.
Account	Update console	From Initial version to Target version.
	Cancel console update	From Initial version to Target version.
Apple push certificate	Upload	Name of the certificate imported into the console
Settings - Remote control	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Network settings	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Indicators of attack (IOA)	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.

Item type	Action	Item
Settings - Per-computer settings	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Program blocking	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Workstations and servers	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Android devices	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - iOS devices	Create	Name of the settings profile the action was performed on.

Item type	Action	Item
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Personal data	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Cytomic Patch	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Endpoint Access Enforcement	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Cytomic Encryption	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.

Item type	Action	Item
	Delete	Name of the settings profile the action was performed on.
Settings - Vulnerability assessment	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Authorized software	Create	Name of the settings profile the action was performed on.
	Edit	Name of the settings profile the action was performed on.
	Delete	Name of the settings profile the action was performed on.
Settings - Trusted network	Edit	Name of the settings profile the action was performed on.
Device	Edit name	Name of the device the action was performed on.
Scheduled report	Create	Name of the scheduled report the action was performed on.
	Edit	Name of the scheduled report the action was performed on.
	Delete	Name of the scheduled report the action was performed on.
Computer	Delete	Name of the device the action was performed on.

Item type	Action	Item
	Edit name	Name of the device the action was performed on.
	Edit description	Name of the device the action was performed on.
	Change group	Name of the device the action was performed on.
	Remote control	Name of the device the action was performed on.
	Remote control attempt	Name of the device the action was performed on.
	Assign ‘Proxy and language’ settings	Name of the device the action was performed on.
	Inherit ‘Proxy and language’ settings	Name of the device the action was performed on.
	Assign 'Per-computer settings'	Name of the device the action was performed on.
	Inherit 'Per-computer settings'	Name of the device the action was performed on.
	Assign 'Workstations and servers' settings	Name of the device the action was performed on.
	Inherit 'Workstations and servers' settings	Name of the device the action was performed on.
	Assign 'Android devices' settings	Name of the device the action was performed on.
	Inherit 'Android devices' settings	Name of the device the action was performed on.

Item type	Action	Item
	Assign 'Sensitive information' settings	Name of the device the action was performed on.
	Inherit 'Sensitive information' settings	Name of the device the action was performed on.
	Assign license	Name of the device the action was performed on.
	Unassign license	Name of the device the action was performed on.
	Restart	Name of the device the action was performed on.
	Lock	Name of the device the action was performed on.
	Wipe data	Name of the device the action was performed on.
	Snap the thief	Name of the device the action was performed on.
	Remote alarm	Name of the device the action was performed on.
	Locate	Name of the device the action was performed on.
	Designate as Cytomic proxy	Name of the computer the action was performed on.
	Revoke Cytomic proxy role	Name of the computer the action was performed on.
	Designate as cache computer	Name of the computer the action was performed on.

Item type	Action	Item
	Configure cache computer	Name of the computer the action was performed on.
	Revoke cache computer role	Name of the computer the action was performed on.
	Designate as discovery computer	Name of the computer the action was performed on.
	Configure discovery	Name of the computer the action was performed on.
	Revoke discovery computer role	Name of the computer the action was performed on.
	Discover now	Name of the computer the action was performed on.
	Move to Active Directory path	Name of the computer the action was performed on.
	Enable Verbose mode	Name of the computer the action was performed on.
	Disable Verbose mode	Name of the computer the action was performed on.
	Isolate	Name of the device the action was performed on.
	Stop isolating	Name of the device the action was performed on.
	Uninstall	Name of the device the action was performed on.
	Reinstall agent	Name of the device the action was performed on.

Item type	Action	Item
	Reinstall protection	Name of the device the action was performed on
	End the "RDP attack containment" mode on the computer.	Name of the device the action was performed on.
Unmanaged computer	Hide	Name of the unmanaged computer the action was performed on.
	Make visible	Name of the unmanaged computer the action was performed on.
	Delete	Name of the unmanaged computer the action was performed on.
	Edit description	Name of the unmanaged computer the action was performed on.
	Install	Name of the unmanaged computer the action was performed on.
Filter	Create	Name of the filter the action was performed on.
	Edit	Name of the filter the action was performed on.
	Delete	Name of the filter the action was performed on.
Group	Create	Name of the group the action was performed on.

Item type	Action	Item
	Edit	Name of the group the action was performed on.
	Delete	Name of the group the action was performed on.
	Change parent group	Name of the group the action was performed on.
	Assign proxy and language settings	Name of the group the action was performed on.
	Inherit proxy and language settings	Name of the group the action was performed on.
	Assign 'Per-computer settings'	Name of the group the action was performed on.
	Inherit 'Per-computer settings'	Name of the group the action was performed on.
	Assign 'Workstations and servers' settings	Name of the group the action was performed on.
	Inherit 'Workstations and servers' settings	Name of the group the action was performed on.
	Assign 'Android devices' settings	Name of the group the action was performed on.
	Inherit 'Android devices' settings	Name of the group the action was performed on.
	Assign 'Sensitive information' settings	Name of the group the action was performed on.
	Inherit 'Sensitive information' settings	Name of the group the action was performed on.

Item type	Action	Item
	Sync group	Name of the group the action was performed on.
	Move computers to their Active Directory path	Name of the group the action was performed on.
Advanced reports	Access	
IOA	Archive for a computer	IOA name (Computer name).
	Mark as pending for a computer	IOA name (Computer name).
IOC	Create (via import)	Name of the IOC the action was performed on.
	Delete	Name of the IOC the action was performed on.
	Create (via wizard)	Name of the IOC the action was performed on.
	Edit	Name of the IOC the action was performed on.
List	Create	Name of the list the action was performed on.
	Edit	Name of the list the action was performed on.
	Delete	Name of the list the action was performed on.
Network Access Enforcement	Edit	Name of the settings profile the action was performed on.
Patch	Exclude for a specific computer	Name of the patch the action was performed on.

Item type	Action	Item
	Exclude for all computers	Name of the patch the action was performed on.
	Stop excluding for a specific computer	Name of the patch the action was performed on.
	Stop excluding for all computers	Name of the patch the action was performed on.
	Mark as 'Manually downloaded'	Name of the patch the action was performed on.
	Mark as 'Requires manual download'	Name of the patch the action was performed on.
Action to take when a threat is reclassified	Edit	
Email sending option	Edit	
Preference for automatic deletion of computers	Edit	
Preference for VDI environments	Edit	
Preference for risk assessment	Edit	
Preference for MDR	Edit	
Access permission for the Cytomic team	Edit	
Access permission for resellers	Edit	
Email sending option	Edit	

Item type	Action	Item
(reseller)		
Two-factor authentication selection	Edit	
Blocked program in the process of classification	Delete from list	Name of the blocked program the action was performed on.
	Allow	Name of the blocked program the action was performed on.
	Stop allowing	Name of the blocked program the action was performed on.
Role	Create	Name of the role the action was performed on.
	Edit	Name of the role the action was performed on.
	Delete	Name of the role the action was performed on.
Task - Security scan	Create	Name of the task the action was performed on.
	Edit	Name of the task the action was performed on.
	Delete	Name of the task the action was performed on.
	Cancel	Name of the task the action was performed on.
	Publish	Name of the task the action was performed on.

Item type	Action	Item
	Create and publish	Name of the task the action was performed on.
Task - IOC detection	Create	Name of the task the action was performed on.
	Edit	Name of the task the action was performed on.
	Delete	Name of the task the action was performed on.
	Cancel	Name of the task the action was performed on.
	Publish	Name of the task the action was performed on.
	Create and publish	Name of the task the action was performed on.
Task - Patch installation	Create	Name of the task the action was performed on.
	Edit	Name of the task the action was performed on.
	Delete	Name of the task the action was performed on.
	Cancel	Name of the task the action was performed on.
	Publish	Name of the task the action was performed on.
	Create and publish	Name of the task the action was performed on.

Item type	Action	Item
User	Create	Name of the user the action was performed on.
	Edit	Name of the user the action was performed on.
	Delete	Name of the user the action was performed on.
	Block	Name of the user the action was performed on.
	Unblock	Name of the user the action was performed on.
Task - Patch uninstallation	Create	Name of the task the action was performed on.
	Delete	Name of the task the action was performed on.
	Cancel	Name of the task the action was performed on.
	Publish	Name of the task the action was performed on.
	Create and publish	Name of the task the action was performed on.

Table 4.10: Item types and actions

Remote control events

When you select the **Remote control** action, the **Remote control session details** page opens with this information:

Field	Description
Date	Date and time the remote control event occurred.

Field	Description
Category	• **Files**: Operation related to the file transfer tool. • **Processes**: Operation related to the process manager. • **Services**: Operation related to the service manager. • **Terminal**: Operation related to the remote command-line tool. • **Connection**: Connection operation between the Advanced EPDR console and the target computer.
Action	Description of the category of the logged action. For the Terminal category, the commands you run remotely on the target computer are logged.

Table 4.11: Fields in the Remote Control Session Details list

System events

This section lists all events that occurred in Advanced EPDR and were not originated by a user account, but by the system itself as a response to the actions listed in **Item types and actions**.

Fields displayed in the System events list

Field	Description	Values
Date	Date and time the event took place.	Date
Event	Action taken by Advanced EPDR	See **Item types and actions**
Type	Type of object the action was performed on.	See **Item types and actions**
Item	Console object the action was performed on.	See **Item types and actions**

Table 4.12: Fields in the System events list

Fields displayed in the exported file

Field	Description	Values
Date	Date and time the event took place.	Date
Event	Action taken by Advanced EPDR	See **Item types and actions**
Type	Type of object the action was performed on.	See **Item types and actions**

Field	Description	Values
Item	Console object the action was performed on.	See **Item types and actions**

Table 4.13: Fields in the System events list

Filter tool

Field	Description	Values
From	Set the start point of the search range.	Date
To	Set the end point of the search range.	Date

Table 4.14: Fields in the System events list

Item types and actions

Item type	Action	Item
Non-persistent computer	Delete automatically	Name of the computer the action was performed on.
Computer	Register on server for the first time	Name of the computer the action was performed on.
	Register on server after computer deletion	Name of the computer the action was performed on.
	Register on server after agent reinstallation	Name of the computer the action was performed on.
	Uninstall agent	Name of the computer the action was performed on.
	Uninstall agent and delete automatically	Name of the computer the action was performed on.
	Delete automatically	Name of the computer the action was performed on.

Item type	Action	Item
Scheduled report	Disable automatically	Name of the scheduled report the action was performed on.

Table 4.15: Item types and actions

Chapter 5

Installing the client software

Installation of the security software involves a series of processes aimed at integrating software components into customers' devices in order to protect against computer threats. This involves the following stages:

- **Deployment**: Creation of the installation package with the components that make up the security solution and which is sent to devices on the network.
- **Installation**: The installation package is unzipped and the files that make up the security software are integrated into the device's operating system.
- **Configuration**: The security software installed on the device receives the required settings and begins to protect the device from the outset, without the need for user action.
- **Integration in the console**: The Advanced EPDR console displays the device to administrators, who can run any necessary actions on it.

Chapter contents

Installation on Windows systems

Protection deployment overview

The installation process consists of a series of steps that depend on the status of the network at the time of deployment and the number of computers and devices you want to protect:

- Find unprotected devices on the network.
- Verify minimum requirements for target devices.

- Uninstall competitor products and restart computers
- Determine device default settings.
- Select a deployment strategy.
- Check that the security software has been correctly installed.

Find unprotected devices on the network

- Find those computers on the network without protection installed or with a third-party security product that needs replacing or complementing with Advanced EPDR. On large networks, this task can be sped up using discovery features (see **Viewing discovered computers**).
- Verify that you have purchased enough licenses for the unprotected devices (see **Licenses** on page **189**).

Advanced EPDR enables you to install the software even when you do not have enough licenses for all the computers you want to protect. Computers without a license show in the management console with some information (such as installed software and hardware), but are not protected.

Verify minimum requirements for target computers

For more information about minimum requirements, see **Installation requirements**.

Uninstall competitor products and restart computers

*To create a security settings profile, see **Security settings for workstations and servers** on page **327**. To assign a settings profile to the computers on your network, see **Manual and automatic assignment of settings profiles** on page **296**.*

The Advanced EPDR protection services work without you having to restart your computers if you do not have any previously installed antivirus programs.

Some older versions of Citrix may require a computer restart or there may be a micro-interruption of the connection.

To install Advanced EPDR on a computer that already has a third-party security solution installed, choose between installing it without removing the previous protection or uninstalling it and working

exclusively with Advanced EPDR. Assign a **Workstations and servers** settings profile with the **Uninstall other security products** option enabled based on your needs (see **Uninstall other security products** on page **331**. While looking for updates, Advanced EPDR checks the assigned settings profiles once a day. For a list of the third-party security products that Advanced EPDR uninstalls automatically, see **https://www.pandasecurity.com/en/support/card?id=50021**.

When you uninstall a third-party antivirus product, you might have to restart the computer..

The default behavior varies depending on the Advanced EPDR version that you want to install:

Trial versions

By default, trial versions of Advanced EPDR can be installed without removing any other pre-existing third-party solution.

Commercial versions

By default, it is not possible to install a commercial version of Advanced EPDR on a computer with a solution from another vendor other than Cytomic. If there is an uninstaller available for the other vendor's product, it is uninstalled and Advanced EPDR is installed. Otherwise, the installation process stops.

This default behavior can be configured both for trial and commercial versions by assigning a **Workstations and servers** settings profile with the **Uninstall other security products** option disabled.

Determine device default settings

When the software is installed on the computer or device, Advanced EPDR assigns the **All** group security settings to it. However, during installation, you can select a different target group for the computer with the required settings. See **Managing settings** on page **287**.

If the network settings for the selected group differ from the settings specified during installation, the installation settings apply. See **Generating the installation package and manual deployment**.

Select a deployment strategy

The deployment strategy depends on the number of computers to protect, the workstations and servers with a Cytomic agent already installed, and the company network architecture. Several options are available:

- Manual deployment. See **Generating the installation package and manual deployment**.
- Centralized distribution tool. See **Installation from a gold image**.
- Remote deployment from the management console. See **Computer discovery and remote installation of the client software**.
- Installation using gold image generation. See **Installation from a gold image**.

Check that the security software has been correctly installed

- Select the **Computers** menu at the top of the console. Find the corresponding computer. For more information about how to find computers, see **Managing computers and devices** on page **211**.
- Click the computer on which the security software has been installed. The computer details page opens.
- Select the **Details** tab. All information collected from the computer is shown, along with the installation status.
- In the **Security** section, check the status of the various modules:
    - **Installing...**: The installation process is incomplete or there has been an error. Wait a few minutes.
    - **Enabled/Disabled:** After a few minutes, if the installation has been successful, the status of the protection modules is shown.

Detect and resolve installation errors

If, after a few minutes, the **Security** section disappears from the computer details page, it is because the security software did not install correctly. Verify this:

- If you installed the security software manually, make sure the user computer does not show any error messages.
- Verify whether the computer appears in lists. See **Checking deployment**.
- Check the Event Viewer on the user computer. See **Checking deployment**
- Verify the user computer meets the requirements specified in **Installation requirements** . Update the product or operating system version if required. See **Product updates and upgrades** on page **203**.

Installation requirements

Make sure the computer you want to install the security software on meets these system and network requirements.

From 30 September 2024, you will not be able to add devices to the management console or install the protection software on new computers that run these operating system versions: Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008 (Windows 2008 R2 will continue to be supported). Existing computers in the management console will continue to be protected. See ***https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.***

Supported operating systems

Advanced EPDR is compatible with 32- and 64-bit x86 microprocessors, as well as ARM microprocessors. For a complete list, see **Supported operating systems** on page **940**.

Advanced EPDR is compatible with Windows XP Embedded and higher. Embedded systems allow custom installations that could impact the way the security software and its modules work.

Hardware requirements

See **Hardware requirements** on page **942**.

Root certificates

It is necessary to keep the root certificates of workstations and servers up to date to use the Advanced EPDR Cytomic Patch module and to establish real-time communications with the management console. See **Root certificates** on page **942**.

SHA-256 compatibility

Workstations or servers must support SHA-256 signed drivers. For more information about affected operating systems and how to update them, see **Support for SHA-256 driver signing** on page **943**. To find computers that do not support SHA-256 driver signing, see **Filter computers not compatible with SHA-256 signed drivers** on page **221**.

Network requirements

Advanced EPDR requires access to multiple Internet-hosted resources. It requires access to ports 80 and 443.

The Advanced EPDR agent requires access to port 33000 for protected computers on the network to communicate with each other (see **Endpoint Access Enforcement settings** on page **518**) and with the Firebox or Access Point device (see **Network Access Enforcement** on page **318**

For a complete list of the URLs that Advanced EPDR requires access to, see **Local ports and URL access** on page **952**.

Time synchronization of computers (NTP)

Although not an essential requirement, we recommend that the clocks on computers protected by Advanced EPDR be synchronized. This synchronization is normally achieved using an NTP server. See **Time synchronization of computers (NTP)** on page **942**.

Internet Explorer 7

For advanced protection to operate correctly on a Windows XP or Windows 2003 computer, Internet Explorer 7 or higher must be previously installed on the computer.

You cannot install or upgrade the security software directly on Windows XP computers. You must use a computer with the cache role. For more information, see **Configuring downloads from cache computers** on page **315**

You can install or upgrade the security software on Windows 2003 computers only when the operating system is fully updated and all required patches are installed. Otherwise, you must use a computer with the cache role. For more information, see **Cytomic Patch (Updating vulnerable programs)** on page **435**.

Generating the installation package and manual deployment

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button in the upper-right corner of the page. A window opens with all platforms supported by Advanced EPDR.
- Click the Windows icon, both for devices with an x86 or ARM processor. The **Windows** window opens.

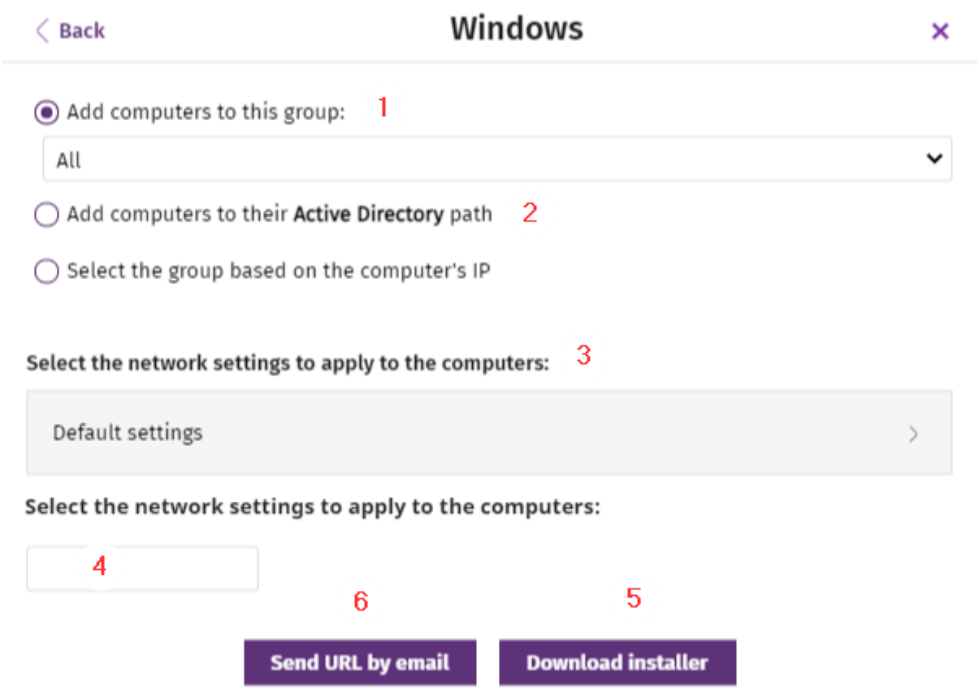


Figure 5.1: Configuring the download package

- Select the group that the computer integrates into in the folder tree (for more information about the different types of groups, see **Group types** on page **222**:
  - To integrate the computer into a native group, click **Add computers to this group (1)**. Select a destination in the folder tree displayed.
  - To integrate the computer into an Active Directory group, click **Add computers to their Active Directory path (2)**.

*The security policies assigned to a computer depend on the group it belongs to. If you have selected **Add computers to their Active Directory path**, and the administrator of the company's Active Directory moves a computer from one organizational unit to another, that change is replicated to the Advanced EPDR console as a group change. Consequently, the security policies assigned to that computer might also change without the administrator of the web management console noticing.*

- To integrate the computer into one group or another based on its IP address, click **Select the group based on the computer's IP (3)** and select the group into which it will be integrated depending on its IP address. See **Integrating computers based on their IP address**.

- To configure network settings that are different from those assigned to the group which the computer will join, click **Select the network settings to apply to the computers (4)** and choose a network settings profile from the drop-down menu: Initially, all the settings profiles that are applied to a computer upon integration into the console are the profiles that are assigned to the console group it belongs to. However, to avoid connectivity failures and prevent the computer from being inaccessible from the console because of incorrect network settings, you can set an alternative profile. For more information about how to create network settings profiles, see **Configuring the agent remotely** on page **307**.
    - **Native groups and IP groups**: The **Select the network settings to apply to the computers (4)** menu shows the network settings assigned to the group selected in **Add computers to this group (1)**.
    - **Active Directory groups**: The **Select the network settings to apply to the computers (4)** menu shows the network settings assigned to the Active Directory group selected in the group tree. If no Active Directory group was selected before clicking **Add computer**, you need to configure network settings.
- To prevent the installer from being used after a certain date, click the **Indicate whether you want the installer to expire after a specific date** text box and select a date in the calendar.
- To send the installer to the target user by email:
    - Click the **Send URL by email** button **(6)**. The email app installed by default on the administrator's computer opens with a predefined message containing the download URL.
    - Add recipients to the message and click **Send**.
    - The user that receives the message must click the URL from the target device to download the installer.

- To download the installation package and share it with the users on the network, click **Download installer (7)**.

Installing the downloaded package

- Double-click the package and follow the installation wizard. Throughout the process, a window is displayed indicating the progress of the task.
- If there are not enough licenses to allocate one to a computer in the installation process, a warning is displayed on screen. Nevertheless, the computer in question is integrated into the management console but is not protected until sufficient licenses are available.

After it is installed, the agent performs a series of checks automatically:

- **Agent integration into Cytomic**: The agent sends information from the computer where it is installed to the Cytomic cloud for integration into the platform.
- **Protection module installer download**: The agent downloads and installs the protection module.
- **Signature file download**: The agent downloads the known malware signature file.
- **Settings download**: The predetermined settings and those created by the administrator are downloaded and applied.
- **Connectivity check to the** Cytomic **cloud**: If connectivity fails, the error type is reported in the following places:
    - **The agent installation console**: An error message is displayed along with the URLs that could not be accessed. Click the **Retry** button to perform a new check.
    - **The Windows Event Viewer (Event Log)**: An error message is displayed along with the URLs that could not be accessed.
    - **The web console**: An error message is displayed along with the URLs that could not be accessed.

Integrating computers based on their IP address

Advanced EPDR enables IP address ranges and individual IP addresses to be assigned to groups. Computers with an IP address in the group's range are automatically included in it when installed. See **Creating and organizing groups** on page **224**.

The purpose of this feature is to save time for administrators by automatically organizing newly integrated computers into groups. Advanced EPDR takes the following steps to integrate a new computer into the service:

- If you select **Select the group based on the computer's IP**, Advanced EPDR searches all IPs associated with the group and child groups you select.

- If a single IP address is found, the computer moves to the relevant group.
- If multiple IP groups match the computer IP address, the group that is deepest in the tree is selected. If there are multiple groups at the same level with IP addresses that match the computer IP address, the last one is selected.
- If no matches are found, the computer moves to the selected group. If the selected group does not exist when the computer is integrated, it moves to the **All** group.

After the solution places a computer in a group, if you change the IP address for the computer, the computer does not automatically move to another group. If you change the IP addresses assigned to a group, the computers in the group are not automatically reorganized.

Installation with centralized tools

On medium-sized and large networks, we recommend that you use centralized tools to install the client software for Windows computers.

Using command line tools to install the installation package

You can automate the installation and integration of the the security software into the management console with these command-line parameters:

- **GROUPPATH="group1\group2"**: Path in the group tree where the computer will reside. The 'All' root node is not specified. If the group does not exist, the computer will be integrated into the 'All' root group.
- **PRX_SERVER**: Name or IP address of the corporate proxy server.
- **PRX_PORT**: Port of the corporate proxy server.
- **PRX_USER**: User of the corporate proxy server.
- **PRX_PASS**: Password of the corporate proxy server.

This example shows how to use command-line parameters to install the agent:

```
Msiexec /i "PandaAetherAgent.msi" GROUPPATH="London\AccountingDept"
PRX_SERVER="CorporateProxy" PRX_PORT="3128" PRX_USER="admin" PRX_
PASS="panda"
```

For a silent installation, you must add the `/qn` parameter:

```
Msiexec /i "PandaAetherAgent.msi" /qn
GROUPPATH="Madrid\Contabilidad" PRX_SERVER="ProxyCorporative" PRX_
PORT="3128" PRX_USER="admin" PRX_PASS="panda"
```

Deploying the agent from Panda Systems Management

- Panda Endpoint Protection on Aether Installer for Windows
- Panda Endpoint Protection on Aether Installer for macOS
- Panda Endpoint Protection on Aether Installer for Linux

- Panda Endpoint Protection on Aether Installer for Windows: 1.5 MB
- Panda Endpoint Protection on Aether Installer for macOS: 3 KB
- Panda Endpoint Protection on Aether Installer for Linux: 3 KB

Deploying the agent with Microsoft Active Directory

Limitations of Microsoft Active Directory when you deploy the security software

- This deployment method enables you to install the security software on a computer for the first time. Active Directory does not support updates of previously installed software.
- The computer where you define the GPO (Group Policy Object) cannot have the security software installed Otherwise, this error message displays: "The process of adding failed. The deployment information could not be retrieved from the package. Make sure the package is correct".

To prepare the installation GPO (Group Policy Object)

1. Download the Advanced EPDR package and share the installer on the network.
    - Save the Advanced EPDR installer file to a shared folder accessible to all the computers that are to receive the software.
2. Create a new OU (Organizational Unit) called "Cytomic deployment".
    - Open the `mmc`. Add the Group Policy Management snap-in.
    - Right- click the domain node. Select **New** and **Organizational Unit**. Create an Organizational Unit called "Cytomic deployment".
    - Right-click the new Organizational Unit and select **Block Inheritance**.

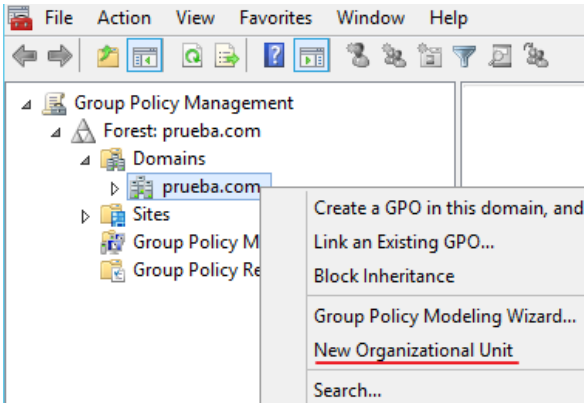


Figure 5.2: New Organizational Unit

3. Create a new GPO with the installation package.

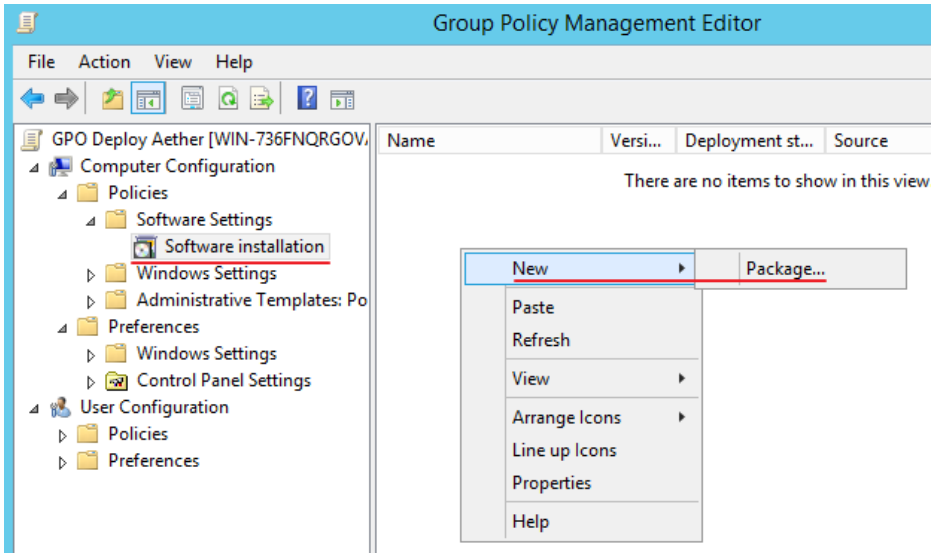


Figure 5.3: New installation package

- Right-click the new Organizational Unit. Select **Create a GPO**. Name the GPO (for example, "Cytomic deployment GPO").
- Edit the new GPO and add the installation package that contains the Advanced EPDR software**.** Click **Computer configuration, Policies, Software Settings, Software installation.**
    - Right-click **Software installation**, and select **New**, **Package**.
    - Add the Advanced EPDR `.msi` installation package.

4. Edit the package properties

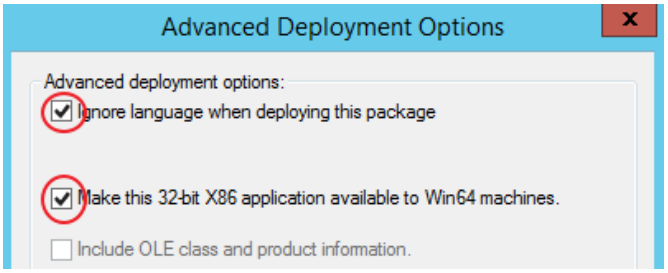


Figure 5.4: Configuring the deployment options

- Right-click the package you added, and select **Properties**, **Deployment** tab, **Advanced**. Select the **Ignore Language when Deploying this Package** and **Make this 32-bit X86 Application Available to Win64 Machines** checkboxes.
- Add all network computers that will receive the agent to the "Cytomic deployment" Organizational Unit.

Installation from a gold image

> *Be sure to follow the steps in this section closely to generate and deploy Windows images with Advanced EPDR installed. If you do not follow the procedure exactly as specified, the management and protection capabilities of your product will be reduced, and it will no longer monitor the actions taken by processes on cloned computers.*

In large networks with many similar computers, you can automate the process to install the operating system and other software with a gold image. This is sometimes referred to as a master image, base image, or clone image. You then deploy the gold image to all computers on the network, which eliminates most of the manual work required to set up a new computer.

To generate a gold image, install an up-to-date operating system with all the software that users might need, such as security tools, on a computer on your network. When that computer is ready, you must use a virtualization software to 'seal' or 'close' the installation and deploy it to the computers on your network. For specific information about your virtualization solution, see the vendor documentation.

Supported virtual platforms

- VMware Workstation
- VMware Server
- VMware ESX
- VMware ESXi

- Citrix XenDesktop
- XenApp
- XenServer
- MS Virtual Desktop
- MS Virtual Servers

Basic concepts and required tools

ID of VDI computers

Advanced EPDR generates a unique ID in the installation process. The solution uses this ID to identify each computer in the management console.

If you install Advanced EPDR once on the gold image you later copy to the computers on your network, instead of installing it individually on each computer, all cloned computers will inherit the same ID.

Having multiple computers with the same ID leads to the following negative consequences:

- Management capabilities are reduced: The management console shows only one computer, usually the first computer that was added to it. All other cloned computers cannot be accessed from the Advanced EPDR console.
- The protection capabilities of the security software are reduced.
- The security software stops monitoring the actions taken by processes.

To avoid having multiple computers with the same ID, you must follow a very strict protocol to generate a gold image with no ID. This protocol includes:

- Deleting the ID from the gold image
- Disabling the protection service

Deleting the ID from the gold image

Download the `Endpoint Agent Tool` free tool from the Cytomic support page (password `panda`):

https://www.pandasecurity.com/resources/tools/endpointagenttool.zip

Disabling the protection service

Many virtualization solutions transparently start the newly created gold image as part of the preparation and deployment process. This causes Advanced EPDR to start. When the security software detects that its ID has been deleted, it generates a new ID, rendering the image unusable. To avoid this, you must disable the protection service before you close the gold image, and schedule it to be launched when the cloned computers are started.

There are multiple ways to do this: The most popular method, which we explain in this section, is through a GPO if the computer belongs to a Windows domain. If that is not the case, there are other alternative solutions:

- Some virtualization solutions incorporate this type of tool. For example, VMware Horizon.
- RMM solutions such as Panda Systems Management.
- Tools such as PDQ Deploy, Sysinternals PsExec, Microsoft PowerShell, or scripts that use WMI, among others.

Enabling and disabling Advanced EPDR updates

In non-persistent environments, where the storage system of cloned computers is emptied from time to time, it is important to prevent protection software updates. This can be done when you maintain the gold image, to reduce the bandwidth usage generated by cloned computers and excessive CPU usage on the host system.

To follow the procedures that enable you to successfully generate a gold image, you must assign settings profiles that enable/disable Advanced EPDR updates to the computer you want to clone.

- To enable or disable agent updates, see **Communications agent updates** on page **206**.
- To enable or disable protection updates, see **Protection engine updates** on page **204**.
- To assign settings profiles to computers, see **Managing settings** on page **287**.
- For more information about groups in Advanced EPDR, see **Group tree** on page **222**

Because in some scenarios you must switch between one set of settings profiles and another, we recommend that you create two computer groups in the management console: one with settings profiles that enable Advanced EPDR updates and one with settings profiles that disable them. This way, to enable or disable the updates, you only have to move the computer that has the gold image from one group to another in the console.

Additionally, every time you make changes to a settings profile in the Advanced EPDR console, we recommend that you follow this procedure to make sure that the computer used to generate the gold image receives the new settings:

- Move the computer to the relevant group so that it inherits the new settings.
- In the notification area of the Windows taskbar, right-click the Advanced EPDR icon. A drop-down menu appears.
- Select **Synchronize**. This downloads the new security settings from the server to the target computer.

Creating and deploying a gold image in persistent VDI environments

Steps to take on the computer where the gold image is generated

- Install an updated version of the operating system and all programs that users might need.
- Make sure the computer is connected to the Internet and the MAC address of the computer's network card is static.

- Install Advanced EPDR on a group with updates enabled by following the steps described in **Generating the installation package and manual deployment**.
- Open the `Endpoint Agent Tool`. Select the checkboxes for **Detections**, **Counters**, and **Check commands**. Click the **Send** button.
- Make sure the **Is a Gold Image** option is not selected.
- If the device is protected by the **anti-tamper protection**, enter the password.
- Click **Prepare image**.
- **Disable the Panda Endpoint Agent service**.
- Turn off the computer and generate the gold image with your virtual environment management software.

Steps to take to enable the protection service

Follow this procedure to enable the Panda Endpoint Agent service on computers cloned through a GPO:

- In the GPO settings, browse to **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **System Services**, **Panda Endpoint Agent**.
- The service appears as **Disabled**. Change it to **Automatic**.

For more information about GPOs, see ***https://www.microsoft.com/en-us/download/details.aspx?id=21895*** .

Creating, deploying, and maintaining a gold image for non-persistent VDI environments

Steps to take on the computer where the gold image is generated

- Install an updated version of the operating system and all programs that users might need.
- Make sure the computer is connected to the Internet.
- Install Advanced EPDR on a group with updates disabled by following the steps described in **Generating the installation package and manual deployment**.
- Move the computer to a group that has updates enabled.
- If the persistence of the cloned computers is set to be less than one week, it is recommended (although not strictly necessary) to preload the Advanced EPDR caches. Follow one of these two procedures:
    - Open the `Endpoint Agent Tool`. Click the **Start cache scan** button and wait for the process to complete.

Or

- Right-click the Advanced EPDR icon on the Windows taskbar.
- Click **Antivirus and advanced protection**.
- Click the **Scan now** button and wait for the process to complete.

- Open the `Endpoint Agent Tool`. Select the checkboxes for **Detections**, **Counters**, and **Check commands**. Click the **Send** button.
- Make sure the **Is a gold image** checkbox is selected.
- If the device is protected by the **anti-tamper protection**, enter the password.
- Click **Prepare image**.
- **Disable the Panda Endpoint Agent service**.
- Turn off the computer and generate the gold image with your virtual environment management software.

Steps to take in the Advanced EPDR management console

- Click **Settings** in the top menu. Click **VDI environments** from the side panel.
- Configure the maximum number of non-persistent VDI computers that can be active simultaneously.

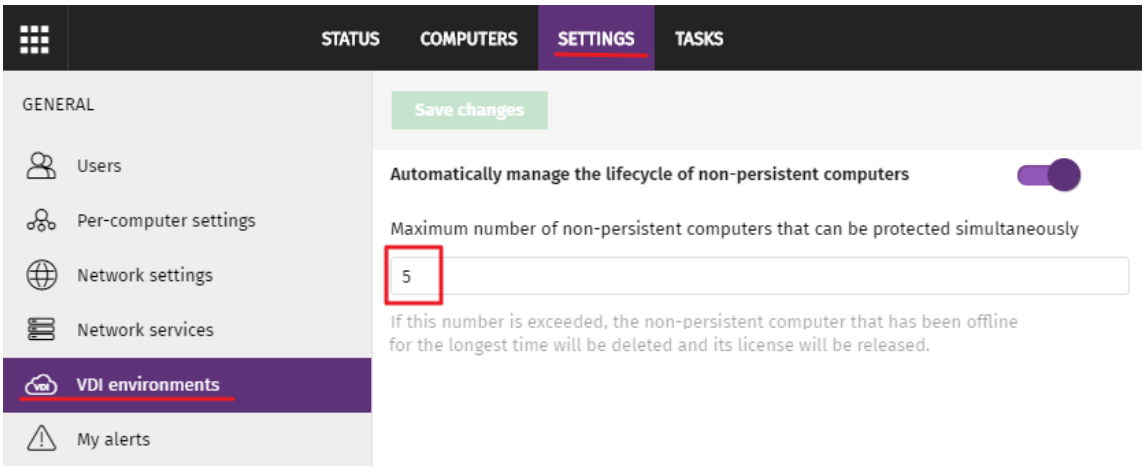


Figure 5.5: Configuring the number of licenses assigned to non-persistent VDI computers

Steps to take to enable the protection service

Follow this procedure to enable the Panda Endpoint Agent service on computers cloned through a GPO:

- In the GPO settings, browse to **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **System Services**, **Panda Endpoint Agent**.
- The service appears as **Disabled**. Change it to **Automatic**.

For more information about GPOs, see ***https://www.microsoft.com/en-us/download/details.aspx?id=21895*** .

Maintaining the gold image in a non-persistent VDI environment

Because the security settings that VDI computers receive have updates disabled, we recommend that you update the gold image manually at least once a month. This makes sure that the VDI computers receive the latest version of the protection and the signature file. To manually update the gold image in a non-persistent VDI environment:

- Make sure the computer is connected to the Internet.
- Move the computer to a group that has updates enabled.
- Updates are performed silently in the background. We recommend you wait a few minutes to make sure the image is properly updated. If a new version of the protection is available, a restart window is displayed and the computer restarts automatically. When the restart is complete, we recommend you force a new synchronization to make sure Advanced EPDR is fully up to date.
- Preload the Advanced EPDR caches. Follow one of these two procedures:
    - Open the `Endpoint Agent Tool`. Click the **Start cache scan** button and wait for the process to complete.

      Or

    - Right-click the Advanced EPDR icon on the Windows taskbar.
    - Click **Antivirus and advanced protection**.
    - Click the **Scan now** button and wait for the process to complete.
- Open the `Endpoint Agent Tool`. Select the checkboxes for **Detections**, **Counters**, and **Check commands**. Click the **Send** button.
- Make sure the **Is a gold image** checkbox is selected.
- If the device is protected by the **anti-tamper protection**, enter the password.
- Click **Prepare image**.
- Turn off the computer and generate the gold image with your virtual environment management software.
- In the VDI environment, replace the previous image with the new one.
- Repeat this maintenance process at least once per month.

Verifying that all computers are cloned correctly

There is not a single way to verify that computers are cloned correctly in all possible scenarios. The following is a minimum checklist of items to check.

Show persistent and non-persistent VDI computers

The presence of a number of VDI computers in the Advanced EPDR management console lower than the number of VDI computers actually installed on the IT network is a symptom of not having followed the procedure to generate gold images correctly. This can severely affect the management and protection capabilities of your security product.

To view a list of non-persistent VDI computers:

- Go to the **Settings** menu at the top of the console. Click **VDI environments** from the left panel. Click the **Show non-persistent computers** link.
- The **Computers** list shows only non-persistent computers.

To view a list of persistent VDI computers:

- Select the **Computers** menu at the top of the console. Click the folder icon  in the left panel. The filter tree appears.
- Click the **All** root node. The right panel shows all computers added to the Advanced EPDR console.
- Verify that all persistent computers are included in the list.

Verify the status of Advanced EPDR updates on cloned computers

- Select the **Computers** menu at the top of the console. Click the folder icon  in the left panel. The filter tree appears.
- Find persistent and non-persistent computers in the right panel.
- Click the name of each cloned computer. A page opens that shows the computer details.
- Select the **Settings** tab. A page opens that shows the settings profiles assigned to the computer.
- Verify the **Per-computer settings** and **Security for workstations and servers** profiles have the correct values:
    - For persistent computers, updates must be enabled.
    - For non-persistent computers, updates must be disabled.

Computer discovery and remote installation of the client software

All products based on Cytomic Platform include tools to find unprotected Windows workstations and servers on the network and to open a remote installation session from the management console.

To remotely install the protection software on a computer using the management console, follow these steps:

- Designate one or more computers on the network as discovery computers. See **Designating a discovery computer**.
- Make sure the computers on the network meet the minimum requirements. See **Operating system and network requirements**.
- Start the remote installation of the security software. See **Remote installation of the client software**.

Discovery computers find computers on the network that the security software does not manage. All computers that meet the necessary requirements appear in the **Unmanaged computers discovered** list, regardless of whether their operating system or device type supports the installation of Advanced EPDR.

The first Windows computer that you add to Advanced EPDR is automatically designated as the discovery computer.

The discovery computer can use one or the two available discovery methods at the same time: discovery using network scanning or discovery using Active Directory. See **Using the network to discover computers** **Using Active Directory to discover computers** and **Designating a discovery computer**.

Designating a discovery computer

- Make sure the computer that you want to designate as a discovery computer has Advanced EPDR installed.
- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab.
- Click the **Add discovery computer** button. From the list, select the computer or computers that you want to perform discovery tasks across the network.

After you have designated a computer as a discovery computer, it is displayed on the list of discovery computers (top menu **Settings**, side menu **Network services**, **Discovery** tab). The following information is displayed for each discovery computer:

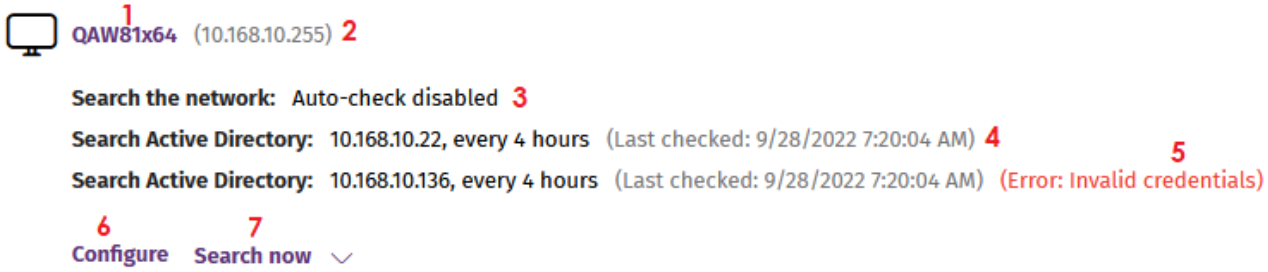


Figure 5.6: Discovery computer information

Field	Description
Computer name (1)	Name of the discovery computer.
IP address (2)	IP address of the discovery computer.
Discovery task settings (3)	Description of the settings of the automatic tasks defined for the discovery computer.
Last checked (4)	Time and date when the discovery task was last launched.
Error codes (5)	• "The computer is turned off or offline": The discovery computer cannot be accessed by the Advanced EPDR server. • Error: Wrong credentials. • Error: Active Directory server not found. • Error (<error code>): If the error is an unknown error.
Configure (6)	Set the discovery task scope and type (automatic or manual). If the task is automatic, it is performed once a day. See **Designating a discovery computer**.
Search now (7)	Launch the search task manually. See **Discovering computers on demand**.

Table 5.1: Information displayed for each discovery computer

Using the network to discover computers

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab. Select the discovery computer that you want to configure. Click the **Configure** link. The **Configure discovery on <computer name>** page opens.
- To enable discovery, click the **Discover computers on the network** toggle.
- In the **Discovery scope** section, select an option to limit the scope of the computer search:
    - **Search across the entire network**: The discovery computer uses the network mask configured on the interface to scan its subnet for unmanaged computers. The search is performed only on private IP address ranges.
    - **Search only in the following IP address ranges**: Enter an IP address or IP address range, separated by commas. The IP address ranges must have a "-" (dash or hyphen) in the middle. You can only specify private IP address ranges.
    - **Search for computers in the following domains**: Enter the Windows domains for the discovery computer to search, separated by commas.

The scope settings affect only the subnet where the discovery computer resides. To search for unmanaged devices across all subnets on the network, add at least one discovery computer from each subnet.

Using Active Directory to discover computers

The discovery computer connects to the company's Active Directory to search for computers on the network. Each discovery computer can connect to a maximum of three servers to launch queries against directories.

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab. Select the discovery computer whose scope you want to configure. Click the **Configure** link. The **Configure discovery** page opens.
- To enable discovery, click the **Discover computers in Active Directory** toggle.
- Click the **Add Active Directory server** link. The **Add Active Directory server** window opens.
- Enter the name or IP address (mandatory field) of the server you want to search. Enter the server credentials if required (optional field).
- Click **Save**. The discovery computer asks Active Directory for computers on the network every four hours.

Scheduling computer discovery tasks

You can configure the discovery computer to run discovery tasks at regular intervals.

Network discovery

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab. In the list of computers, next to the discovery computer you want to configure, click **Configure**.
- From the **Run automatically** drop-down menu, select **Every day**.
- Select the time of day when the search runs.
- To specify the time based on the time on the discovery computer, select the **Computer's local time** checkbox. If you do not select this checkbox, the time is based on the Advanced EPDR server time.
- Click **Save**. The discovery computer shows a summary of the scheduled task in its description.

Discovery using Active Directory

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab. Select the computer that you want to configure. Click the **Configure** link. The **Configure discovery** page opens.
- Click the Active Directory you want to configure. The **Edit Active Directory server** window opens.
- From the **Recurrence** drop-down menu, select how often searches are run (hours).

Discovering computers on demand

To discover computers on demand, the discovery computer must be up and running and connected to the Advanced EPDR server.

- Select the **Settings** menu at the top of the console. Select **Network services** from the side menu. Select the **Discovery** tab.
- Click the **Check now** link next to your chosen discovery computer. If the discovery computer has only one discovery method configured, the **Search for unmanaged computers in progress** message appears and the discovery task is launched in the background.
- If the discovery computer has multiple discovery methods configured, a context menu appears when you click the **Check now** link.
    - **Search everywhere**: The discovery computer scans the network and all configured Active Directory servers.
    - **Search the network**: The discovery computer scans the network.
    - **Search <server_name>**: The discovery computer searches only the selected server.

Viewing discovered computers

Computers discovered using network scanning or Active Directory are shown in the **Unmanaged computers discovered** list.

For more information about computer discovery methods, see ***Using the network to discover computers*** *and* ***Using Active Directory to discover computers****.*

There are two ways to access the **Unmanaged computers discovered** list:

- **Protection status widget**: Go to the **Status** menu at the top of the console. Go to the Advanced EPDR dashboard that contains the **Protection status** widget. At the bottom of the widget, find the following text: **xx computers have been discovered that are not being managed by Advanced EPDR**. Click the link to open the **Unmanaged computers discovered** list.
- Go to **My lists** in the side menu. Click the **Add** link. A window opens. Select the **Unmanaged computers discovered** list.

Unmanaged computers discovered list

This list shows all computers on the network that do not have Advanced EPDR installed, and those computers where the protection is not working properly, despite being correctly installed.

Field	Description	Values
Computer	Name of the discovered computer.	Character string
Status	Indicates the computer status with regard to the installation process.	— **Unmanaged**: The computer is eligible for installation, but the installation process has not started yet. **Installing**: The installation process is in progress. **Installation error**: A message specifying the type of error. For a description of error messages, see **Computer notifications section (2)** on page **256**. With errors whose origin is unknown, the associated error code will be displayed.
IP address	The computer's primary IP address.	Character string
NIC manufacturer	Manufacturer of the discovery computer	Character string

Field	Description	Values
	network interface card.	
Active Directory path	Active Directory path where the computer was last discovered.	Character string
Last discovery computer	Name of the discovery computer that last found the unmanaged workstation or server.	Character string
Last seen	Date when the computer was last discovered.	Date

Table 5.2: Fields in the Unmanaged computers discovered list

If the **Status** field shows the text **Installation error** and the origin of the error is known, a text string is added with a description of the error. For a list of the installation errors reported by Advanced EPDR, see **Computer notifications section (2)** on page **256**.

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Name	Name of the discovered computer.	Character string
IP	The computer's primary IP address.	Character string

Field	Description	Values
MAC address	The computer's physical address.	Character string
NIC manufacturer	Manufacturer of the discovery computer network interface card.	Character string
Domain	Windows domain the computer belongs to.	Character string
Active Directory	Active Directory path where the computer was last discovered.	Character string
First seen	Date when the computer was first discovered.	Character string
First seen by	Name of the discovery computer that first found the user computer.	Character string
Last seen	Date when the computer was last discovered.	Date
Last seen by	Name of the discovery computer that last found the user computer.	Character string
Description	Description of the discovered computer.	Character string
Status	Indicates the	• **Unmanaged**: The computer is eligible for

Field	Description	Values
	computer status with regard to the installation process.	installation, but the installation process has not started yet. • **Installing**: The installation process is in progress. • **Installation error**: A message specifying the type of error. For a description of error messages, see **Computer notifications section (2)** on page **256**.
Error	Error description.	For more information, see **Computer notifications section (2)** on page **256** .
Installation error date	Date and time when the error occurred.	Date

Table 5.3: Fields in the Unmanaged computers discovered list exported file

Filter tool

Field	Description	Values
Search	Search by computer name, IP address, NIC manufacturer, or discovery computer.	Character string
Status	Advanced EPDR installation status.	• **Unmanaged**: The computer is eligible for installation, but the installation process has not started yet. • **Installing**: The installation process is in progress. • **Installation error**: A message specifying the type of error.
Last seen	Date when the computer was last discovered.	• Last 24 hours • Last 7 days • Last month
Discovery	Method used to discover the	• All

Field	Description	Values
method	computer	• Network scanning. See **Computer discovery and remote installation of the client software** • Active Directory. See **Computer discovery and remote installation of the client software**

Table 5.4: Filters available in the Unmanaged computers discovered list

Computer details page

Click any of the rows in the list to open the computer details page.

Discovered computer details

In the **Unmanaged computers discovered** list, click a computer to view its details page. This page is divided into three sections:

- **Computer alerts (1)**: Includes information on alerts or notifications to help you identify installation problems.
- **Computer details (2)**: Gives a summary of the computer's hardware, software, and security settings.
- **Last discovery computer (3)**: Shows the discovery computer that last found the computer.

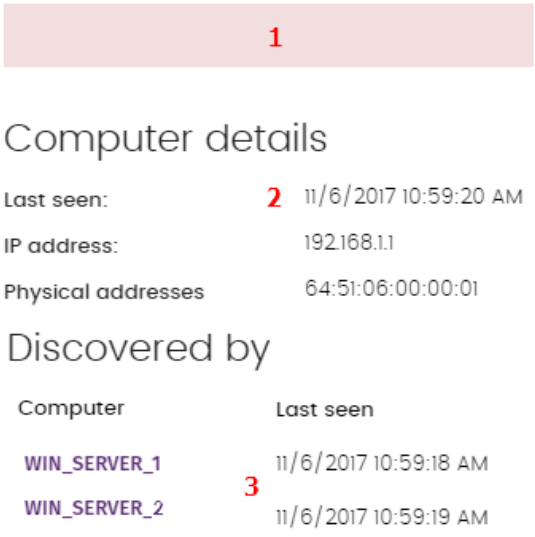


Figure 5.7: Discovered computer details

Computer alerts (1)

Status	Type	Recommended action
Error installing the Cytomic agent	This message specifies the reason why the agent installation failed.	
	Wrong credentials	Start the installer again with the required credentials to perform the installation.
	Unable to connect to the computer	Make sure the computer is turned on and meets the remote installation requirements.
	Unable to download the agent installer	Make sure the computer is turned on and meets the remote installation requirements.
	Unable to copy the agent installer	Make sure the computer is turned on and meets the remote installation requirements.
	Unable to install the agent	Make sure the computer is turned on and meets the remote installation requirements.
	Unable to register the agent	Make sure the computer is turned on and meets the remote installation requirements.

Status	Type	Recommended action
Error installing the Advanced EPDR protection	This message indicates the reason for the protection installation failure.	
	Insufficient disk space to perform the installation	To see the free space required for installing Advanced EPDR, see **Hardware requirements** on page **942**.
	Windows Installer is not operational	Make sure the Windows Installer service is active. Stop and start the service.
	Removal of the third-party protection installed was canceled by the user	Accept the removal of the third-party antivirus solution found.
	Another installation is in progress	Wait for the current installation to finish.
	Error automatically uninstalling the third-party protection installed	For a list of the third-party solutions that Cytomic can uninstall, see **Supported uninstallers**.
	There is no uninstaller available to remove the third-party protection installed	Contact technical support to obtain the relevant uninstaller.
Installing the Cytomic agent	When the installation process is complete, the computer will no longer appear on the list of unmanaged computers discovered.	
Unmanaged computer	The computer does not have the Cytomic agent installed. Make sure the computer is compatible with Advanced EPDR and meets the requirements specified in **Product features and requirements** on page **932**	

Table 5.5: Computer alerts

Computer details (2)

Field	Description
Computer name	Name of the discovered computer.
Description	Enter a description for the unmanaged computer.
First seen	Date and time when the computer was first discovered.
Last seen	Date and time when the computer was last discovered.
Active Directory path	If the unmanaged computer was discovered using Active Directory, this field indicates the path where it was discovered.
IP address	IP address of the computer network interface card.
Physical addresses (MAC)	Physical address of the computer network interface card.
Domain	Windows domain the computer belongs to.
NIC manufacturer	Manufacturer of the computer network interface card.

Table 5.6: Discovered computer details

Last discovery computer (3)

Field	Description
Computer	Name of the discovery computer that last found the unmanaged computer.
Last seen	Date and time when the computer was last discovered.
Discovery method	Indicates whether the computer was discovered through Active Directory or network scanning.

Table 5.7: Last discovery computer

Deleting and hiding computers

Deleting computers

Advanced EPDR does not automatically delete from the **Unmanaged computers discovered** list computers that are no longer accessible because they were removed from the network (due to theft, failure, or for other reasons).

To manually delete those computers that are no longer accessible:

- In the **Unmanaged computers discovered** list, click **Discovered** or **Hidden** in the upper-right corner of the page.
- Select the computers you want to remove.
    - To delete multiple computers simultaneously, select the computers. Select **Delete** from the general context menu above the table.
    - To delete a single computer, click the computer's context menu. Select **Delete**.

Any computer you delete from the console without uninstalling the Advanced EPDR software or removing it physically from the network will reappear in the next discovery task. Delete only those computers that you are sure will never be accessible again.

Hiding computers from installation

To minimize long lists of discovered computers that contain devices not eligible for Advanced EPDR, you can hide computers from the installation:

- In the **Unmanaged computers discovered** list, click **Discovered** in the upper-right corner of the page.
- Select the computers you want to hide.
- To hide multiple computers simultaneously, select the computers. Select **Hide and do not discover again** from the general context menu above the table.
- To hide a single computer, click the computer's context menu. Select **Hide and do not discover again**.

Remote installation of the client software

You can remotely install the security software on any unprotected computer discovered. To do that, you must have a discovery computer set up that can connect to the computer you want to install the software on.

Remote installation is only compatible with Windows platforms.

Operating system and network requirements

To install Advanced EPDR remotely, make sure the target computers meet these requirements:

- UDP ports 21226 and 137 must be open for the `system` process.
- TCP port 445 must be open for the `system` process.
- NetBIOS over TCP must be enabled.
- DNS resolution must be enabled.
- Access to the `Admin$` administrative share must be allowed. You must explicitly enable this feature on Windows Home editions.
- You must have domain administrator credentials or credentials for the local administrator account created by default when the operating system was installed.
- Windows Remote Management must be enabled.

*To meet these requirements quickly without needing to manually add rules to the Windows firewall, turn on network discovery and file and printer sharing. In **Control Panel** > **Network and Sharing Center** > **Advanced Sharing Settings**, select **Turn on network discovery** and **Turn on file and printer sharing**.*

- Additionally, for a network computer with Advanced EPDR installed to find unmanaged computers on the network, the computers must:
    - Not be hidden by the administrator.
    - Not be currently managed by Advanced EPDR on Cytomic Platform.
    - Be located on the same subnet segment as the discovery computer.

Remote installation from the Unmanaged computers discovered list

- Go to the **Unmanaged computers discovered** list.
    - Go to the **My lists** section in the left menu. Click the **Add** link. From the window displayed, select the **Unmanaged computers discovered** list.
    - Go to the **Status** menu at the top of the console. In the **Protection status** widget, click the **xx computers have been discovered that are not being managed by Advanced EPDR** link.

- Go to the **Computers** menu at the top of the console. Click **Add computers**. Select **Discovery and remote installation**. A wizard opens. Click the **View unmanaged computers discovered** link.

- In the **Unmanaged computers discovered** list, click **Discovered** or **Hidden**, based on the status of the relevant computers.
- Select the computer you want to install the software on.
    - To install the software on multiple computers simultaneously, select the checkboxes to the left of each computer, then select **Install Cytomic agent** from the general context menu.
    - To install the software on a single computer, click the computer's context menu, then click **Install Cytomic agent**.
- Configure the installation by following the steps described in **Generating the installation package and manual deployment**.
- Enter one or multiple installation credentials. Use the local administrator credentials for the target computer(s) or domain administrator credentials.

Remote installation from the computer details page

Select a discovered computer. The computer details page opens. Click **Install Cytomic agent**. Follow the steps described in **Generating the installation package and manual deployment**.

Differences in the installation process based on the discovery method used

The procedure to install the protection on selected computers varies based on the method used to discover them.

Installing the protection on computers discovered using network scanning

When a discovery computer discovers another computer using network scanning, it is always connected to the discovered computer. No additional configuration is required beyond what is described in **Generating the installation package and manual deployment**.

- **If all computers are discovered by the same discovery computer**: The discovery computer launches the installation process on all discovered computers.
- **If NOT all computers are discovered by the same discovery computer**: Each discovery computer launches the installation process on the computers it discovered.

Installing the protection on computers discovered using Active Directory

The fact that a discovery computer discovers another computer by searching in Active Directory does not necessarily mean that it is connected to the discovered computer. In such a case, to remotely install the security software, you must select the discovery computer that will connect to the discovered computer to perform the installation.

- If all selected computers were discovered only through Active Directory, you must select the installer computers that will launch the installation process on the selected computers.
- If the selected computers include computers that were discovered using both methods, you must select the discovery computer that will launch the installation on the selected computers that were discovered only through Active Directory. For all other computers, install the protection as usual by following the steps in **Generating the installation package and manual deployment**.

Possible installation errors

If the installer computer cannot successfully connect to the discovered computer, the following installation errors are shown:

- In the unmanaged computers discovered list: **Error installing. Unable to connect to the computer.** See **Viewing discovered computers**.
- On the **Computer details** on page **252** page: **Error installing the Cytomic agent**. **Make sure the computer is turned on and meets the remote installation requirements**. See **Computer discovery and remote installation of the client software**.

Installation on Linux systems

Protection deployment overview

The installation process consists of a series of steps that depend on the status of the network at the time of deploying the software and the number of computers to protect:

- Find unprotected computers on the network
- Verify minimum requirements for target computers
- Uninstall competitor products and restart computers
- Determine computer default settings
- Select an installation method
- Verify the security software has been correctly installed.

Find unprotected computers on the network

Find computers on the network without protection installed or with a third-party security product that needs replacing or complementing with Advanced EPDR. Verify that you have purchased enough licenses for the unprotected computers. See **Licenses** on page **189**.

Advanced EPDR enables you to install the software even when you do not have enough licenses for all the computers you want to protect. Computers without a license show in the management console with some information (such as installed software and hardware), but are not protected.

Verify minimum requirements for target computers

For more information about minimum requirements, see **Installation requirements**.

Uninstall competitor products

We recommend that you uninstall any third-party antivirus and security software prior to installing Advanced EPDR.

Determine computer default settings

When the software is installed on the computer or device, Advanced EPDR assigns the **All** group security settings to it. However, during installation, you can select a different target group for the computer with the required settings. See **Managing settings** on page **287**.

Verify the security software has been correctly installed

- Select **Computers** from the top menu. Find the corresponding computer. For more information about how to find computers, see **Managing computers and devices** on page **211**.
- Select the computer on which the security software has been installed. The computer details page opens.
- Select the **Details** tab. All information collected from the computer is shown, along with the installation status.
- In the **Security** section, verify the status of the various modules:
    - **Installing...**: The installation process is incomplete or there has been an error. Wait a few minutes.
    - **Enabled/Disabled:** After a few minutes, if the installation has been successful, the status of the protection modules is shown.

Detect and resolve installation errors

If, after a few minutes, the **Security** section disappears from the computer details page, it is because the security software did not install correctly. Verify this:

- If the computer has a graphical user interface installed, verify whether there any error messages.
- Verify whether the computer appears in lists. See **Checking deployment**.

- Verify whether the user computer meets the requirements specified in **Installation requirements** . Update the product or operating system version if required. See **Product updates and upgrades** on page **203**.

Installation requirements

Make sure the computer you want to install the security software on meets these system and network requirements.

Supported operating systems

See **Supported distributions** on page **947**.

Supported kernels

For more information about the supported Linux kernel versions for each distribution, see **https://info.cytomicmodel.com/resources/help/EPDR/v16/en/Content/28_ hardware_ software_ network_requirements/linux_kernels.htm**.

Hardware requirements

See **Hardware requirements** on page **948**.

Network requirements

Ports 3127, 3128, 3129, and 8310 must be accessible for web filtering and malware web detection to work. On computers with no graphical environment, web filtering and web detection are disabled.

Advanced EPDR requires access to multiple Internet-hosted resources. It requires access to ports 80 and 443.

The Advanced EPDR agent requires access to port 33000 for protected computers on the network to communicate with each other (see **Endpoint Access Enforcement settings** on page **518**) and with the Firebox or Access Point devices (see **Network Access Enforcement** on page **318**

For a complete list of the URLs that Advanced EPDR requires access to, see **Local ports and URL access** on page **952**.

Time synchronization of computers (NTP)

Although not an essential requirement, we recommend that the clocks on computers protected by Advanced EPDR be synchronized. This synchronization is normally achieved using an NTP server. See **Time synchronization of computers (NTP)** on page **942**.

Access to the distribution repository

The security software installation process requires access to the repositories that contain the installation packages. These repositories are the responsibility of the distribution vendor who maintains at least one repository for each published version. When a version reaches end-of-life (EOL), the vendor deletes the repository which can cause the security software installation to fail. We recommend that you:

- Use a local repository.
- Install the software without dependencies. See **Installation on Linux computers with limited Internet access** on page **144**.

Packages installed on computers

When you run it, the installation script performs a number of checks that require installation of one of these packages:

- wget
- curl

If neither of these packages are installed, the installation process fails returning an error.

Generating the installation package and manual deployment

- From the top menu, select **Computers**. In the upper-right corner of the page, click **Add computers.** A dialog box opens that shows all platforms supported by Advanced EPDR.
- Click the **Linux** icon. The **Linux** dialog box opens.

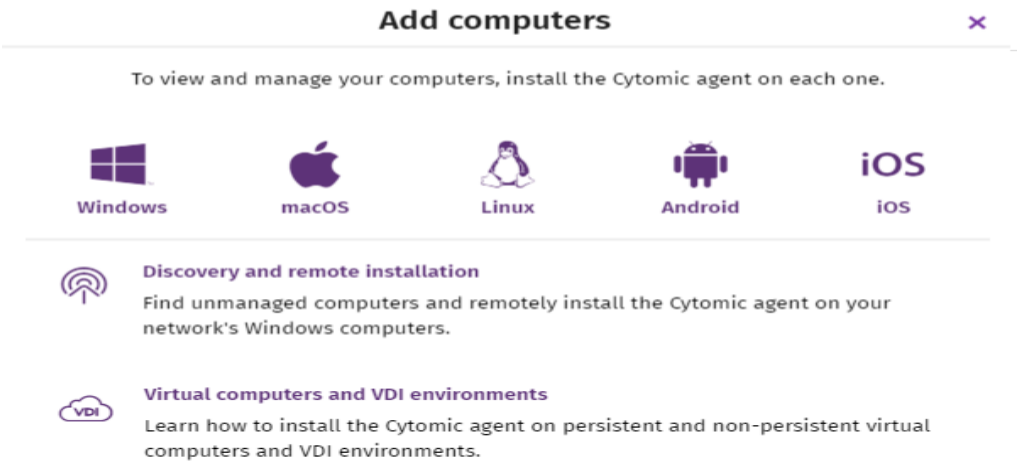


Figure 5.8: Dialog box for selecting a platform supported by Advanced EPDR

- To add the computer to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.
- To add the computer to an Active Directory group, select **Add computers to their Active Directory path**.

*The security policies assigned to a computer depend on the group it belongs to. If you select **Add computers to their Active Directory path**, and the Active Directory administrator moves a computer from one organizational unit to another, the change is reflected in the Advanced EPDR console as a group change. The security policies assigned to the computer might also change.*

- To establish a network settings profile other than the profile of the group the computer is added to, click **Select the network settings to apply to the computers**. From the drop-down list, select a settings profile. Initially, all the settings profiles that are applied to a computer when you add it to the console are the profiles that are assigned to the console group it belongs to. However, to avoid connectivity issues and prevent the computer from being inaccessible from the console because of incorrect network settings, you can set an alternative profile. For more information about how to create network settings profiles, see **Configuring the agent remotely** on page **307**.
- To send the installer to the target user by email:
    - Click the **Send URL by email** button. Your email application opens a new email with the download URL.
    - Add recipients to the message. Click **Send**.
    - When a user clicks the link, the installer downloads.
- To download the installation package and share it with the users on the network, click **Download installer**.

Installation on Linux computers

Depending on the characteristics of the target computer, you can install the agent in multiple ways:

- Installation on Linux computers with an Internet connection
- Installation on Linux computers with Secure Boot
- Installation on Linux computer with limited Internet access

Installation on Linux computers with an Internet connection

Make sure you have administrator permissions on the device. Make sure the downloaded package has execute permissions. The installer searches the target computer for the libraries it needs. If it cannot find the libraries, it downloads them automatically from the Internet.

- Open a terminal in the folder where the downloaded package is located. Run these commands:

```
$ sudo chmod +x "/DownloadPath/Panda Endpoint Agent.run"
$ sudo "/DownloadPath//Panda Endpoint Agent.run"
```

- On hardened computers, use the `--target ./install/` command to generate a temporary folder in the script location.

```
$ sudo "/DownloadPath/Panda Endpoint Agent.run" --target ./install/
```

- If you use a proxy server to access the Internet, add this parameter: `--proxy`. If you want to specify a list of proxy servers, use this parameter: `--proxy=<proxy-list>` . The installation script uses the first proxy server in the list. If the server fails, the script continues down the list of proxy servers until it finds one that works.

  `<proxy-list>` is a list of proxy servers separated by commas. Users and protocols are indicated with this syntax:

```
<http|https>://<user1>:<pass1>@<host1>:<port1>
```

  For example, to install a Linux agent that uses two proxy servers:

```
$ sudo "/DownloadPath/Panda Endpoint Agent.run" -- --
proxy=http://user1:pass1@192.168.0.1:3128,
http://user2:pass2@192.168.0.2:3128
```

- To verify that the `AgentSvc` process is running, run this command:

```
$ ps ax | grep Agent Svc
```

- Make sure this installation directory was created:

```
/usr/local/management-agent/*
```

Installation on Linux computers with Secure Boot

Some Linux distributions detect when a computer has Secure Boot enabled. With Secure Boot enabled, the security software that is not correctly signed is automatically disabled. Secure Boot is detected when the software is installed, or later, if the distribution did not initially support this feature but it was added in a later update. In either case, the console shows an error and the protection software does not run. To solve the protection errors related to Secure Boot from the computer experiencing the problem, make sure your system meets these requirements and complete the steps to resolve the errors:

System requirements

- **DKMS (Dynamic Kernel Module Support) systems**: `mokutil` and `openssl` packages.
- **Oracle Linux 7.x/8.x with UEKR6 kernel**: Repository `ol7_optional_latest` enabled, and `openssl`, `keyutils`, `mokutil`, `pesign`, `kernel-uek-devel-$(uname -r)` packages.

Enabling the security software on computers with Secure Boot

To enable the security software on the target computer:

- Check the state of Secure Boot:

```
$ mokutil --sb-state
```

If Secure Boot is enabled on the computer, `Secure Boot enabled` displays.

- Verify that the protection driver is not loaded:

```
$ lsmod | grep prot
```

- Import the protection keys:

```
$ sudo /usr/src/protection-agent-<version>/scripts/sb_import_key.sh
```

The agent and protection files have this format: ***protection-agent-03.01.00.0001-1.5.0_741_g8e14e52****. The name varies according to the version and the driver.*

A message appears to explain the implications of Secure Boot.

- Press **C** to register the certificate used to sign the modules.
- Enter an eight-character password.
- Restart the computer and complete the registration process:
    - To start the registration process, press any key. This screen appears for a limited time. If you do not press a key, you must restart the registration process.
    - Select **Enroll MOK**. To view the keys that are going to be registered, select **View key**.
    - Confirm the keys belong to Panda Security. Select **Continue**.
    - To enroll the key, select **Yes**.
    - Enter the password created in step 3. Select **Reboot**.
    - Confirm the driver is loaded:

```
$ lsmod | grep prot
```

Oracle Linux 7.x/8.x with UEKR6 kernel

When the distribution installed is Oracle Linux 7.x/8.x with UEKR6 kernel, after you complete the steps to register the certificate, follow these steps:

- Run this command:

```
$ sudo /usr/src/protection-agent-<version>/scripts/sb_import_key.sh
```

This command adds the certificate used to sign the modules to the list of certificates trusted by the kernel. The modified kernel is signed and added to the list of kernels in GRUB.

- Restart the computer. The module is loaded and started.
- To confirm that the certificate was added correctly, run this command:

```
$ sudo /usr/src/protection-agent-<version>/scripts/sb_import_key.sh
```

The results should be:

```
The signer's common name is UA-MOK Driver Signing
 Image /boot/vmlinuz-kernel-version-panda-secure-boot is already
signed
 Kernel module is successfully loaded
```

Installation on Linux computers with limited Internet access

Advanced EPDR must connect to the Internet to work correctly. However, you might want to restrict Internet access for the servers on which the security software runs to prevent information from being downloaded or sent from or to unknown external sources. In such case, Advanced EPDR cannot complete the installation process because it requires access to external repositories to satisfy its dependencies.

This installation method enables you to install the security software on computers that can access only the Cytomiccloud, from which they can download a package with all required libraries.

With this installation method, the third-party libraries included in the package that have errors or vulnerabilities do not automatically update on the protected computer.

The installer is compatible with these Red Hat-based distributions:

- Red Hat
- CentOS
- CentOS Stream
- SuSE Linux Enterprise
- openSUSE
- Oracle Linux
- Alma Linux
- Rocky Linux

For more information about the supported versions of these distributions, see **Supported distributions** on page **947**

The installer is compatible with these Linux agent and protection versions:

- Protection version: 3.00.00.0050 and higher.
- Agent version: 1.10.06.0050 and higher.

If you use the package with an unsupported Linux distribution, the installation process will fail. You can use this installation method only if you install the solution on a computer that does not have a previous version of the security software installed. Otherwise, the repository previous settings are kept.

To install the Advanced EPDR agent without an Internet connection, open a terminal in the folder where the downloaded package is located. Run these commands:

```
$ sudo chmod +x "/DownloadPath//Panda Endpoint Agent.run"
$ sudo "/DownloadPath/Panda Endpoint Agent.run" -- --no-deps
```

Installation on macOS systems

Protection deployment overview

The installation process consists of a series of steps that vary depending on the status of the network at the time of deploying the software and the number of computers to protect:

- Find unprotected devices on the network
- Verify minimum requirements for target devices
- Uninstall competitor products
- Determine device default settings
- Verify the security software has been correctly installed.

Find unprotected devices on the network

Find devices on the network without protection installed or with a third-party security product that needs replacing or complementing with Advanced EPDR. Verify that you have purchased enough licenses for the unprotected devices. See **Licenses** on page **189**.

> *Advanced EPDR enables you to install the software even when you do not have enough licenses for all the computers you want to protect. Computers without a license show in the management console with some information (such as installed software and hardware), but are not protected.*

Verify minimum requirements for target devices

For more information about minimum requirements, see **Installation requirements**.

Uninstall competitor products

We recommend that you uninstall any third-party antivirus and security software prior to installing Advanced EPDR.

Determine device default settings

When the software is installed on the computer or device, Advanced EPDR assigns the **All** group security settings to it. However, during installation, you can select a different target group for the computer with the required settings. See **Managing settings** on page **287**.

Verify the security software has been correctly installed

- Select **Computers** from the top menu. Find the corresponding computer. For more information about how to find computers, see **Managing computers and devices** on page **211**.
- Select the computer on which the security software has been installed. The computer details page opens.
- Select the **Details** tab. All information collected from the computer is shown, along with the installation status.
- In the **Security** section, verify the status of the various modules:
    - **Installing...**: The installation process is incomplete or there has been an error. If the process failed, the status does not change until the installation problem is resolved.
    - **Enabled/Disabled:** After a few minutes, if the installation has been successful, the status of the protection modules is shown.

Detect and resolve installation errors

If, after a few minutes, the **Security** section disappears from the computer details page, it is because the security software did not install correctly. Verify this:

- Verify whether the user computer shows error messages.
- Verify whether the computer appears in lists. See **Checking deployment**.
- Verify whether the user computer meets the requirements specified in **Installation requirements** . Update the product or operating system version if required. See **Product updates and upgrades** on page **203**.

Installation requirements

Make sure the computer you want to install the security software on meets these system and network requirements.

From 30 September 2024, you will not be able to add devices to the management console or install the protection software on new computers that run these operating system versions: macOS Yosemite, El Capitan, Sierra, High Sierra, or Mojave. Existing computers in the management console will continue to be protected. See ***https://www.watchguard.com/wgrd-trust-center/end-of-life-policy***.

Supported operating systems

See **Supported operating systems** on page **944**.

Hardware requirements

See **Hardware requirements** on page **945**.

Network requirements

Advanced EPDR requires access to multiple Internet-hosted resources. It requires access to ports 80 and 443. For a complete list of the URLs that Advanced EPDR requires access to, see **Local ports and URL access** on page **952**.

The Advanced EPDR agent requires access to port 33000 for protected computers on the network to communicate with each other (see **Endpoint Access Enforcement settings** on page **518**) and with the Firebox or Access Point devices (see **Network Access Enforcement** on page **318**

To activate the product, access to certain IP address ranges is required. For more information, see **IP addresses required for product activation** on page **945**.

Time synchronization of computers (NTP)

Although not an essential requirement, we recommend that the clocks on computers protected by Advanced EPDR be synchronized. This synchronization is normally achieved using an NTP server. See **Time synchronization of computers (NTP)** on page **942**.

Required permissions

For the protection to operate correctly, you must enable:

- Network extensions.
- System extensions.
- Full disk access.
- Background execution.

For more information, see **Required permissions** on page **945**.

Manually deploying the macOS agent

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button in the upper-right corner of the page. A window opens with all platforms supported by Advanced EPDR.
- Click the **macOS** icon. The **macOS** window opens.

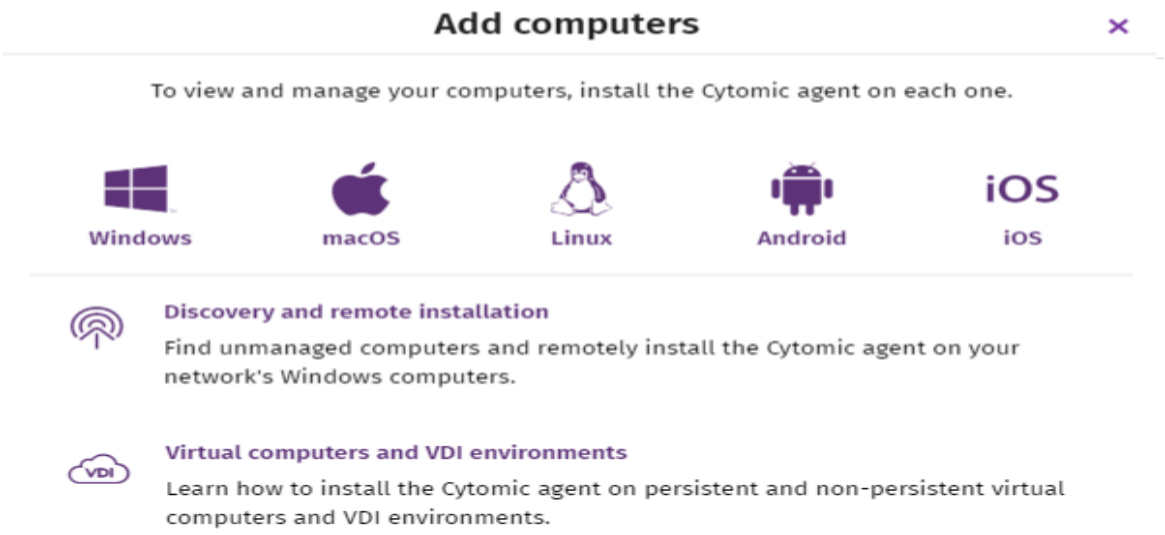


Figure 5.9: Window for selecting a platform supported by Advanced EPDR

- To add the device to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.
- To establish a network settings profile other than the profile of the group the computer is integrated into, click **Select the network settings to apply to the computers**. Choose a settings profile from the drop-down list. Initially, all the settings profiles that are applied to a computer upon integration into the console are the profiles that are assigned to the console group it belongs to. However, to avoid connectivity failures and prevent the computer from being inaccessible from the console because of incorrect network settings, you can set an

alternative profile. For more information about how to create network settings profiles, see **Configuring the agent remotely** on page **307**.

To send the installer to the target user by email:

- Click the **Send URL by email** button. The email app installed on the administrator's computer opens with a predefined message containing the download URL.
- Add the desired recipients to the message. Click **Send**.
- The user that receives the message must click the URL from the target device to download the installer.

- To download the installation package and share it with the users on the network, click **Download installer (7)**.

Installing the downloaded package

- Double-click the `.dmg` file. Run the `.pkg` container. A progress bar displays during the installation process. Regardless of whether there are free licenses available, the computer is integrated into the service. However, if there is no available license to assign to the target computer, the computer is not protected.
- When the installation completes, the product checks that it has the latest version of the signature file and the protection engine. If not, it updates them automatically.
- To make sure the agent is installed, and verify that the AgentSvc process is running, run this command:

```
$ ps ax | grep Agent Svc
```

- (Optional) Verify that the installer created these directories:

```
/Applications/Management-Agent.app/
/Library/Application Support/Management Agent/
```

To install the product agent on devices with macOS Catalina, you must assign specific permissions. For more information, see: ***https://www.pandasecurity.com/en/support/card?id=700079*** .

Installation on Android systems

Protection deployment overview

The installation process consists of a series of steps that depend on whether the target devices are managed with an MDM/EMM solution or not.

MDM (Movile Device Management)/EMM (Enterprise Mobility Management) is software that enables organizations to monitor and manage mobile devices regardless of the mobile operator or service provider chosen. MDM/EMM solutions enable you to remotely install apps on managed devices, locate and track managed devices, sync files across them, and report data remotely and centrally. These solutions are commonly found in companies that manage a large number of devices.

To deploy and install the protection software, follow these steps:

- Find unprotected devices on the network.
- Verify minimum requirements for target devices. See **Installation requirements**.
- Uninstall competitor products prior to installing Advanced EPDR.
- Determine device default settings. See **Determine device default settings**.
- Select a deployment strategy based on whether the target device is enrolled into an MDM/EMM solution. See **Select a deployment strategy**.

Find unprotected devices on the network

Find devices on the network without protection installed or with a third-party security product that needs replacing or complementing with Advanced EPDR. Verify that you have purchased enough licenses for the unprotected devices. See **Licenses** on page **189**.

Advanced EPDR enables you to install the software even when you do not have enough licenses for all the computers you want to protect. Computers without a license show in the management console with some information (such as installed software and hardware), but are not protected.

Determine device default settings

When the software is installed on the computer or device, Advanced EPDR assigns the **All** group security settings to it. However, during installation, you can select a different target group for the computer with the required settings. To create and assign new settings profiles, see **Managing settings** on page **287**.

Select a deployment strategy

Depending on whether the target devices are enrolled into an MDM/EMM solution or not, and on the type of solution, the following deployment types are supported:

- Manual deployment on devices not enrolled into an MDM/EMM solution. See **Manually deploying and installing the Android agent**.
- Deployment using a third-party MDM/EMM solution. See **Deploying the Android agent using an MDM/EMM solution** .

Installation requirements

Make sure the device you want to install the security software on meets these system and network requirements.

Supported operating systems

See **Supported operating systems** on page **949**.

Hardware requirements

See **Hardware requirements** on page **950**.

Network requirements

In normal conditions, if the device is connected to the network by 2G, 3G, 4G, or higher, there are no specific network requirements. In other scenarios, you must open certain ports to all IP addresses contained in the IP blocks listed in Google's ASN 15169. See **Network requirements** on page **950**.

Permissions required on the device

To use all of the Advanced EPDR features, the user of the device must allow all permissions requested by the application. For a complete list of required permissions, see **Permissions required on the device** on page **950**.

Manually deploying and installing the Android agent

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button in the upper-right corner of the page. A window opens with all platforms supported by Advanced EPDR.
- Click the **Android** icon. The **Android** window opens.

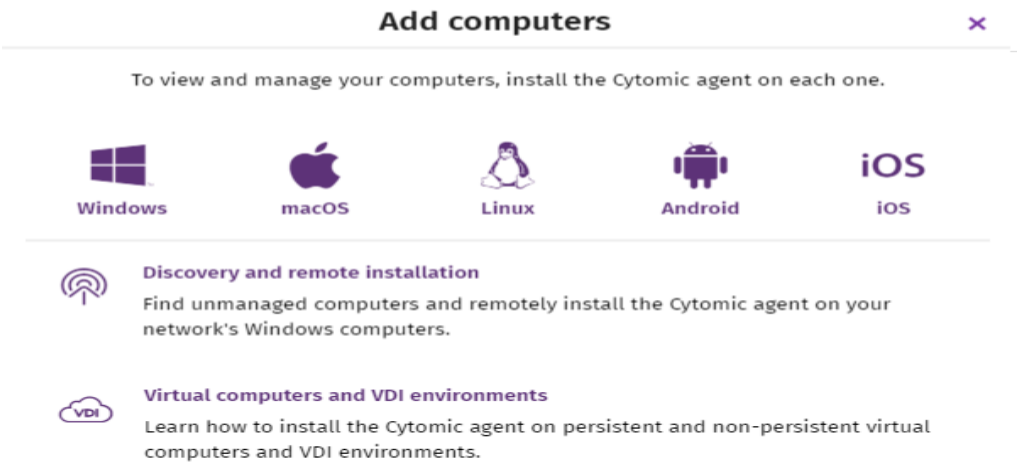


Figure 5.10: Window for selecting a platform supported by Advanced EPDR

- To add the Android device to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.
- To install the Android agent on the device using the QR code:
  - Point the device camera at the QR code on the computer screen. You are taken to the **Protection - Panda Aether** app page on Google Play.
  - Tap the **Install** button. The app is automatically downloaded and installed.
- To download the installer to the target device directly from Google Play:
  - Tap the **Go to Google Play** icon from the target device. You are taken to the **Protection** - **Panda Aether** app page on Google Play.
  - Tap the **Install** button. The app is automatically downloaded and installed.
- To send the installer to the target user by email:
  - Click the **Send URL by email** button. The email app installed by default on the administrator's computer opens with a predefined message containing the download URL.
  - Add the desired recipients to the message. Click **Send**.
  - The user that receives the message must tap the URL from the target device. The user is taken to the **Protection - Panda Aether** app page on Google Play.
  - The user must tap the **Install** button. The app is automatically downloaded and installed.
- The first time the app is launched on the mobile device, the **Enter alias** screen opens.
- Enter the name that will be displayed in the Advanced EPDR console to identify the device. Tap **Continue**. A series of installation status messages is displayed, and a screen for the user to grant a number of permissions to the app. If the user does not grant those permissions to the

app, the app will not work correctly. See **Permissions required on the device** on page **950**.

- Regardless of whether the permissions are granted or not, the installation process completes and the device appears in the Advanced EPDR management console.

Deploying the Android agent using an MDM/EMM solution

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button. A window opens with the platforms supported by Advanced EPDR.
- Click the **Android** icon. The **Android** window opens.
- Click the **Send URL by email** button. The email program installed by default on the administrator's computer opens with a predefined message containing the download URL Write down the link to use it as integration URL with your MDM/EMM solution.
- In your MDM or EMM solution, import the **WatchGuard Mobile Security** app that you obtained from Play Store.
- In your MDM or EMM solution, add the following as parameters for the app you imported in the previous step:
    - **Use automatic name**: Boolean parameter. If the value of the parameter is **True**, a name based on the "<Device model>_<Unique identifier>" pattern is automatically assigned.
    - **Device name**: The name that is assigned to the device if the value of the **Use automatic name** parameter is **False**. You can use wildcards and other special characters as per the specifications of your MDM or EMM solution to generate a different name for each device.
    - **Integration URL**: The integration URL shown in the Advanced EPDR console.
- The first time the app is launched on the mobile device, the **Enter alias** screen opens.
- If the **Use automatic name** parameter is set to **False**, and **Device name** is not defined, the app prompts for the name with which it will show the device in the Advanced EPDR console.
- Tap **Continue**. A series of messages showing the status of the installation process is displayed, as well as a screen prompting the user to grant a number of permissions to the app. If the user does not grant those permissions to the app, the app will not work correctly. See **Permissions required on the device** on page **950**.
- Regardless of whether the permissions are granted or not, the installation process completes and the device appears in the Advanced EPDR management console.

Installation on iOS systems

Protection deployment overview

The installation process of the protection on iOS devices consists of a series of steps that depend on whether there is an MDM (Mobile Device Management) solution implemented in the organization:

- Find unprotected devices.
- Verify minimum requirements for target devices. See **Installation requirements**.
- Uninstall competitor products prior to installing Advanced EPDR.
- Determine device default settings. See **Select a deployment strategy**.
- Select a deployment strategy based on whether the target device is enrolled into an MDM solution. See **Select a deployment strategy**.

Find unprotected devices on the network

Find devices on the network without protection installed or with a third-party security product that needs replacing or complementing with Advanced EPDR. Verify that you have purchased enough licenses for the unprotected devices. See **Licenses** on page **189**.

Advanced EPDR enables you to install the software even when you do not have enough licenses for all the computers you want to protect. Computers without a license show in the management console with some information (such as installed software and hardware), but are not protected.

Determine device default settings

When the software is installed on the computer or device, Advanced EPDR assigns the **All** group security settings to it. However, during installation, you can select a different target group for the computer with the required network settings. To create and assign new settings profiles, see **Managing settings** on page **287**.

Select a deployment strategy

The iOS agent deployment process varies depending on whether the target device is managed with an MDM solution or not.

- Manual deployment on devices not enrolled into an MDM solution See **Deploying and installing the agent on devices not enrolled into an MDM solution**.
- Deployment using the Cytomic MDM solution. See **Deploying and installing the agent on devices enrolled into the Cytomic MDM solution**.

- Deployment using a third-party MDM solution. See **Deploying and installing the agent on devices enrolled into a third-party MDM solution**.
- Deployment on supervised devices with Cytomic MDM. See **Configuring the device in supervised mode and enrolling it into the Cytomic MDM solution**.
- Deployment on supervised devices with third-party MDM. See **Enabling supervised mode and deploying the iOS agent from a third-party MDM solution**.

For more information about possible scenarios in Advanced EPDR, see **Basic concepts**.

If the target device is managed with the Cytomic MDM solution, see **Managing the Apple ID and digital certificates**.

Basic concepts

MDM (Movile Debice Management)

MDM is software that enables organizations to monitor and manage mobile devices regardless of the mobile operator or service provider chosen. Most MDM solutions enable you to remotely install apps on iOS devices, locate and track iOS devices, sync files across them, and report data remotely and centrally. These solutions are commonly found in companies that manage a large number of devices.

Managing iOS devices with an MDM solution

An iOS device can only be remotely managed with one MDM solution at a time. To manage an iOS device using an MDM solution, you must first enroll it into the solution. At the end of the enrollment process, a settings profile is sent from the MDM solution to the device, which the user must install on it.

CytomicMDM

Because the remote management options for an iOS device are very limited if the device is not enrolled into an MDM solution, Advanced EPDR seamlessly incorporates its own MDM solution into the management console. Additionally, because each iOS device can only be remotely managed with one MDM solution, it is very important that you make the right decision regarding which MDM solution will manage the organization's devices when integrating them into Advanced EPDR.

*If your iOS devices were already enrolled into a third-party MDM solution and you decide to enroll them into the Cytomic MDM solution, you will lose the centralized management capabilities provided by your MDM solution and will not be able to access any software you deployed through it. See **Enrollment types supported by Advanced EPDR**.*

Enrollment types supported by Advanced EPDR

Based on the enrollment type, Advanced EPDR provides the administrator with different features from the management console.

Enrollment type	Features available in the Advanced EPDR console
Installation on iOS devices enrolled into the Cytomic (recommended if you did not already use an MDM solution)	• Hardware inventory • Software inventory • Web protection * • Web filtering * • Geolocation • Remote alarm • Wipe data • Lock
Installation on iOS devices enrolled into a third-party MDM solution (recommended if you already used an MDM solution)	• Hardware inventory • Web protection * • Web filtering * • Geolocation • Remote alarm
Installation on iOS devices not enrolled into an MDM solution	• Hardware inventory • Geolocation • Remote alarm

Table 5.8: Enrollment types supported by Advanced EPDR

* To filter web traffic, the iOS device must be in supervised mode.

Requirements for integrating a device using the Cytomic MDM solution

To integrate an iOS device into the Advanced EPDR management console using the Cytomic MDM solution, you need:

- **An Apple user account (Apple ID)**: Required to generate and import certificates into the management console. You can use an existing account or create a new one.
- **A digital certificate issued by Apple**: Required for the iOS devices you want to manage to be able to communicate securely with the Apple servers. Digital certificates are valid for one

year, after which they expire. Register all of your company's iOS devices with the same digital certificate.

For more information, see **Managing the Apple ID and digital certificates**.

Installation requirements

Make sure the device you want to install the security software on meets these system and network requirements.

Supported operating systems

See **Supported operating systems** on page **950**.

Hardware requirements

The minimum space required to install the security software varies depending on the operating system version installed on the device. On average, the security software requires 12 MB of available space for installation.

Network requirements

The application installed on the mobile device uses the Apple Push Notification service to communicate with Advanced EPDR. If the device is connected to the network by 2G, 3G, or 4G, there are no specific network requirements. For other scenarios, see **Network requirements** on page **951**.

Permissions required on the device

To use all of the Advanced EPDR features, the user of the device must allow all permissions requested by the application. For a complete list of required permissions, see **Permissions required on the device** on page **952**.

Deploying and installing the iOS agent

Deploying and installing the agent on devices not enrolled into an MDM solution

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button in the upper-right corner of the page. A window opens with all platforms supported by Advanced EPDR.

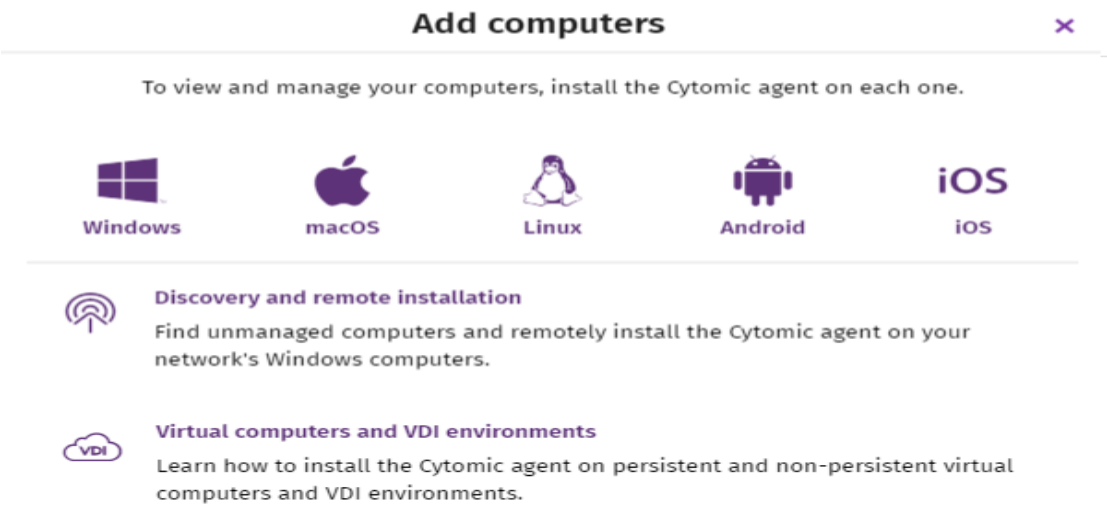


Figure 5.11: Window for selecting a platform supported by Advanced EPDR

- Click the **iOS** icon. The **iOS** window opens.
- Click the **Installation without an MDM solution** link. The **iOS** window opens.
- To add the iOS device to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.
- To install the iOS agent on the device using the QR code:
    - Point the device camera at the QR code on the computer screen. You are taken to the **WatchGuard Mobile Security** app page on the App Store.
    - Tap the **Install** button. The app is automatically downloaded and installed.
- To download the installer to the target device directly from the App Store:
    - Tap the **Go to Apple Store** icon from the target device. You are taken to the **WatchGuard Mobile Security** app page on the App Store.
    - Tap the **Install** button. The app is automatically downloaded and installed.
- To send the installer to the target user by email:
    - Click the **Send URL by email** button. The email app installed by default on the administrator's computer opens with a predefined message containing the download URL.
    - Add recipients to the message and click **Send**.
    - The user that receives the message must tap the URL from the target device. The user is taken to the **WatchGuard Mobile Security** app page on the App Store.
    - The user must tap the **Install** button. The app is automatically downloaded and installed.

- The first time the app is launched on the iOS device, a welcome window opens with the text **"WatchGuard Mobile Security" Would Like to Send You Notifications**. Tap the **Allow** button.
- If the **WatchGuard Mobile Security** app was installed by searching for it manually on the App Store, you must integrate it manually into Advanced EPDR.
    - Tap the **Use QR Code** button. The message **"WatchGuard Mobile Security" Would Like to Access the Camera** appears.
    - Tap **Allow**. Point the phone camera at the QR code in the Advanced EPDR management console. The message **Downloading configuration** appears on the mobile phone.
- When the configuration finishes downloading, the message **"WatchGuard Mobile Security" Would Like to Find and Connect to Devices on Your Local Network** appears. Tap **OK**. The **Enter alias** window opens.
- Enter the name that will be used in the Advanced EPDR console to identify the device. Tap **Continue**. A number of installation status messages are shown. Then, the message **"WatchGuard Mobile Security" Would Like To Filter Network Content** appears.
- Tap the **Allow** button. The **Enter the iPhone code** window opens.
- Enter the device password. The **OK** window opens. The installation is complete.

Deploying and installing the agent on devices enrolled into the Cytomic MDM solution

- Verify you have a valid Apple certificate uploaded to the Advanced EPDR management console. To generate a certificate, see **Creating and importing the digital certificate into the Advanced EPDR console** . If your certificate is about to expire, see **Renewing the Apple certificate**.
- Make sure your company's iOS devices do not have a third-party MDM profile already installed. If they do, delete the profile from your devices. For more information about the implications of deleting a third-party MDM profile, see **Managing iOS devices with an MDM solution** and **Enrollment types supported by Advanced EPDR**.
- Select the **Computers** menu at the top of the Advanced EPDR management console. Click the **Add computers** button. A window opens with the platforms supported by Advanced EPDR.
- Click the **iOS** icon. A window opens with information about the previously uploaded certificate.

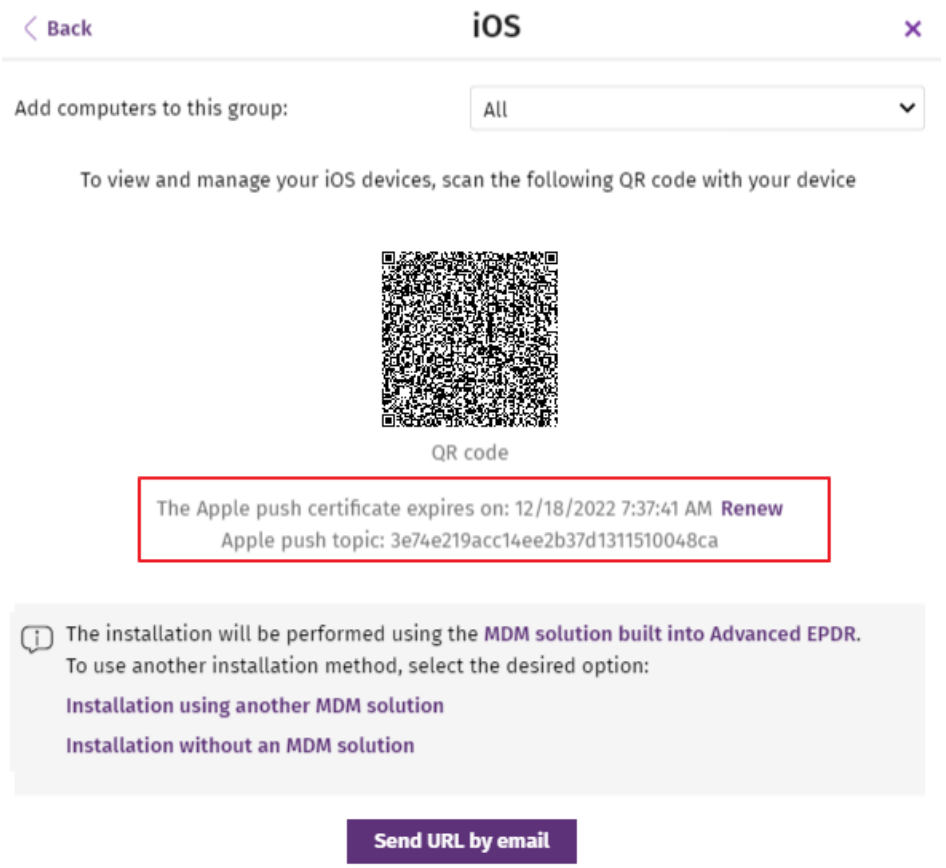


Figure 5.12: Window with the uploaded Apple digital certificate

- To add the iOS device to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.
- Choose a method for sending the installation profile to the target iOS device:
    - To send the installation profile using the QR code, scan the code with the device camera. The device shows the message **This website is trying to download a configuration profile**. **Do you want to allow this?**
    - To send the installation profile download link to the target user by email, click the **Send URL by email** button. When the device user clicks the link, the device shows the message **This website is trying to download a configuration profile**. **Do you want to allow this?**
- Tap **Allow**. After the profile has been downloaded to the iOS device, the message **Profile Downloaded** appears.
- Open the **Settings** app on the iOS device.
- Tap **General**.
- Tap **VPN and device management**. The **WatchGuard MDM Service** downloaded profile is shown.

- Tap **WatchGuard MDM Service**. The **Install profile** window opens with information about the security of the downloaded file.
- Tap **Install** in the upper-right corner. You are asked to enter the phone password.
- Enter the password. A **Warning** message appears, indicating that the device will be managed remotely.
- Tap **Install** in the upper-right corner. The **Remote Management** window opens.
- Tap **Trust**. The profile is installed. After a few minutes, the device shows a notification to automatically download and install the Advanced EPDR agent.
- Tap the **Install** button. The app is downloaded and installed on the device.
- After the app is downloaded and installed, tap it to run it for the first time. The message **"WatchGuard Mobile Security" Would Like to Send You Notifications** appears.
- Tap the **Allow** button. The device is integrated into the Advanced EPDR console and the **Enter the iPhone code** window opens.
- Enter the device password. The **OK** window opens. The installation is complete.

Deploying and installing the agent on devices enrolled into a third-party MDM solution

The procedures in this section associated with the MDM software vary based on the vendor you select. See your product help for more information.

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button. A window opens with all platforms supported by Advanced EPDR.
- Click the **iOS** icon. The **iOS** window opens.
- Click the **Installation using another MDM solution** link. The **iOS - Another MDM solution** window opens with the information the MDM solution needs to integrate the device.

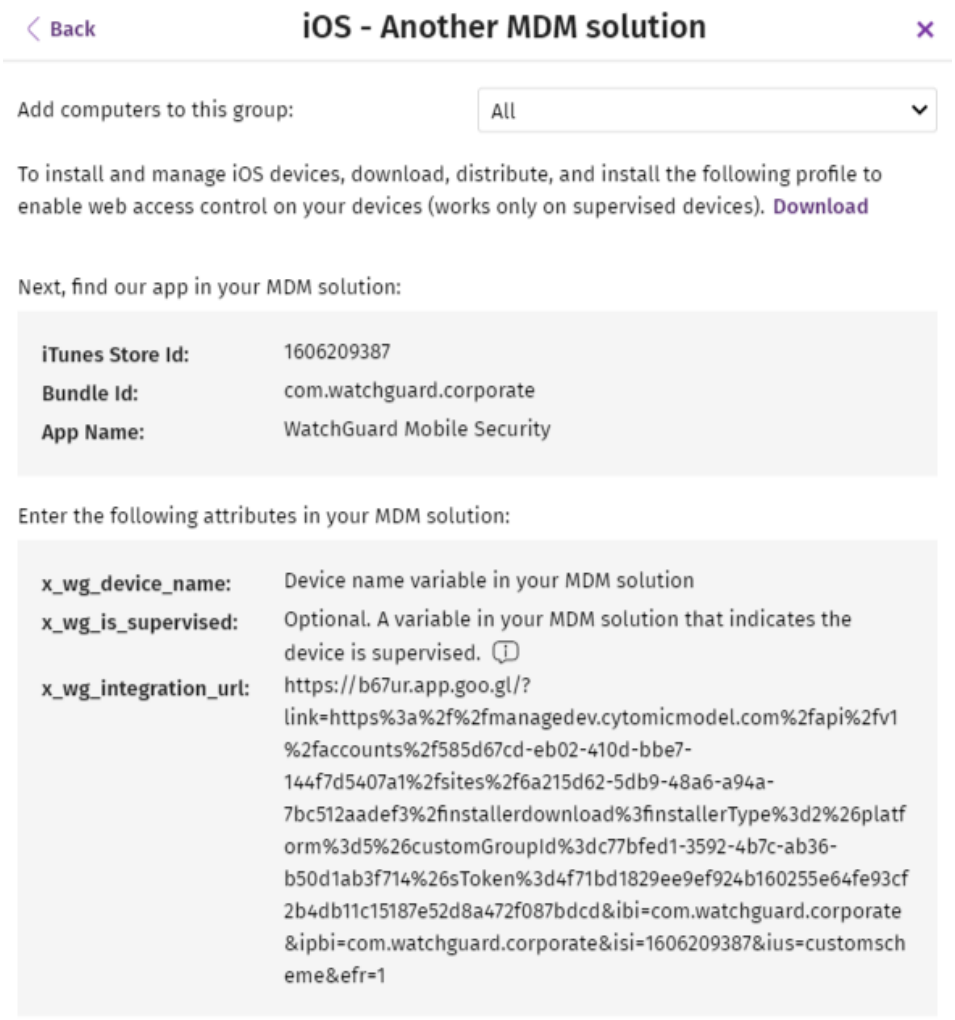


Figure 5.13: Window with the integration parameters for the third-party MDM solution

- In the third-party MDM solution, import the **WatchGuard Mobile Security** app directly from the Apple Store. To do this, use the **iTunes Store Id**, **Bundle Id**, or **App Name** fields in figure **Figure 5.13:** , or the search features included in the MDM solution.
- Associate and define the parameters **x_wg_device_name** and **x_wg_integration_url** in the **WatchGuard Mobile Security** app imported into the third-party MDM solution repository. The information contained in these parameters is sent along with the **WatchGuard Mobile Security** app when you push the app to the devices managed with the MDM solution.
    - **x_wg_device_name**: Contains the device name that will be shown in the Advanced EPDR console. In the **x_wg_device_name** parameter, enter the variable used by the MDM solution to represent the name of the device that will receive the **WatchGuard Mobile Security** app.
    - **x_ wg_ integration_ url**: Contains the URL that points to the information that **WatchGuard Mobile Security** needs to integrate into the group chosen by the Advanced EPDR administrator. Copy the content of the **x_ wg_ integration_ url**

attribute shown in the Advanced EPDR console to the parameter defined in the MDM solution.

Each MDM solution uses a different variable name and syntax. See your product documentation for this information.

Use a variable for the x_wg_device_name *parameter. If, instead of the variable that represents the device name, you enter a device name, all the mobile devices that receive* ***WatchGuard Mobile Security*** *will be shown with the same name in the Advanced EPDR console.*

- Push the WatchGuard Mobile Security app from the MDM solution to the devices that you want to protect. After a few minutes, the device shows a notification to automatically download and install the Advanced EPDR agent.
- Tap the **Install** button. The app is downloaded and installed on the device.
- After the app is downloaded and installed, tap it to run it for the first time. The message **"WatchGuard Mobile Security" Would Like to Send You Notifications** appears.
- Tap the **Allow** button. The device is integrated into the Advanced EPDR console and the **Enter the iPhone code** window opens.
- Enter the device password. The **OK** window opens. The installation is complete.

Deploying and installing the agent on supervised devices

You must configure iOS devices in supervised mode to leverage the URL filtering capabilities provided by Advanced EPDR.

When you place a device in supervised mode, you must reset the device to factory-default settings. All data, programs, and settings delete. To remove the supervised state, reset the device to factory-default settings again.

Concepts

Supervised mode

It is an execution mode for iOS devices used in corporate environments. It provides administrators with greater flexibility to configure apps and manage devices. In supervised mode, the administrator can, the first time the device is turned on and before it is activated, apply

configuration profiles for apps and resources on the phone, schedule the installation of apps, or restrict app usage. To configure an iOS device in supervised mode, you must attach it to a macOS computer using a USB cable.

Apple Configurator 2

An app that is run on the macOS computer and enables you to configure iOS devices in supervised mode.

Finder

This is the native macOS file explorer. It is used to create a full backup of the iOS device and restore it later.

iCloud

Cloud storage service. With an Apple ID, users can access their documents, photos, calendars, and other resources online without the need to store them on their mobile device.

Blueprint

A container that stores the apps that you want to send to a device to configure it. Additionally, the Blueprint has the mobile device management (MDM) information and enables you to enable or disable part of the Setup Assistant that is shown to the user the first time that they turn on the device.

Requirements

- A macOS computer with macOS 10.15.6 or higher.
- The Apple Configurator 2 app. You can download it for free at **https://apps.apple.com/us/app/apple-configurator/id1037126344?mt=12**
- A USB cable to attach the iOS device to the macOS computer.
- To enable web filtering on supervised iOS devices enrolled into a third-party MDM solution, the MDM solution must allow import of external profiles. Verify whether your MDM solution supports this feature before you begin the procedure described in this section.
- **Optional**: Finder app to create a backup if needed and restore it. See **Configuring an iOS device in supervised mode without loss of data**.

Configuring the device in supervised mode and enrolling it into the Cytomic MDM solution

The process to configure an iOS device in supervised mode is carried out independently from the process to enroll it into the Cytomic MDM solution.

When you configure an iOS device in supervised mode, all data and apps on the device delete. To create a backup of the data and restore it after the procedure has been completed, see **Configuring an iOS device in supervised mode without loss of data**.

To verify that the iOS device is in supervised mode, see **Verifying that the device is supervised**

Creating the Blueprint

- On the macOS computer, open the Apple Configurator 2 app. Select **File**, **New Blueprint**. The **All Blueprints** window opens, showing all Blueprints created so far. The newly created Blueprint is automatically selected.
- Type the name of the new Blueprint. Press **Enter**.

Getting the Advanced EPDR MDM solution enrollment URL

- Verify you have a valid Apple certificate uploaded to the Advanced EPDR management console. To generate a certificate, see **Creating and importing the digital certificate into the Advanced EPDR console** . If your certificate is about to expire, see **Renewing the Apple certificate**.
- Make sure your company's iOS devices do not have a third-party MDM profile already installed. If they do, delete the profile from your devices. For more information about the implications of deleting a third-party MDM profile, see **Managing iOS devices with an MDM solution** and **Enrollment types supported by Advanced EPDR**.
- Select the **Computers** menu at the top of the Advanced EPDR management console. Click the **Add computers** button. A window opens with the platforms supported by Advanced EPDR.
- Click the **iOS** icon. The **iOS** window opens with information about the previously uploaded certificate.

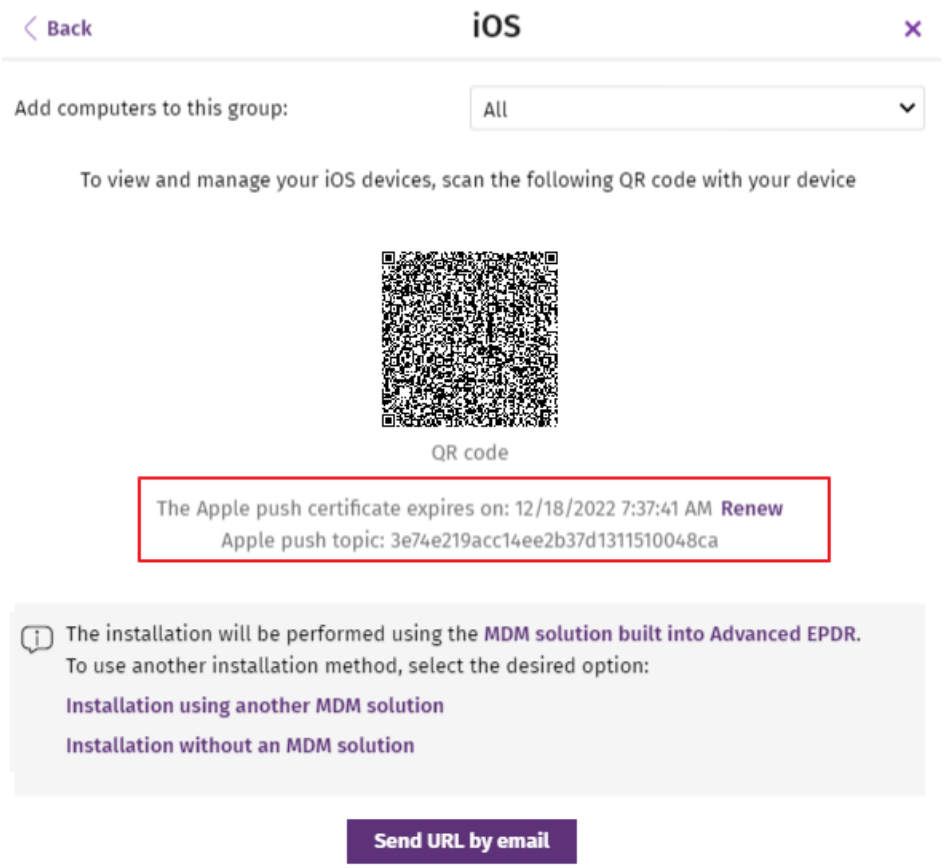


Figure 5.14: Window with the uploaded Apple digital certificate

- To add the iOS device to a group created in the management console, select **Add computers to this group**. From the drop-down list, select a folder.
- Click the **Send URL by email** button. The email program installed on the computer opens.
- Enter the email address of the user that will use the iOS device you want to enroll. Click **Send**.

Preparing the device

- In the Apple Configurator 2 app, select the created Blueprint and click **Prepare** in the top bar. The **Prepare devices** window opens.
- In **Prepare with**, select **Manual configuration**, **Supervise devices**, and **Allow devices to pair with other computers**. Click **Next**. The **Enroll in MDM server** window opens.
- In **Server**, select **Do not enroll in MDM**. Click **Next**. The **Sign in to Apple Business Manager or Apple School Manager** window opens.
- Click **Skip**. The **Create an organization** window opens.
- Enter your company's details. Click **Next**.
- Select **Create a new supervision identity**. Click **Next**. The **Configure iOS Setup Assistant** window opens.

- Choose which steps will be presented to the user in the Setup Assistant the first time the user turns on the iOS device. Click **Prepare**. A window opens that prompts for the macOS computer administrator credentials.
- Click **Update settings**. A pop-up window opens that shows the status of the configuration process.
- After the procedure is complete, the Blueprint is created and ready to be applied to all relevant iOS devices.

Applying the Blueprint to iOS devices

*Before enrolling a supervised iOS device into an MDM solution, make sure the **Find My iPhone** option is disabled.*

- Disable **Find My iPhone** on the user's iOS device.
    - Tap **Settings**.
    - Tap the user's name. Tap **Find My**.
    - Tap **Find My iPhone**, then tap to disable it.
    - Enter the Apple ID password.
    - Tap **Turn off**.
- Connect the iOS device to the macOS computer with a USB cable. The Apple Configurator 2 app must be open during the process. The message **Trust this computer?** appears on the mobile device.
- Tap **Trust**.
- In the Apple Configurator 2 app, click **All devices** in the top bar. After connecting, you can see the device in the Apple Configurator window.
- Right-click the device. A drop-down menu appears.
- Click **Apply**. Select the created Blueprint. A window opens for you to confirm you want to apply the Blueprint.
- When you click **Apply**, the following actions are taken on the iOS device:
    - The device is reset to its factory-default settings.
    - All data and apps are deleted from the device.
    - The device is placed in supervised mode.

Verifying that the device is supervised

- In the Apple Configurator 2 app, click **Supervised** in the top bar. The new supervised device is shown.
- Tap **Settings** on the iOS device. In the upper-left corner, under the phone name, the message "This iPhone is supervised and managed by (company name)" is shown.

Enrolling the supervised device into the Cytomic MDM solution

- Configure the email app on the supervised iOS device. Download the message that contains the MDM enrollment URL. This message was sent earlier from the Advanced EPDR console.
- Tap the link. A window opens that shows the message **This website is trying to download a configuration profile**. **Do you want to allow this?**
- Tap **Allow**. After the profile has been downloaded to the iOS device, the message **Profile downloaded** appears.
- Open the **Settings** app on the iOS device. The **Settings** window opens.
- Tap **General**. The **General** window opens.
- Tap **VPN and device management**. The **WatchGuard MDM Service** downloaded profile is shown.
- Tap **WatchGuard MDM Service**. The **Install profile** window opens with information about the security of the downloaded file.
- Tap **Install** in the upper-right corner. You are asked to enter the phone password.
- Enter the password. A **Warning** message appears, indicating that the device will be managed remotely.
- Tap **Install** in the upper-right corner. The **Remote Management** window opens.
- Tap **Trust**. The profile is installed. After a few minutes, the Advanced EPDR agent is downloaded and installed automatically.
- After the app is downloaded and installed, tap it to run it for the first time. The message **"WatchGuard Mobile Security" Would Like to Send You Notifications** appears.
- Tap the **Allow** button. The device is added to the Advanced EPDR console and the configuration process is complete.

Enabling supervised mode and deploying the iOS agent from a third-party MDM solution

The various MDM solutions available on the market support different methods to enable supervised mode on iOS devices. See the documentation to enable supervised mode on the iOS devices enrolled into your MDM solution.

To set WatchGuard Mobile Security as the app in charge of filtering web traffic on iOS devices, the MDM solution that you use must allow import of external configuration profiles. See the documentation for your MDM solution for information about how to enable supervised mode on enrolled iOS devices.

Deploying the WatchGuard Mobile Security app using a third-party MDM solution

The procedures in this section associated with the MDM software vary based on the vendor you select. See your product help for more information.

- Select the **Computers** menu at the top of the management console. Click the **Add computers** button. A window opens that shows all platforms supported by Advanced EPDR.
- Click the **iOS** icon. The **iOS** window opens.
- Click the **Installation using another MDM solution** link. The **iOS - Another MDM solution** window opens with the information the MDM solution needs to integrate the device.

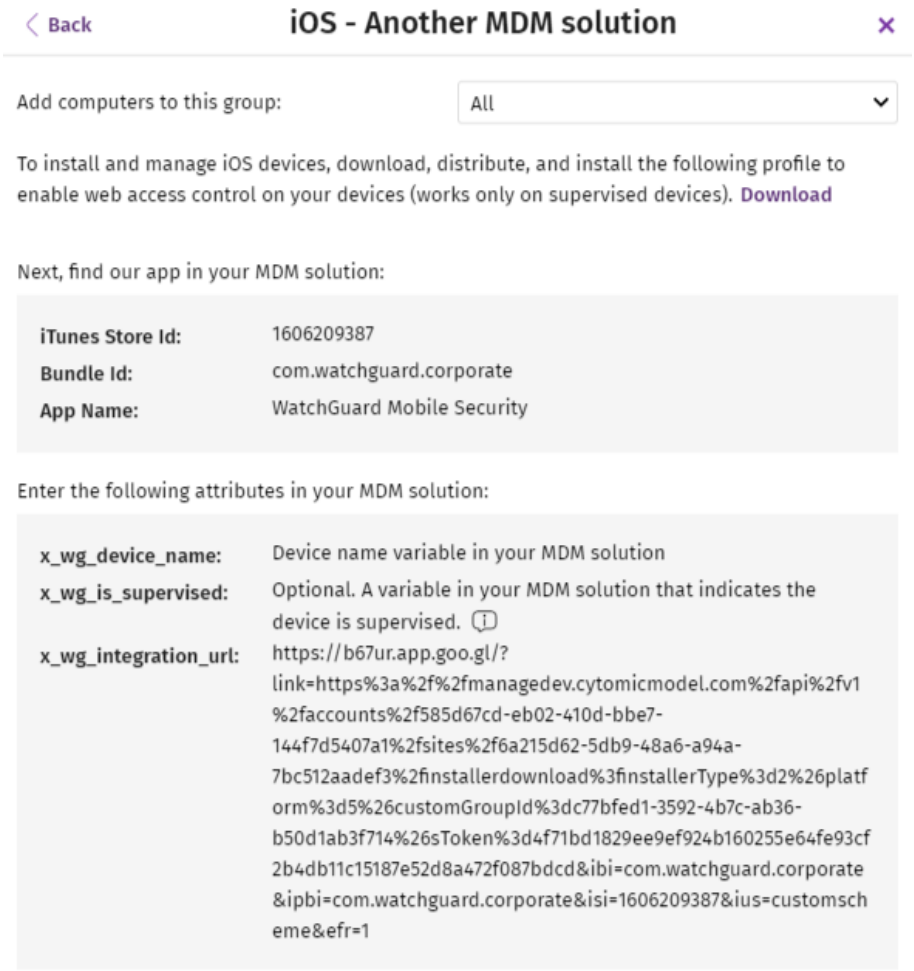


Figure 5.15: Window with the integration parameters for the third-party MDM solution

- Click the **Download** link to get the profile that will set **WatchGuard Mobile Security** as the app configured to filter web traffic on the target iOS devices. An XML file with the .mobileconfig

extension downloads to your computer.

- Import the .mobileconfig file into the third-party MDM solution and push it to the iOS devices where you want to enable URL filtering.
- In the third-party MDM solution, import the **WatchGuard Mobile Security** app directly from the Apple Store. To do this, use the **iTunes Store Id**, **Bundle Id**, or **App Name** fields in figure **Figure 5.15:** , or the search features included in the MDM solution.
- Associate and define the parameters **x_wg_device_name**, **x_wg_integration_url**, and **x_wg_is_supervised** in the **WatchGuard Mobile Security** app imported into the third-party MDM solution repository. The information contained in these parameters is sent along with the **WatchGuard Mobile Security** app when you push the app to the devices managed with the MDM solution.
    - **x_wg_device_name**: Contains the device name that will be shown in the Advanced EPDR console. In the **x_wg_device_name** parameter, enter the variable used by the MDM solution to represent the name of the device that will receive the **WatchGuard Mobile Security** app.
    - **x_ wg_ integration_ url**: Contains the URL that points to the information that **WatchGuard Mobile Security** needs to integrate into the group chosen by the Advanced EPDR administrator. Copy the content of the **x_ wg_ integration_ url** attribute shown in the Advanced EPDR console to the parameter defined in the MDM solution.
    - **x_wg_is_supervised**: Tells **WatchGuard Mobile Security** whether the device where it is going to be installed is supervised or not. If your MDM solution has a variable that enables you to dynamically set the content of this parameter, add it. Otherwise, do not add the parameter. **WatchGuard Mobile Security** will try to determine on its own whether it is running on a managed device or not.

Each MDM solution uses different variable names and syntaxes. See your product documentation for this information.

*Use variables with the x_wg_device_name and x_wg_is_supervised parameters. If, instead of the variable that represents the device name, you enter a device name, all the mobile devices that receive **WatchGuard Mobile Security** will be shown with the same name in the Advanced EPDR console.*

- Push the **WatchGuard Mobile Security** app from the MDM solution to the devices that you want to protect. After a few minures, the app is installed silently.

- After the app is installed, tap it to run it for the first time. The message **"WatchGuard Mobile Security" Would Like to Send You Notifications** appears.
- Tap the **Allow** button. The device is added to the Advanced EPDR console and the configuration process is complete.

Configuring an iOS device in supervised mode without loss of data

The following procedure for creating a backup and restoring it later is not officially supported by Apple. For this reason, we recommend that you run it first in a test environment before you apply it to your company's mobile phones.

Determine whether you need to create a manual backup

When you configure an iOS device in supervised mode, you reset it to factory-default settings. As a result, all apps and data stored on the device by the user are lost. To avoid this, you must use a backup and restore method that will vary based on the type of data stored and the backup software used:

- **iCloud**: If the user uses Apple's cloud storage service, it is very likely that you will not need to create any backups manually; in this case, their documents, photos, and other items are not stored on the mobile device but are automatically stored in the cloud. After the device has been formatted and placed in supervised mode, the user simply has to use their Apple ID to regain access to all their information.

To verify whether iCloud stores in the cloud all the types of data you want to recover after having enabled supervised mode, see ***https://support.apple.com/en-us/HT207428****. If iCloud does not store all the types of data you want to keep, use the Finder app as explained in this article.*

- **Finder**: If the user does not use iCloud or wants to keep apps or types of data not supported by Apple's cloud, you must create a backup of the mobile device by following a very specific protocol. This is required because Finder also stores the device state in the backup, so, when you restore the device data, you also restore the previous, non-supervised state of the device.

Finder does not store the settings of all the apps that exist on Apple Store. As a previous step, check whether the apps installed on the user's device will require manual configuration after the restore process is performed.

Requirements for creating a backup using Finder

- A macOS computer with the Catalina operating system or higher and the Finder app.
- The user's iPhone that you want to supervise.
- A secondary iPhone with the same operating system version as the user's iPhone.
- A lightning to USB cable.

Creating and restoring the backup

Back up the user's iPhone

- On the user's mobile phone, disable **Find My iPhone**:
    - Tap **Settings**.
    - Tap the user's name. Tap **Find My**.
    - Tap **Find My iPhone**, then tap to disable it.
    - Enter the Apple ID password.
    - Tap **Turn off**.
- Open the **Finder** app. Connect the user's iPhone to the macOS computer.
- If you are prompted to enter the device code or confirm that you trust the macOS computer, follow the on-screen instructions.
- In the left panel of the Finder, click the user's iPhone.
- On the **General** tab, select **Back up all the data on your iPhone to this Mac**.
- Click the **Back Up Now** button.
- When the process is complete, make a note of the exact time the backup was created.

Restore the user's iPhone backup to the secondary iPhone

- Disable **Find My iPhone** on the secondary mobile phone:
    - Tap **Settings**.
    - Tap the phone name. Tap **Find My**.
    - Tap **Find My iPhone**, then tap to disable it.

- Enter the Apple ID password.
- Tap **Turn off**.

- Disconnect the user's iPhone and connect the secondary iPhone to the macOS computer.
- If you are prompted to enter the device code or confirm that you trust the macOS computer, follow the on-screen instructions.
- In the left panel of the Finder, click the secondary iPhone.
- On the **General** tab, select **Restore Backup**.
- Select the backup that you created earlier. You can identify the backup by its timestamp.

Back up the secondary iPhone

- Verify that **Find My iPhone** is disabled on the secondary mobile phone. If it is not disabled:
  - Tap **Settings**.
  - Tap the phone name. Tap **Find My**.
  - Tap **Find My iPhone**, then tap to disable it.
  - Enter the Apple ID password.
  - Tap **Turn off**.
- In the left panel of the Finder, click the secondary iPhone.
- On the **General** tab, select **Back up all the data on your iPhone to this Mac**.
- Click the **Back Up Now** button.
- When the process is complete, make a note of the exact time the backup was created.

Restore the secondary iPhone backup to the user's iPhone

- Verify that **Find My iPhone** is disabled on the user's mobile phone. If it is not disabled:
  - Tap **Settings**.
  - Tap the user's name. Tap **Find My**.
  - Tap **Find My iPhone**, then tap to disable it.
  - Enter the Apple ID password.
  - Tap **Turn off**.
- Disconnect the secondary iPhone and connect the user's iPhone to the macOS computer.
- If you are prompted to enter the device code or confirm that you trust the macOS computer, follow the on-screen instructions.
- In the left panel of the Finder, click the user's iPhone.
- On the **General** tab, select **Restore Backup**.
- Select the backup that you created earlier. You can identify the backup by its timestamp.

- When the process is complete, a **Hello** screen is displayed on the user's iPhone. At this point, it is very important that you do not perform any actions on the device and start the process to put it in supervised mode. See **Configuring the device in supervised mode and enrolling it into the Cytomic MDM solution**.

Managing the Apple ID and digital certificates

Creating an Apple ID

- Open a supported web browser and go to **https://appleid.apple.com/account**. The **Create Your Apple ID** page opens.
- Fill in the form. You must specify an email account and the phone number of the device that will be used to verify the certificate request (usually, this is the device assigned to the Advanced EPDR administrator). Click **Continue**. You will receive a message with a verification code at the email address provided in the form.
- Enter the verification code in the form. Click **Continue**. You will receive a new code by SMS at the phone number provided in the form.
- Enter the SMS code. Click **Continue**. The process is complete and the dashboard associated with the newly created account opens. This dashboard enables you to manage your account and see all certificates generated so far.

Creating and importing the digital certificate into the Advanced EPDR console

To integrate iOS devices into Advanced EPDR using the Cytomic MDM solution, you must generate a digital certificate that ensures the confidentiality of communications with the Apple servers:

- Select the **Computers** menu at the top of the console. Click the **Add computers** button. A window opens with the platforms supported by Advanced EPDR.
- Click the **iOS** icon. If no certificate has been previously imported, a window opens with the procedure for creating a valid certificate.

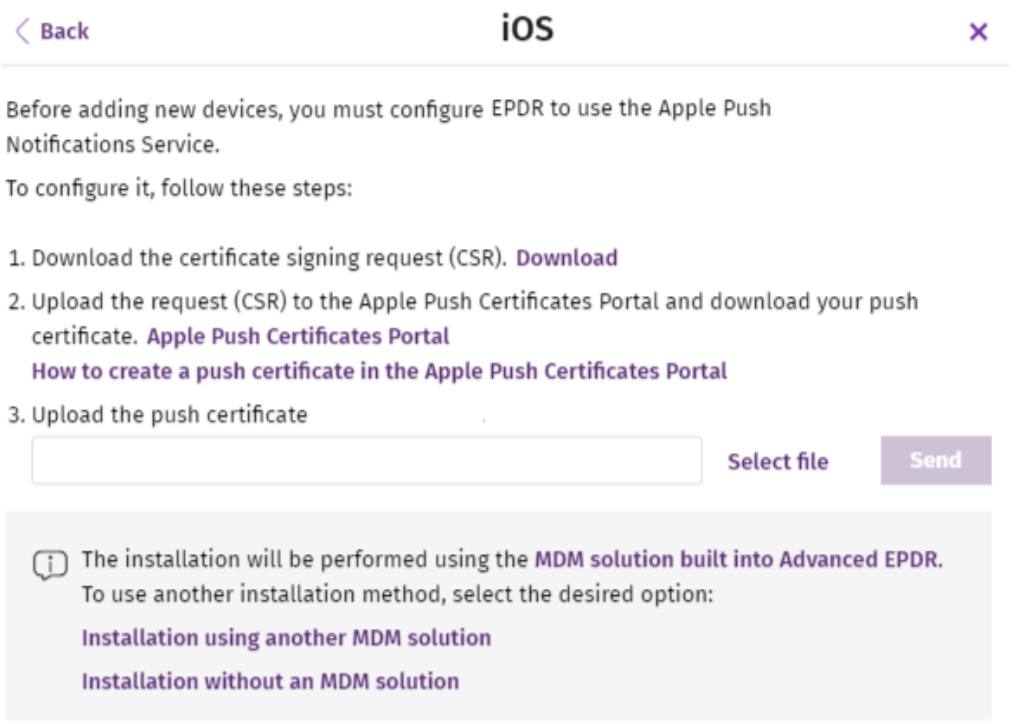


Figure 5.16: Window detailing the procedure for creating and importing an Apple digital certificate

- Click the **Download** link. The `apple_push.csr` file is downloaded. This file contains the signed certificate request encoded as Base64.
- Click the **Apple Push Certificates Portal** link. If you have previously logged in, the web browser opens the page for managing Apple digital certificates. Otherwise, enter your Apple ID credentials. See **Creating an Apple ID**.
- Click the **Create Certificate** icon. The **Terms of Use** page opens.
- Select **I have read and agree to these terms and conditions**. Click **Accept**. The **Create a New Push Certificate** page opens.
- Click **Choose File**. Select the `apple_push.csr` file you previously downloaded from the Advanced EPDR management console. Click **Upload**. A **Confirmation** page opens with information about the generated certificate. You will receive an informational email message.
- Click the **Download** button. The `MDM_ Panda Security, S.L._Certificate.pem` file is downloaded. This file contains the digital certificate.
- In the Advanced EPDR management console, click the **Select file** link. Choose the `MDM_ Panda Security, S.L._Certificate.pem` file you downloaded from the Apple portal. The **iOS** window appears, with the ID and expiration date of the imported certificate.

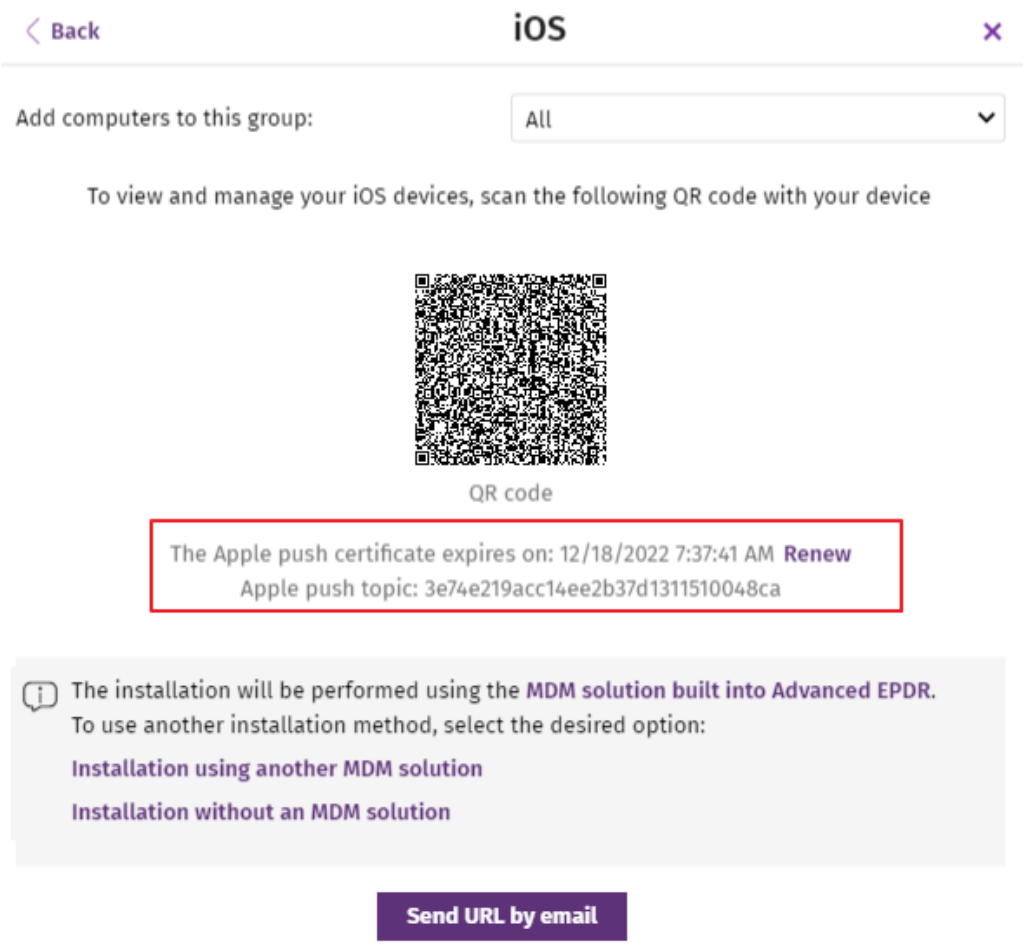


Figure 5.17: Window with information about the uploaded digital certificate

Renewing the Apple certificate

Apple certificates are valid for one year, after which they expire.

> *Renew your Apple certificate well before its expiration date. If your certificate expires, you will no longer be able to manage your devices from the Advanced EPDR management console. You will have to generate a certificate again and reintegrate all of your company's iOS devices.*

- Go to **https://identity.apple.com/pushcert/** and log in using your Apple ID credentials (see **Creating an Apple ID**). The **Certificates for Third-Party Servers** page opens.

Figure 5.18: **Certificates for Third-Party Servers** page

- Click the **Renew** button associated with the certificate in use. The **Renew Push Certificate** page opens.
- Click **Choose File**. Choose the `apple_push.csr` file. If the file is no longer available, you can create a new one. See **Creating and importing the digital certificate into the Advanced EPDR console**.
- Click the **Upload** button. The **Confirmation** page opens.
- Click the **Download** button. The updated certificate is downloaded.
- Select the **Computers** menu at the top of the Advanced EPDR management console. Click the **Add computers** button. A window opens with all platforms supported by Advanced EPDR.
- Click the **iOS** icon. A window opens with information about the previously uploaded certificate.
- Click **Renew**. The **iOS** window opens, with the certificate expiration date and ID (Apple Push Topic).
- Click the **Select file** link. Choose the `apple_push.csr` file you used when you first created the certificate. If the file is no longer available, you can download a new file from the Advanced EPDR management console. See **Creating and importing the digital certificate into the Advanced EPDR console**.
- Click the **Send** button. The **iOS** window opens, with an updated expiration date for the certificate.

Checking the expiration date of a certificate

- Select the **Computers** menu at the top of the console. Click the **Add computers** button. A window opens with the platforms supported by Advanced EPDR.
- Click the **iOS** icon. If a certificate has been previously imported, its data is shown.
- If the certificate is expired, a warning message is shown.

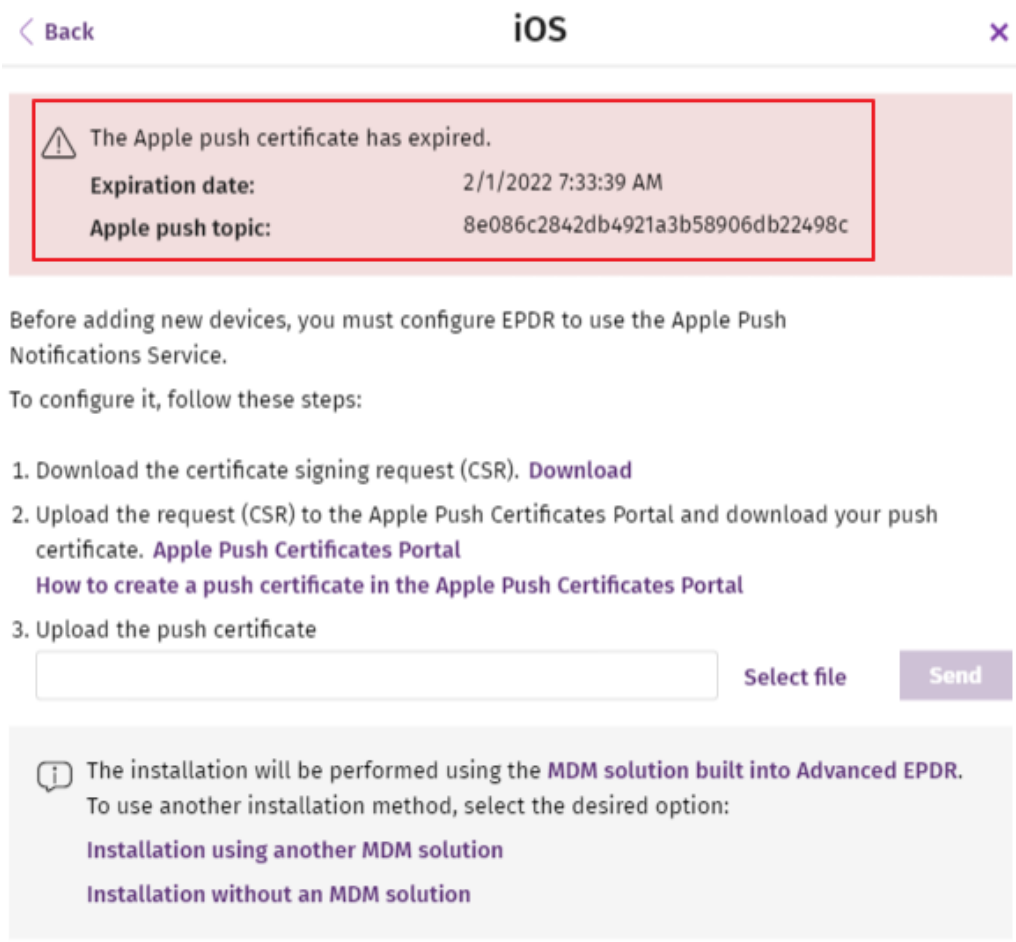


Figure 5.19: Window with information about an expired digital certificate

Checking deployment

There are three complementary ways in which you can check the result of the Advanced EPDR software deployment operation across the managed network:

- Using the **Protection status** widget. See **Protection status** on page **662** for more information.
- Using the **Computer protection status** list. See **Computer protection status** on page **683** for more information.
- Using the Event Viewer Application log on Windows computers.

Windows Event Viewer

The Application log in the Event Viewer provides extended information about the result of the installation of the agent on the user's computer and how it works after it is installed. The table below shows the information provided by Advanced EPDR in each field of the Event Viewer.

Message	Level	Category	ID
The device %deviceId% was unregistered	Warning	Registration (1)	101
The device %deviceId% was registered	Information	Registration (1)	101
A new SiteId %SiteId% was set	Warning	Registration (1)	102
Error %error%: Cannot change SiteId	Error	Registration (1)	102
Error %error%: Calling %method%	Error	Registration (1)	103
Error %code%: Registering device, %description%	Error	Registration (1)	103
Installation success of %fullPath% with parameters %parameters%	Information	Installation (2)	201
A reboot is required after installing %fullPath% with parameters %parameters%	Warning	Installation (2)	201
Error %error%: executing %fullPath% with parameters %parameters%	Error	Installation (2)	201
Message: %Module% installer error with following data: (optional) Extended code: %code% (optional) Extended subcode: %subCode% (optional) Error description: %description% (optional) The generic uninstaller should be launched (optional) Detected AV: Name = %name%, Version = %version%	Error	Installation (2)	202
Uninstallation success of product with code %productCode% and parameters %parameters%	Information	Uninstallation (4)	401
A reboot is required after uninstalling product with code %productCode% and	Warning	Uninstallation (4)	401

Message	Level	Category	ID
parameters %parameters%			
Error %error%: Uninstalling product with code %productCode% and parameters %parameters%	Error	Uninstallation (4)	401
Uninstallation of product with code %productCode% and command-line parameters %commandLine% was executed	Information	Uninstallation (4)	401
Error %error%: Uninstalling product with code %productCode% and command-line parameters %commandLine%	Error	Uninstallation (4)	401
Error %error%: Uninstalling product with code %productCode% and command-line parameters %commandLine%	Error	Uninstallation (4)	401
Generic uninstaller executed: %commandLine%	Information	Uninstallation (4)	402
Error %error%: Generic uninstaller executed %commandLine%	Error	Uninstallation (4)	402
Configuration success of product with code %productCode% and command-line parameters %commandLine%	Information	Repair (3)	301
A reboot is required after configuring product with code %productCode% and command-line parameters %commandLine%	Warning	Repair (3)	301
Error %error%: Configuring product with code %productCode% and command-line parameters %commandLine%	Error	Repair (3)	301

Table 5.9: Agent installation result codes in the Event Viewer

Automatic deletion of computers

This feature releases the security software license from protected computers and removes them from the console. Computers whose license you want to release must meet certain conditions defined in a filter you must create before enabling the feature. After you have created the filter, it is applied periodically.

Required permissions

Automatic deletion of computers is visible to all users of the web console. However, to configure and modify this feature, the user must have full visibility into all computers and the **Add, discover, and delete computers** permission.

For more information, see **Understanding permissions** on page **72**.

Consequences of deleting computers

Computers are deleted once a day, between 01:00 AM and 03:00 AM UTC.

When you delete a computer:

- The computer and all its information are deleted from the console.
- The computer is unprotected.
- If the computer was encrypted, it remains encrypted but you cannot get the recovery keys.

We recommend that you turn off a computer after it is deleted. Otherwise, it will reappear in the web console as soon as it reconnects to the Cytomic servers.

The information generated by a protected computer is not permanently deleted from the Advanced EPDR servers: If you reassign a license to the computer and it reconnects to the Cytomic server, all its information reappears in the web console. Nevertheless, if the filter is not disabled, the computer will be deleted again the next day.

Creating a filter to delete computers

For more information about all items available to configure a filter, see **Configuring filters** on page **218**.

Note that, because this is a feature for deleting computers, we recommend that the filter name be as easy to identify as possible.

To create a filter that finds computers not connected to the Cytomic server, use the following parameters:

- **Category**: Computer
- **Property**: Last connection
- **Operator:**
    - Is between (finds computers not connected to the server between two specific dates)
    - Before (finds computers not connected to the server before a specific date)
    - After (finds computers not connected to the server after a specific date)

Enabling the feature

- Select the **Settings** menu at the top of the console. Select **Computer maintenance** from the side menu.
- Click the **Enable automatic deletion of computers** toggle.
- From the drop-down menu, select the filter you want to apply.
- Click **Save changes**.

You cannot modify or delete the filter during its execution.

Scheduled reports of the computers to be deleted

You can schedule the automatic sending of a periodic report containing a list of computers to be deleted. See **Accessing the sending of reports and lists** on page **867**

Uninstalling the software

You can uninstall the Advanced EPDR software manually from the control panel of the operating system on each computer, or you can uninstall remotely from the security software management console.

Manual uninstallation

End users can manually uninstall the security software, if the administrator has not configured an uninstallation password in the security settings profile applied to the computer. If an uninstallation password is required, the end user requires authorization or the necessary credentials to uninstall the software.

To set or delete the agent uninstallation password, see ***Configuring security against protection tampering*** *on page* ***321***.

When you install Advanced EPDR, multiple applications are installed, based on the platform:

- **Windows and macOS computers**: Agent and endpoint security product.
- **Linux computers**: Agent, endpoint security product, and kernel module.
- **Android devices**: Endpoint security product.
- **iOS devices**: Endpoint security product and MDM solution management profile.

To completely uninstall Advanced EPDR, you must remove all modules. If you only uninstall the security product, the agent will install it again.

On a Windows 8 or later device

- Control Panel > Programs > Uninstall a program.
- Alternatively, type 'uninstall a program' at the Windows Start screen.

On a Windows Vista, Windows 7, Windows Server 2003, or later device

As of 30 September 2024, you cannot add devices to the management console or install the protection software on new computers that run these operating system versions: Windows XP, Windows Vista, Windows Server 2003, or Windows Server 2008 (Windows 2008 R2 will continue to be supported). Existing computers in the management console are still protected. See ***https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.***

- Control Panel > Programs and Features > Uninstall or change a program.

On a Windows XP device

- Control Panel > Add or remove programs.

Uninstallation using the uninstallation tool

On Windows computers, during the uninstallation process, some files or libraries might not be completely removed and cause errors. You can use a Cytomic tool to completely uninstall the agent and protection.

> *The uninstallation process can take a few minutes. When it is complete, restart the computer.*

Follow these steps:

- Download and unzip the file **GU.zip** (Password: panda).
- Run the agent removal file `GU_AGENT.exe`. Restart the computer.
- Run the protection removal file `GU_PROT.exe`. Restart the computer.

On a macOS device

> *Support for macOS Yosemite, El Capitan, Sierra, High Sierra, and Mojave is only available for customers who purchased Advanced EPDR version 4.30 / 9.30 or earlier.*

- Open Terminal Finder > Applications > Utilities > Terminal.
- To uninstall the protection software, run this command: `sudo sh /Applications/Endpoint-Protection.app/Contents/uninstall.sh`
- To uninstall the agent, run this command: `sudo sh /Applications/Management-Agent.app/Contents/uninstall.sh`

On an Android device

- Go to Settings > Security > Device Administrators.
- Clear the Advanced EPDR checkbox. Tap Disable > OK.
- In Settings, tap Apps. Tap Advanced EPDR > Uninstall > OK.

On an iOS device when it is not integrated with an MDM solution

- On the Home screen, press and hold the WatchGuard Mobile Security app.
- Tap the "-" icon on the WatchGuard Mobile Security app. The **Delete WatchGuard Mobile Security** dialog box opens.

- Tap **Delete app**. The **Do you want to delete WatchGuard Mobile Security?** dialog box opens.
- Tap **Delete**. The app is removed from the device.

On an iOS device when it is integrated with the Cytomic MDM solution

- On the Home screen, tap **Settings**. The **Settings** app opens.
- From the side panel, tap **General**. The **General** page opens.
- Tap **VPN and device management**. The **WatchGuard MDM Service** downloaded profile opens.
- Tap **Remove management**. The **Remove management** window opens.
- Tap **Remove**. The management profile is removed. The WatchGuard Mobile Security app is also removed.

On an iOS device when it is integrated with a third-party MDM solution

If your WatchGuard Mobile Security app is installed on an iOS device and it is integrated with a third-party MDM solution, we recommend that you uninstall the WatchGuard Mobile Security app from the third-party MDM solution. If you delete the management profile manually from the device, all the software that was installed with the MDM solution is also lost. The device can no longer be centrally managed from the MDM solution.

On a Linux device

On Linux, use the desktop environment to manage the packages included in the distribution.

- **Fedora**: Activities > Software > Installed
- **Ubuntu**: Ubuntu software> Installed

We recommend that you use the command line as `root` to uninstall the product. Use the `--totp` parameter if two-factor authentication is enabled, and `--pass` if agent uninstallation is password protected. See **Configuring security against protection tampering** on page **321**.

```
$ /usr/local/management-agent/repositories/pa/install --remove --
totp=value

(uninstalls the security software)

$ /usr/local/management-agent/repositories/ma/install --remove --
pass="password" --totp=value

(uninstalls the agent and repositories)
```

Manual uninstallation result

When you uninstall the Advanced EPDR software (Cytomic agent and protection) from a computer, all data associated with the computer disappears from the management console.

When you reinstall the Advanced EPDR software, the associated data and counters are restored.

Uninstallation from the management console

> *Remote uninstallation of the security software is not supported for computers that run macOS Catalina or Big Sur. In these instances, you must uninstall the software directly on the target computer.*

To uninstall the security software from Windows, Linux, or macOS computers from the management console:

- Go to the **Computers** menu (or the **Licenses** or **Computer protection status** lists). Select the checkboxes for the computers that you want to uninstall the security software from.
- From the action bar, select **Delete**. A confirmation dialog box opens.
- In the confirmation dialog box, select the **Uninstall the Cytomic agent from the selected computers** checkbox to completely remove the Advanced EPDR software.
- To complete uninstallation on macOS computers, the security software prompts the local user of the device for the password of an account with administrative privileges.

Remote reinstallation

To resolve a situation when Advanced EPDR does not run correctly on a workstation or server, you can reinstall it remotely from the management console.

You must reinstall the agent and the protection module separately.

Remote reinstallation requirements

- The target computer must be a Windows workstation or server.
- A computer with the discovery computer role must exist on the same network segment as the computer you want to reinstall software on. The discovery computer and Cytomic server can communicate.
- You have local admin or domain admin account credentials.

Accessing the feature

You can access this feature from any of the lists below. To access these lists, from the top menu, select **Status**. From the side menu, click the **Add** link:

- **Computer protection status** on page **683**.
- **Patch management status** on page **478**.
- **Cytomic Data Watch status** on page **409**.
- **Encryption status** on page **563**.
- **Licenses module lists** on page **196**.
- **Hardware** on page **243**.

Alternatively, to access this feature, from the top menu, select **Computers**. On the **Computers** page, click a branch in the folder or filter tree in the side panel.

> *The **Reinstall protection (requires restart)** and **Reinstall agent** options appear only for Windows computers.*

Identifying unprotected computers

Use the **Unmanaged computers discovered** list to find computers and servers on the network that need to have software reinstalled. See **Viewing discovered computers**.

Reinstalling the software on a single computer

- Use the list to find a computer that needs to have software reinstalled.
- From the computer context menu, select **Reinstall protection (requires restart)** or **Reinstall agent**. A dialog box opens where you can configure the reinstallation options. See **Reinstall protection dialog box** and **Reinstall agent dialog box**.

Reinstalling the software on multiple computers

- Use the checkboxes to select the computers that need to have the security software or the agent reinstalled.
- From the toolbar, select **Reinstall protection (requires restart)** or **Reinstall agent**. A dialog box opens where you can configure the reinstallation options. See **Reinstall protection dialog box** and **Reinstall agent dialog box**.

Reinstall protection dialog box

When you choose to reinstall a computer security software, a dialog box opens that shows these two options:

- **Reinstall the protection immediately (requires restart)**: The software reinstalls after one minute. If the target computer is not available (offline), the restart command remains active

for 1 hour.

- **Delay reinstallation for a certain time**: The software reinstalls after the amount of time you select (5 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, or 8 hours). If the target computer is not available (offline), the restart command remains active for 7 days.

The computer user receives a message to restart the computer immediately or wait until the time configured by the administrator. After the wait period expires, the software is uninstalled, and the computer restarts automatically to reinstall the software.

If an error occurs during the process, Advanced EPDR launches an uninstaller in the background in order to retry the operation and remove any traces of the previous installation. This might require an additional restart.

Reinstall agent dialog box

When you choose to reinstall a computer agent, a dialog box opens that prompts you to enter this information:

Discovery computer from which the agent is reinstalled:

- Make sure the discovery computer is on the same network segment as the computer you want to reinstall the agent on.
- If the discovery computer is turned off, the request is queued until the computer becomes available again. Requests are queued for a maximum of one hour, after which time they are discarded.

Credentials for reinstalling the agent: Enter one or multiple installation credentials. Use the target computer's local or domain administrator account to complete the reinstallation.

After you have entered the information, the discovery computer takes these actions:

- Connects to the computer you want to reinstall the agent on.
- Uninstall the agent installed on the computer.
- Downloads a new agent preconfigured with the customer, group, and network settings assigned to the computer. The agent is copied to the computer and runs remotely.
- If an error occurs during the process, an uninstaller launches and, if needed, a message prompts the user to restart the computer.

Error codes

For information on software reinstallation errors, see **Protection software reinstallation errors** on page **261**.

Chapter 6

Licenses

To protect your network computers from cyberthreats, you must purchase a number of Advanced EPDR licenses equal to or greater than the number of workstations and servers to protect. Each Advanced EPDR license can be assigned to only one device at a given time.

Next is a description of how to manage your Advanced EPDR licenses: how to assign them to the computers on your network, release them, and check their status.

Chapter contents

Definitions and basic concepts

The following is a description of terms required to understand the graphs and data provided by Advanced EPDR to show the product's licensing status.

To purchase and/or renew licenses, contact your designated partner.

License contracts

The licenses purchased by a customer are grouped into license contracts. A license contract is a group of licenses with characteristics common to all of them:

- **Product type**: Advanced EPDR, Cytomic Encryption, Cytomic Patch, Advanced EPDR with Cytomic Insights, Advanced EPDR with Cytomic Data Watch, Advanced EPDR with Cytomic Insights and Cytomic Data Watch.
- **Contracted licenses**: The number of licenses in the license contract.
- **License type**: NFR, Trial, Commercial, Subscription.
- **Expiration date**: The date when all licenses in the license contract expire and the computers cease to be protected.

Computer status

From a licensing perspective, the computers on the network can have three statuses in Advanced EPDR:

- **Computer with a license**: The computer has a valid license in use.
- **Computer without a license**: The computer does not have a valid license in use, but is eligible to have one.
- **Excluded**: Computers for which it has been decided not to assign a license. These computers are not and will not be protected by Advanced EPDR, even if there are licenses unassigned. Nevertheless, they are displayed in the console and some management features are valid for them. To exclude a computer, you have to release its license manually.

It is important to distinguish between the number of computers without a license assigned (those which could have a license if there are any available), and the number of excluded computers (those which could not have a license, even if there are licenses available).

License status and groups

There are two possible statuses for contracted licenses:

- **Assigned**: This is a license used by a network computer.
- **Unassigned**: This is a license that is not being used by any computer on the network.

Additionally, licenses are separated into two groups according to their status:

- **Used licenses**: Includes all licenses assigned to computers.
- **Unused licenses**: Includes the licenses that are not assigned.

Types of licenses

- **Commercial licenses**: These are the standard Advanced EPDR licenses. A computer with an assigned commercial license benefits from the complete functionality of the product.
- **Trial licenses**: These licenses are free and valid for thirty days. A computer with an assigned trial license benefits temporarily from the product functionality.
- **NFR licenses**: Not For Resale licenses are for Cytomic partners and personnel. It is not permitted to sell these licenses, nor for them to be used by anyone other than Cytomic partners or personnel.
- **Subscription licenses**: These are licenses that have no expiration date. This is a 'pay-as-you-go' type of service.

Assigning licenses

You can assign licenses in two ways: manually and automatically.

For more information about the search tool, the folder tree, and the filter tree, see ***Managing computers and devices*** *on page* ***211****.*

Automatic assignment of licenses

After you install the Advanced EPDR software on a computer on the network, and provided there are unused licenses, the system assigns an unused license to the computer automatically.

Manual assignment of licenses

Follow these steps to manually assign a license to a computer on the network.

- From the top menu, select **Computers**. Find the computer or device you want to assign the license to. You can use the folder tree, the filter tree, or the search tool.

- Select the computer to open its details page.
- Select the **Details** tab. The **Licenses** section shows the **No licenses** status. Click the icon to assign an unused license to the computer automatically.

Releasing licenses

Just as with the license assignment process, you can release licenses in two ways: manually and automatically.

Automatic release

- When the Advanced EPDR software is uninstalled from a computer on the network, the system automatically recovers a license and returns it to the group of licenses available for use.
- Similarly, when a license contract expires, licenses are automatically released from computers in accordance with the process explained in the Withdrawal of expired licenses section.

Manual release

Manual release of a license previously assigned to a computer means the computer becomes 'excluded'. As such, even though there are licenses available, they are not assigned automatically to this computer.

Follow these steps to manually release a Advanced EPDR license:

- From the top menu, select **Computers**. Find the device whose license you want to release. You can use the folder tree, the filter tree, or the search tool.
- Select the computer to open its details page.
- Select the **Details** tab. The **Licenses** section shows the name of the product license assigned to the computer. Click the icon to release the license and send it back to the group of unused licenses.

Processes associated with license assignment

Case 1: Computers with assigned licenses and excluded computers

By default, each new computer added to the Cytomic platform is assigned a Advanced EPDR product license automatically, and as such acquires the **Computer with an assigned license** status. This process continues until the number of unused licenses reaches zero.

When a license is manually withdrawn from a computer, its status becomes that of **Excluded computer**. From this point on, the computer does not compete for automatic assignment of unassigned licenses.

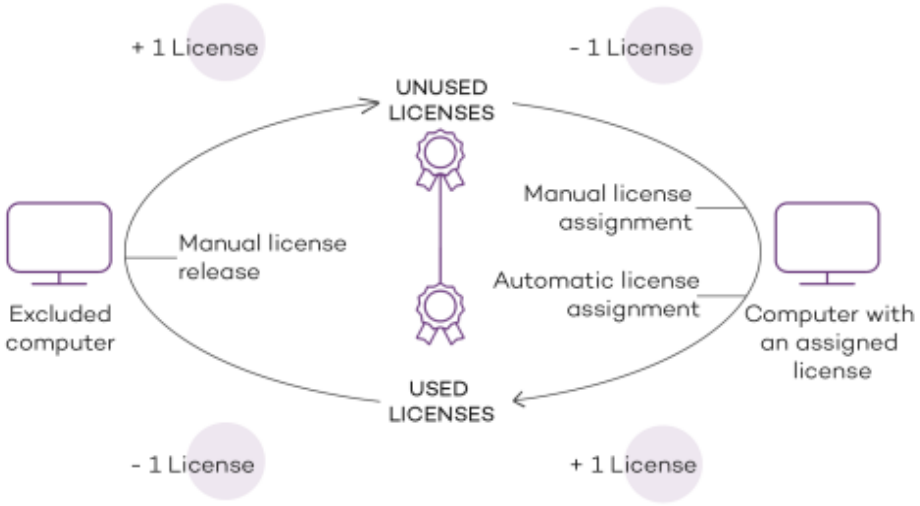


Figure 6.1: Modification of license groups with computers with licenses assigned and excluded computers

Case 2: Computers without an assigned license

As new computers are added to Cytomic and the pool of unused licenses reaches zero, these computers have the **Computers without a license** status. As new licenses become available, these computers are automatically assigned a license.

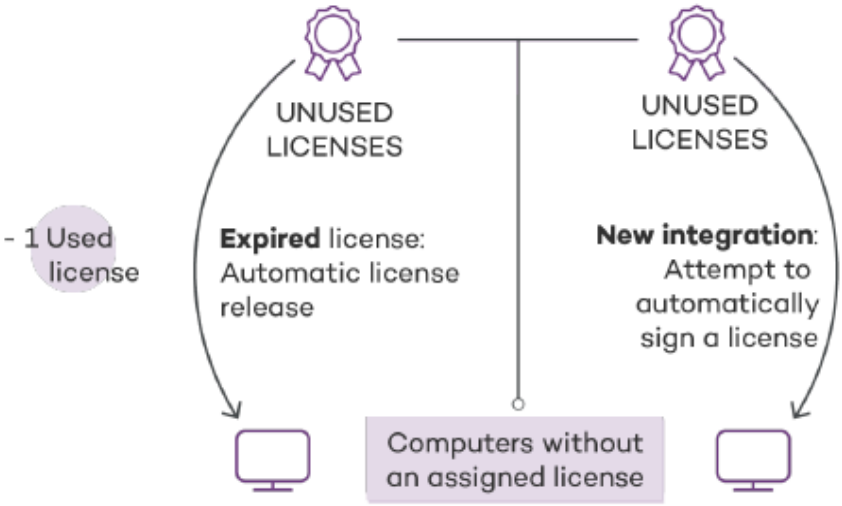


Figure 6.2: Computers without an assigned license due to expiration of the license contract and because the group of unused licenses was empty at the time of onboarding

Similarly, when an assigned license expires, the computer status is **No license** in accordance with the license expiration process explained in the Withdrawal of expired licenses section.

Licenses module panels/widgets

Accessing the dashboard

To access the dashboard, click the **Status** menu at the top of the console. Click **Licenses** from the side menu.

Required permissions

No additional permissions are required to access the widgets associated with the Licenses dashboard.

To see details of contracted licenses, click the **Status** menu at the top of the console. Click **Licenses** from the side menu. A page opens with two graphs (widgets): **Contracted licenses** and **License expiration**.

Licenses

The panel shows how the contracted product licenses are distributed.

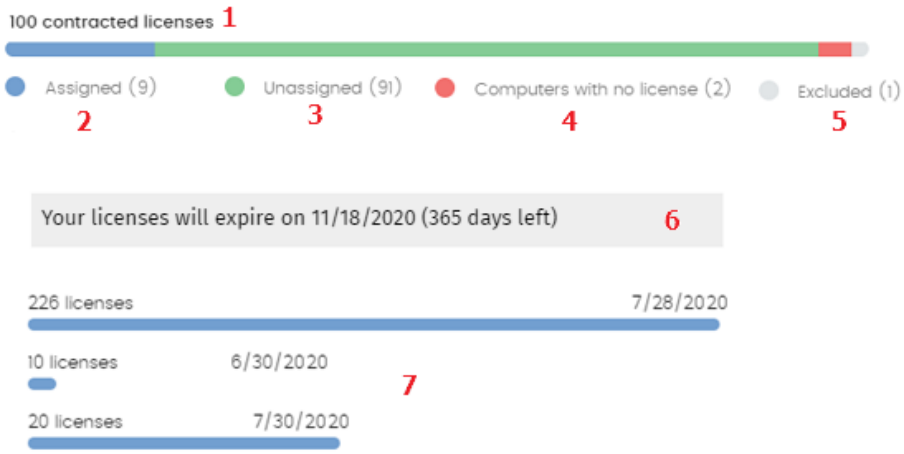


Figure 6.3: License panel with three license contracts

Meaning of the data displayed

Hotspot	Description
Total number of contracted licenses (1)	Maximum number of computers that can be protected if all the contracted licenses are assigned.
Number of assigned licenses (2)	Number of computers protected with an assigned license.

Hotspot	Description
Number of unassigned licenses (3)	Number of licenses contracted that have not been assigned to any computer and are therefore not being used.
Number of computers without a license (4)	Computers that are not protected as there are insufficient licenses. Licenses are assigned automatically as they are bought.
Number of excluded computers (5)	Computers without a license assigned and that are not eligible to have a license.
License expiration date (6)	If there is only one license contract, all licenses expire at the same time, on the specified date.
License contract expiration dates (7)	If one product has been contracted several times over a period of time, a horizontal bar chart is displayed with the licenses associated with each license contract and their expiration date.

Table 6.1: Description of the data displayed in the Licenses panel

Lists accessible from the panel

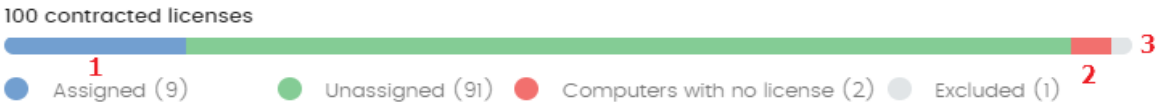


Figure 6.4: Hotspots in the Contracted licenses panel

Click the hotspots shown in the figure to open the **Licenses** list with the following predefined filters:

Filter field	Value
(1) License status	Assigned
(2) License status	No license

Filter field	Value
(3) License status	Excluded

Table 6.2: Filters available in the Licenses panel

Licenses module lists

Accessing the lists

You can access the lists in two ways:

- Click the **Status** menu at the top of the console. Click **Licenses** from the side menu. Click the relevant widget.

Or,

- Click the **Status** menu at the top of the console. Click the **Add** link from the side menu. A window opens with the available lists.
- Select the **Licenses** list from the **General** section to view the associated template. Edit it and click **Save**. The list is added to the side menu.

Required permissions

No additional permissions are required to access the **Licenses** list.

Licenses

Shows details of the licensing status of the computers on the network, with filters that help you locate desktops, laptops, servers, or mobile devices based on their licensing status.

Field	Description	Values
Computer	Computer name.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
License status	The computer's license status.	• Assigned • Computer without a license • Excluded

Field	Description	Values
Last connection	Date when the computer status was last sent to the Cytomic cloud.	Date

Table 6.3: Fields in the Licenses list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account that the product belongs to.	Character string
Computer type	Purpose of the computer within the organization's network	• Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS • Android
Active Directory	Path to the computer in the company's Active Directory.	Character string
Virtual machine	Indicates whether the computer is physical or virtual.	Boolean
Agent version	Internal version of the agent component that is part of the Advanced EPDR client software.	Character string
Protection version	Internal version of the protection component that is part of the Advanced EPDR client software.	Character string

Field	Description	Values
Last bootup date	Date when the computer was last booted.	Date
Installation date	Date when the Advanced EPDR software was successfully installed on the computer.	Date
Last connection date	Date when the computer status was last sent to the Cytomic cloud.	Date
License status	The computer's license status.	• Assigned • No license • Excluded
Group	Folder within the Cytomic folder tree the computer belongs to.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer.	Character string

Table 6.4: Fields in the Licenses exported file

Filter tool

Field	Description	Values
Search computer	Computer name.	Character string
Computer type	Purpose of the computer within the organization's network	• Workstation • Laptop • Server • Mobile device
Platform	Operating system installed on the computer.	• All

Field	Description	Values
		• Windows • Linux • macOS • Android
Last connection	Date when the Advanced EPDR status was last sent to the Cytomic cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago
License status	The computer's license status.	• Assigned • No license • Excluded

Table 6.5: Filters available in the Licenses list

Computer details page

Click any of the rows in the list to open the computer details page. See **Computer details** on page **252** for more information.

Expired licenses

Apart from subscription ones, all other license contracts have an expiration date assigned, after which the computers cease to be protected.

Behavior of Cytomic-based products when their licenses expire

Expiration of Cytomic-based products has a significant impact on affected computers, because:

- All protections configured for the computers are disabled.
- The signature file is no longer updated on the computers. The computers cannot access the collective intelligence databases.
- Scheduled tasks no longer run on the computers. You cannot run scheduled scans of the computers or install patches to update vulnerable programs.

Computers become very vulnerable to potential data leaks and dangerous infections, from PUPs (potentially unwanted programs), to ransomware and even APTs (advanced persistent threats) with multiple targets.

Seven-day grace period

To prevent this situation, Cytomic provides a seven-day grace period during which time devices remain protected while you renew their licenses.

Behavior when one of your license contracts expires

In cases where you have multiple license contracts, each for a number of licenses with a different expiration date, computers with licenses assigned do not belong to a particular license contract. Instead, all licenses from all license contracts are included in a single pool of available licenses, which are then distributed to the computers on your network.

When a license contract expires, Advanced EPDR determines the number of licenses assigned to that contract. Then, the solution sorts the computers on the network that have an assigned license by the **Last connection** field, which indicates the date the computer last connected to the Cytomic cloud.

Computers and devices that have been offline for the longest time lose their license and are unprotected.

Selecting which computers are the first to lose their license

Cytomic enables you to select which computers will lose their license before it expires.

To do that, you can:

- Remove computers from the console. The computer list management tools provides an option to remove computers. See **Management tools** on page **240**.
- Disable computers you do not want to protect but still want to manage from the console. For more information, see **Manual release**.

When you remove a computer from the console, make sure that you uninstall the agent. Otherwise, the next time the agent contacts the Advanced EPDR server, the computer is re-added to the console and takes up a license.

Advanced EPDR behavior after all licenses expire

From the time all licenses expire until the end of the seven-day grace period (day N to day N+7):

- You can access the console
- Protections continue to update and work correctly

After the grace period (day N+8) and for the next 83 days (day N+8 to day N+90), the license contract data is kept, but computers are unprotected. During this time:

- You cannot access the console
- All protections are disabled

Renewal within 90 days after license expiration

If licenses are renewed within 90 days after they expire:

- Device protection is automatically re-enabled and updated on devices connected to the Internet (usually within 4 hours).

Renewal more than 90 days after license expiration

Ninety days after your licenses expire (day N+90), the agent and the protections are automatically uninstalled. Additionally, the license contract data is deleted from the Cytomic databases.

If you renew the licenses, you must:

- Create users
- Reinstall the agent and the protections
- Create and assign all settings again

Expiration notifications

Thirty days before a license contract expires, the **Licenses** page shows a message indicating the remaining days and the number of licenses that are affected.

Additionally, you can see the license contracts that have expired during the last thirty days.

When all products and license contracts have expired, you can no longer access the management console.

Computer search based on license status

The Advanced EPDR filter tree enables you search for computers based on the status of their licenses.

*See **Creating and organizing filters** on page **216** for more information about how to create filters in Advanced EPDR.*

The properties of the **License** category are as follows (these properties enable you to create filters that generate lists of computers with specific licensing information):

Category	Property	Value	Description
License	Status	Create filters based on the following license statuses:	
		Assigned	Lists computers with a Advanced EPDR license assigned.
		Not assigned	Lists computers that do not have a Advanced EPDR license assigned.
		Unassigned manually	Lists computers whose Advanced EPDR license was manually released by the network administrator.
		Unassigned automatically	Lists computers whose Advanced EPDR license was automatically released by the system.

Table 6.6: Fields in the License filter

Chapter 7

Product updates and upgrades

Advanced EPDR is a cloud-based managed service that does not require network administrators to perform maintenance on the back-end infrastructure that supports it. However, administrators do need to update the client software installed on the computers on the network, and launch upgrades of the management console, when required.

Chapter contents

Updatable modules in the client software

The components installed on user computers are these:

- Cytomic Platform communications agent.
- Advanced EPDR protection engine.
- Signature file.

The update procedure and options vary depending on the operating system of the device to update, as indicated in **Table 7.1:** .

Module	Platform			
	Windows	macOS	Linux	Android
Cytomic agent	On demand			
Advanced EPDR protection	Configurable	Configurable	Configurable	No
Signature file	Enable/Disable	Enable/Disable	Enable/Disable	No

Table 7.1: Update procedures based on the client software component

- **On demand**: You can launch the update when you want, provided there is an update available, or postpone it for as long as you want.
- **Configurable**: You can configure update windows for future and recurrent updates, and disable them as well.
- **Enable/Disable**: You can enable and disable updates. If updates are enabled, they will run automatically when they are available.
- **No**: You cannot influence the update process. Updates run as soon as they are available, and you cannot disable them.

Protection engine updates

To configure protection engine updates, you must create and assign a **Per-computer settings** profile. To do this, select **Settings** in the top menu. In the left menu, select **Per-computer settings**.

Limits to downloading engine updates from cache and Cytomic proxy computers

You can download protection engine updates directly from the Internet or through a cache or Cytomic proxy computer. See **Configuring downloads from cache computers** on page **315** and **Configuring proxies lists for Internet access** on page **313**.

There are limitations to using one method or another, depending on the computer operating system:

- **Computers with a Windows or macOS operating system**: They can download installation packages from cache computers, proxy computers, and the Internet.

- **Computers with a Linux operating system**: They use the distribution's own package manager to perform downloads. Therefore, they cannot download installation packages through a cache or Advanced EPDR proxy computer.

Cache computers store installation packages until they are no longer valid, at which time they are deleted.

Updates

To enable automatic updates of the Advanced EPDR protection module, click the **Automatically update Advanced EPDR on devices** toggle. This enables all other configuration options on the page. If this option is disabled, the protection module will never be updated.

We recommend that you do not disable protection engine updates. A computer with out-of-date protection becomes more vulnerable to malware and advanced threats over time.

Running updates at specific time intervals

Configure these parameters for computers to run updates at specific time intervals:

- Start time
- End time

To run updates at any time, select **Anytime**.

Running updates on specific days

Use the drop-down menu to specify the days on which updates should be run:

- **Any day**: The updates will run when they are available. This option does not link Advanced EPDR updates to specific days.
- **Days of the week**: Use the checkboxes to select the days of the week on which the Advanced EPDR updates will run. If an update is available, it will run on the first day of the week that matches your selection.
- **Days of the month**: Use the drop-down menus to set a range of days of the month for the Advanced EPDR updates to take place. If an update is available, it will run on the first day of the month that matches your selection.
- **On the following days**: Use the drop-down menus to set a specific date range for the Advanced EPDR updates. This option enables you to select update intervals that will not repeat over time. After the specific date range, no updates will be run. This option forces you to constantly establish a new update interval as soon as the previous one expires.

Computer restart

Advanced EPDR enables you to define a logic for computer restarts, if needed, through the drop-down menu at the bottom of the settings page:

- **Do not restart automatically**: A restart dialog box on the target computer prompts the user to restart the computer. The dialog box continues to open until the computer restarts.
- **Automatically restart workstations only**.
- **Automatically restart servers only**.
- **Automatically restart both workstations and servers**.

Communications agent updates

The Cytomic agent is updated on demand. Advanced EPDR shows a notification in the management console every time a new agent version is available. After that, you can launch the update whenever you want.

Updating the Cytomic agent does not require restarting users' computers. These updates usually contain changes and improvements to the management console to facilitate security management.

Limits to downloading communications agent updates from cache and Cytomic proxy computers

You can download communications agent updates directly from the Internet or through a cache or Cytomic proxy computer. See **Configuring downloads from cache computers** on page **315** and **Configuring proxies lists for Internet access** on page **313**.

There are limitations to using one method or another, depending on the computer operating system:

- **Computers with a Windows or macOS operating system**: They can download installation packages from cache computers, proxy computers, and the Internet.
- **Computers with a Linux operating system**: They use the distribution's own package manager to perform downloads. Therefore, they cannot download installation packages through a cache or Cytomic proxy computer.

Cache computers store installation packages until they are no longer valid, at which time they are deleted.

Knowledge updates

To configure updates of the Advanced EPDR signature file, you must edit the security settings of the device type in question.

Knowledge downloads from cache and Cytomic proxy computers

Computers with a Windows, macOS, or Linux operating system can download knowledge directly from the Internet or through a cache or Cytomic proxy computer.

Cache computers store signature files until they are no longer valid, at which time they are deleted.

Windows, Linux, and macOS devices

In the top menu, select **Settings**. In the left menu, select **Workstations and servers**.

Go to **General**. These options are shown:

- **Automatic knowledge updates**: Enable or disable signature file downloads. If you clear this option, the signature file will never be updated.

We recommend that you do not disable automatic knowledge updates. A computer with out-of-date protection becomes more vulnerable to malware and advanced threats over time.

- **Run a background scan every time there is a knowledge update**: Runs a scan automatically whenever a signature file is downloaded to the computer. These scans have minimum priority so as not to interfere with the user work.

Android devices

In the top menu, select **Settings**. In the left menu, select **Mobile devices**.

Advanced EPDR enables you to restrict software updates so that they do not consume mobile data.

Select the **Only update over Wi-Fi** option to restrict updates to those occasions when there is an available Wi-Fi connection for the target smartphone or tablet.

Management console upgrades

Network administrators can choose when to start the process of upgrading the management console on the Cytomic servers. Otherwise, Cytomic automatically upgrades the management console to the latest available version.

To carry out this operation, the user account that accesses the web console must have the Full Control role. See **Full Control role** on page **70**.

Considerations prior to upgrading the console version

Although this is a process that takes place entirely on the Cytomic servers, upgrading the console version can push new versions of the security software to customer computers. This can result in traffic loads and the need to restart the computers on the network in some cases. To reduce traffic during upgrades, see "**Configuring downloads from cache computers** on page **315**".

Console upgrades are transparent to administrators. They do not affect the console operation. When the process completes, the console closes automatically. When you log in again, you access the upgraded version of the console.

Starting the management console upgrade

- In the upper-right corner of the top menu, click the **Web notifications** icon  . The unread notifications appear.
- If there is a console upgrade available, a message entitled **New management console version** is shown, along with the **New features and improvements** link, the version to which the console will be upgraded, and the **Upgrade console now** button. This type of notification cannot be deleted, as it does not show the  icon. See **Web notifications icon** on page **39**.

> *The **Upgrade console now** button is shown only if the user account used to access the management console has the Full Control role assigned to it.*

- After you click the button, the upgrade request is queued on the server, waiting to be processed. The maximum time the request remains queued on the server is 10 minutes.
- After the request has been processed, the upgrade process starts and the notification shows the text **Upgrade in progress**. If any user account tries to log in to the console, access is denied. For the duration of the upgrade process, you cannot log in to the management console.
- After some time, which depends on the number of managed computers and the data stored on the console, the upgrade process finishes.

Canceling the upgrade

- After the upgrade process has started, click the **Web notifications** icon  in the upper-right corner of the top menu. The unread notifications appear.
- If a console upgrade exists in the request queue that has not started yet, a message entitled **New management console version** is shown, along with the **New features and improvements** link and the **Cancel upgrade** button.

- To remove the upgrade request from the queue, click the **Cancel upgrade** button. The button disappears and the **Upgrade console now** button is shown again.

Chapter 8

Managing computers and devices

The web console shows managed devices in an organized and flexible way, enabling you to apply different strategies to rapidly find and manage them.

In order for a computer on the network to be managed through Advanced EPDR, the Cytomic agent must be installed on it. Computers without a license but with the Cytomic agent installed appear in the management console, although their protection is out of date and you cannot run scans or perform other tasks associated with the protection service on them.

Chapter contents

The Computers area

The **Computers** area in the web console enables you to manage all devices integrated into Advanced EPDR.

To access the computer management page, click the **Computers** menu at the top of the console. Two different areas are displayed: a side panel with the **Computer Tree (1)** and a center panel with the **list of computers (2)**. Both panels work together. When you select a branch in the computer tree, the computer list is updated with the computers assigned to that branch.

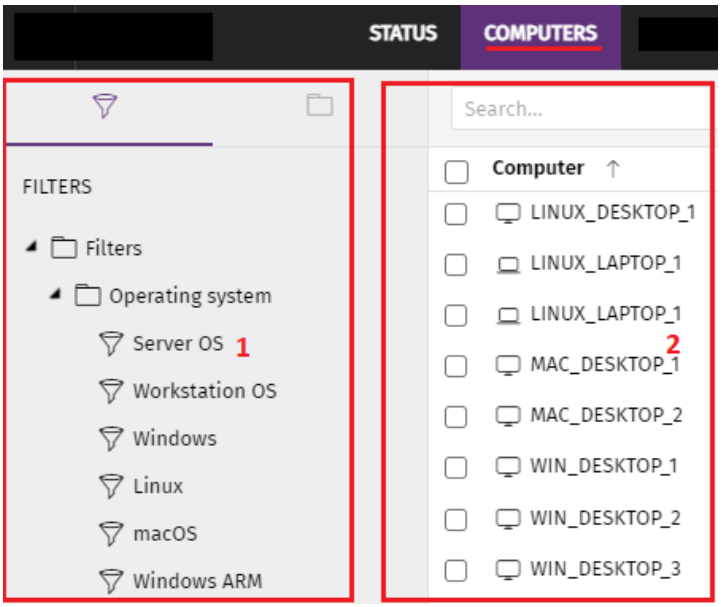


Figure 8.1: General view of the panels in the Computers area

Show computers in subgroups

You can restrict or expand the information displayed on the list of computers by using the **Show computers in subgroups** option accessible from the general context menu.

- If the option is selected, all computers in the selected branch and its corresponding sub-branches are displayed.
- If the option is cleared, only those computers that belong to the selected branch of the tree are displayed.

The Computer tree panel

Advanced EPDR displays the computers on the network through the **Computer tree (1)**, which provides two independent views or trees **(2)**:

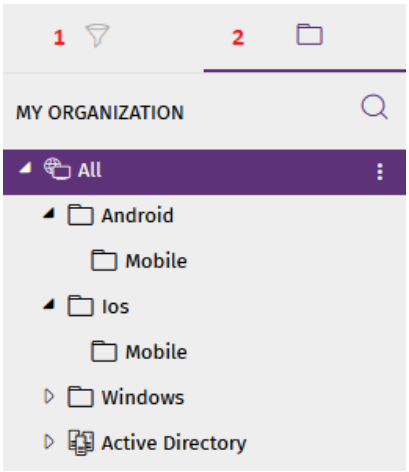


Figure 8.2: The Computer tree panel

- **Filter tree (1)**: Enables you to manage the computers on your network using dynamic groups. Computers are assigned to this type of group automatically.
- **Group tree (2)**: Enables you to manage the computers on your network through static groups. Computers are assigned to this type of group manually.

These two tree structures are designed to display devices in different ways, in order to facilitate different tasks such as:

- Find computers that fulfill certain criteria in terms of hardware, software, or security.
- Quickly assign security settings profiles.
- Take remediation actions on groups of computers.

For more information about how to find unprotected computers or those with certain security characteristics or protection status, see ***Malware and network visibility*** *on page* ***661****. For information about how to assign security settings profiles, see* ***Manual and automatic assignment of settings profiles*** *on page* ***296****. For more information about how to take remediation actions, see* ***Remediation tools*** *on page* ***877****.*

Point the mouse to the branches in the filter and group trees to display the context menu icon. Click it to display a pop-up menu with all available operations for the relevant branch.

Filter tree

The filter tree is one of the two computer tree views. It enables you to dynamically group computers on the network using rules and conditions that describe characteristics of devices, and logical operators that combine them to produce complex expressions.

The filter tree can be accessed from the left panel, by clicking the filter icon  . Clicking different items in the tree updates the right panel, presenting all the computers that meet the criteria established in the selected filter.

About filters

Filters are effectively dynamic groups of computers. A computer automatically belongs to a filter when it meets the criteria established for that filter by the administrator.

A computer can belong to more than one filter.

As such, a filter consists of a series of rules or conditions that computers have to satisfy in order to belong to it. As computers meet these conditions, they join the filter. Similarly, when the status of a computer changes and ceases to fulfill those conditions, it automatically ceases to belong to the group defined by the filter.

Filters can be grouped manually in folders using whatever criteria the administrator chooses.

Predefined filters

Advanced EPDR includes common filters that you can use to organize and locate network computers. You can edit or delete these predefined filters.

Cannot recover a predefined filter after you delete it.

Name	Group	Description
Server OS	Operating system	Lists computers with a server type operating system installed.
Workstation OS	Operating system	Lists computers with a workstation type operating system installed.
Windows	Operating system	Lists all computers with a Windows operating system installed.
Android	Operating system	Lists all devices with an Android operating system installed.
iOS	Operating system	Lists all devices with an Android operating system installed.
Linux	Operating system	Lists all computers with a Linux operating system installed.
macOS	Operating system	Lists all computers with a macOS operating system installed.
Windows ARM	Operating system	List all computers with Windows operating system and ARM microprocessor
Workstations and servers	System type	Lists physical workstations and servers.
Laptops	System type	Lists physical laptops.
Smartphones and tablets	System type	Lists smartphones and tablets.
Virtual machines	System type	Lists virtual machines.
<2GB of memory	Hardware	Lists computers with memory less than 2 GByte
Java	Software	Lists all computers with the Java JRE SDK installed.
Adobe Acrobat	Software	Lists all computers with Acrobat Reader installed.

Name	Group	Description
Reader		
Adobe Flash Player	Software	Lists all computers with the Flash Player plugin installed.
Google Chrome	Software	Lists all computers with the Chrome browser installed.
Mozilla Firefox	Software	Lists all computers with the Firefox browser installed.

Table 8.1: Predefined filter list

Creating and organizing filters

To create and organize filters, click the context menu icon next to a branch of your choice in the filter tree. A pop-up menu is displayed with the actions available for that particular branch.

Creating folders

- Click the context menu of the branch where you want to create the folder, and click **Add folder**.
- Enter the name of the folder and click **OK**.

You cannot add a folder below a filter. If you select a filter and then add a folder, the folder is added at the same level as the filter, in the same parent folder.

Creating filters

To create a filter, follow the steps below:

- Click the context menu of the folder where the filter will be created.
    - If you want to create a hierarchical structure of filters, create folders and move your filters to them. A folder can contain other folders with filters.
- Click **Add filter**.
- Type the name of the filter. It does not have to be a unique name. See **Configuring filters** for more information.

Deleting filters and folders

To delete a filter or a folder, click the context menu of the branch to delete, and click **Delete**. This deletes the folder and all of the filters in it.

You cannot delete the Filters root folder.

Moving and copying filters and folders

- Click the context menu of the branch you want to copy or move.
- Click **Move** or **Make a copy**. A pop-up window appears with the target filter tree.
- Select the target folder and click **OK**.

You cannot copy filter folders. Only filters can be copied.

Renaming filters and folders

- Click the context menu of the branch you want to rename.
- Click **Rename**.
- Type a new name.

You cannot rename the root folder. Additionally, to rename a filter you must edit it.

Searching for filters

In very large IT infrastructures, the filter tree can contain a large number of items. This makes finding specific filters difficult.

To find a filter:

- Click the  icon at the top of the filter tree. A text box appears.
- Type the letters of the name of the filter you want to find. All filters whose name starts with, ends with, or contains the character string entered are shown.
- After the search is complete, select the filter you wanted to find. Click the  icon. The full filter tree is shown again and the filter you searched for appears selected.

Configuring filters

To configure a filter, click its context menu and select **Edit filter** from the menu displayed. This opens the filter's settings window.

A filter consists of one or more rules, which are related to each other with the logical operators AND/OR. A computer is part of a filter if it meets the conditions specified in the filter rules.

A filter has four sections:

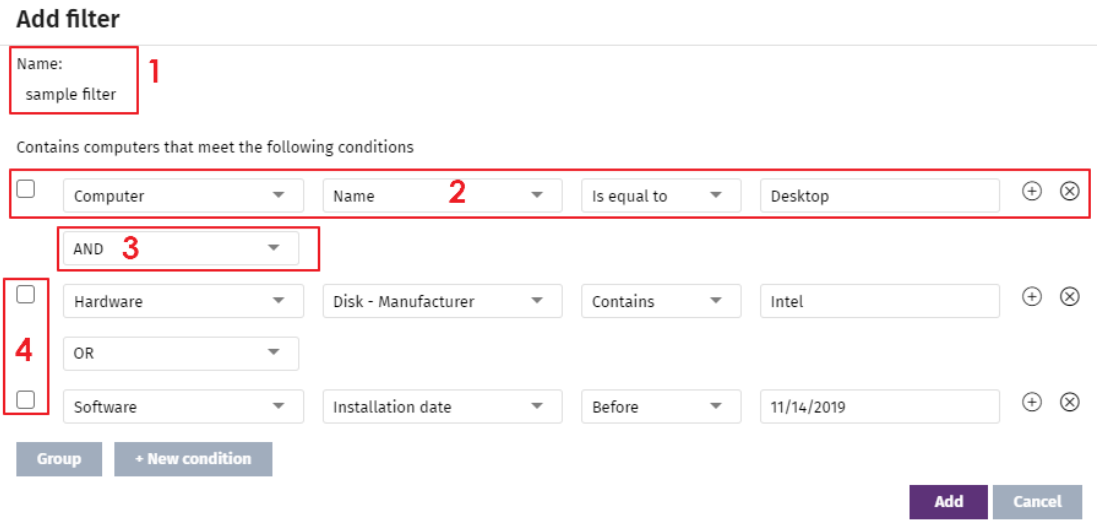


Figure 8.3: Filter settings overview

- **Filter name (1)**: Identifies the filter.
- **Filter rules (2)**: Enables you to set the conditions for belonging to a filter. A filter rule defines only one characteristic of the computers on the network.
- **Logical operators (3)**: Enable you to combine filter rules with the logical operators AND or OR.
- **Groupings (4)**: Enable you to change the order of the filter rules related with logical operators.

Filter rules

A filter rule consists of the items described below:

- **Category**: Groups the properties in sections to make it easy to find them.
- **Property**: The characteristic of a computer that determines whether or not it belongs to the filter.
- **Operator**: Determines the way in which the computer's characteristics are compared to the values set in the filter.
- **Value**: The content of the property. Depending on the type of property, the value field reflects entries such as 'date', etc.

To add rules to a filter, click the icon. To delete them, click .

Logical operators

To combine two rules in the same filter, use the logical operators AND and OR. This way, you can interrelate several rules. As soon as you add a rule to a filter, the options AND/OR automatically appear to establish the relation between the rules.

Filter rule groupings

In a logical expression, parentheses are used to change the order in which operators (in this case, the filter rules) are evaluated.

As such, to group two or more rules in a parenthesis, you must create a grouping by selecting the corresponding rules and clicking **Group conditions**. A thin line appears covering the filter rules that are part of the grouping.

The use of parentheses enables you to group operands at different levels in a logical expression.

Example filters

This topic includes examples of filters commonly created by network administrators:

Filter Windows computers based on the installed processor (x86, x64, ARM64)

Lists all computers that have a Windows operating system installed and an ARM microprocessor.

This filter has two conditions linked by the AND operator:

- **Condition 1**:
    - **Category**: Computer
    - **Property**: Platform
    - **Condition**: Is equal to
    - **Value**: Windows
- **Condition 2**:
    - **Category**: Computer
    - **Property**: Architecture
    - **Condition**: Is equal to
    - **Value**: {architecture name: ARM64, x86, x64}

Filter computers without a specific patch installed

Lists computers that do not have a specific patch installed. See **Cytomic Patch (Updating vulnerable programs)** on page **435** for more information about Cytomic Patch.

- **Category**: Software
- **Property**: Software name
- **Condition**: Doesn't contain
- **Value**: {Patch name}

Filter computers that have not connected to the Cytomic cloud in X days

Lists computers that have not connected to the Cytomic cloud in the specified period.

- **Category**: Computer
- **Property**: Last connection
- **Condition**: Before
- **Value**: {Date in dd/mm/yy format}

Filter computers that cannot connect to the Cytomic security intelligence services

Finds all computers that have problems connecting to any of the Cytomic security intelligence services. Create the following rules linked by the OR operator:

- **Rule**:
    - **Category**: Security
    - **Property**: Connection for sending events.
    - **Condition**: Is equal to
    - **Value**: With problems
- **Rule**:
    - **Category**: Security
    - **Property**: Connection for collective intelligence.
    - **Condition**: Is equal to
    - **Value**: With problems
- **Rule**:
    - **Category**: Security
    - **Property**: Connection for web protection.
    - **Condition**: Is equal to
    - **Value**: With problems

Filter isolated computers

Lists computers that have been isolated from the network. See **Computer isolation** on page **888** for more information.

- **Category**: Computer
- **Property**: Isolation status
- **Condition**: Is equal to
- **Value**: Isolated

Filter computers in RDP attack containment mode

Lists computers that have received a high number of RDP connection attempts which have started to be blocked by Advanced EPDR.

- **Category**: Computer
- **Property**: "RDP attack containment" mode
- **Condition**: Is equal to
- **Value**: True

Filter computers integrated with other management tools

Lists computers with a name that matches a computer name specified in a list obtained by a third-party tool. Each line in the list must end with a carriage return and is considered a computer name.

- **Category**: Computer
- **Property**: Name
- **Condition**: In
- **Value**: Computer name list

Filter computers not compatible with SHA-256 signed drivers

- **Category**: Computer
- **Property**: Supports SHA-256 signed drivers
- **Condition**: Is equal to
- **Value**: False

Computers with a public IP address

Lists computers that accessed the Internet through a device (router/proxy/VPN endpoint) that has the specified IP address.

- **Category**: Computer
- **Property**: Public IP address
- **Condition**: Is equal to (lists computers that accessed the Internet through a device with a specific IP address).

Computers discovered in Active Directory

Lists managed and unmanaged computers that have been discovered using Active Directory.

- **Category**: Computer
- **Property**: Last seen in Active Directory
- **Condition**: Is between (to list computers discovered between two specific dates).

Group tree

The group tree enables you to statically arrange the computers on the network in the groups that you choose.

To access the group tree, follow the steps below:

- Click the folder icon  from the left panel.
- By clicking the different branches in the tree, the panel on the right is updated, presenting all the computers in the selected group and its subgroups.

About groups

A group contains computers manually assigned by the administrator. The group tree enables you to create a structure with a number of levels comprising groups, subgroups, and computers.

The maximum number of levels in a group is 10.

Group types

Group type	Description
Root group 	This is the top group under which all other groups reside.
Native groups 	These are Advanced EPDR groups, some of which are predefined. These groups support all operations (such as move, rename, or delete) and can contain other groups and computers.

Group type	Description
IP-based groups	Native group with associated IPs or IP ranges to speed up integration of new computers in the security service.
Active Directory groups	These groups replicate your Active Directory structure. These groups do not support some operations. They can contain other Active Directory groups and computers..
Active Directory root group	This group contains all Active Directory domains configured on the organization's network.. It contains Active Directory domain groups.
Active Directory domain group	These groups are Active Directory branches that represent domains. They contain other Active Directory domain groups, Active Directory groups, and computers.

Table 8.2: Group types in Advanced EPDR

The size of the organization, the uniformity of the managed computers, and the presence or absence of an Active Directory server on the company network determines the structure of the group tree. The group structure may vary from a flat tree with a single level for the simplest cases, to a complex structure with several levels for large networks made up of highly heterogeneous computers.

Unlike filters, a computer can only belong to a single group.

Active Directory groups

For organizations with an Active Directory server, Advanced EPDR can automatically replicate the Active Directory structure on the My Organization tab. This works as follows: The Cytomic agent installed on each computer reports the Active Directory group it belongs to to the web console and, as agents are deployed, the tree is populated with the various organizational units. This way, the branch shows a structure familiar to you, helping you find and manage your computers faster.

To make sure the structure is consistent between Active Directory and the My Organization tab, you cannot modify Active Directory groups in Advanced EPDR. Advanced EPDR automatically updates Active Directory groups within one hour when you make changes to your Active Directory structure.

In Advanced EPDR, if you move a computer from an Active Directory group to a native group or to the root group, the synchronization relationship with Active Directory breaks. Any changes you make to Active Directory groups that affect the moved computer are not reflected in Advanced EPDR.

For information on how to reestablish the synchronization relationship between Active Directory and Advanced EPDR, see **Returning multiple computers to their Active Directory group**.

Creating and organizing groups

The actions you can take on groups are available through the pop-up menu displayed when clicking the context menu for the relevant branch in the group tree. The menu displayed shows the actions available for that particular branch.

Creating a group

- Click the context menu of the parent group to which the new group will belong, and click **Add group**.
- Type the name of the group in the **Name** text box and click the **Add** button.

You cannot create Active Directory groups from the group tree. The tree replicates the groups and organizational units that already exist on your Active Directory server.

To automatically assign computers to a group when you install the Advanced EPDR agent, you can specify the IP addresses or an IP address range for the group:

- Click the **Add IP-based automatic assignment rules** link. A text box is displayed for you to type the IP addresses of the computers to move to the group.
- You can enter individual IP addresses separated by commas, or IP address ranges separated by a dash.

Computers are added to the group when you install the Advanced EPDR agent. If the computer IP address changes, the computer remains in the original group.

Deleting groups

Click the context menu of the group you want to delete. To delete a group, it must be empty. If the group contains subgroups or computers, an error message appears.

You cannot delete the All group.

To delete empty Active Directory groups included in another group, click the group's context menu and select **Delete empty groups**.

Moving groups

- Click the context menu of the group you want to move.
- Click **Move**. A pop-up window appears with the target group tree.
- Select the target group and click **OK**.

You cannot move the All group or any Active Directory groups.

Renaming groups

- Click the context menu of the group you want to rename.
- Click **Change name**.
- Type a new name.

You cannot rename the All group or any Active Directory groups.

Importing IP-based assignment rules to existing groups

Follow the steps below to add IP addresses to an existing native group:

- Select the context menu of a native group other than the Al' group and select the **Import IP-based assignment rules** option. A window opens for you to drag a file with the IP addresses to add.
- The import file must contain one or more rows of text with the following format:
    - For individual IP addresses, include one address per row. For example:
        - `.\Group\Group\Group (Tab) IP address`
    - For IP address ranges, include one range per row. For example:
        - `.\Group\Group\Group (Tab) Start IP-End IP`
    - Advanced EPDR interprets all specified paths as part of the selected group.
    - If the groups indicated in the file do not already exist, Advanced EPDR creates them and assigns the specified IP addresses to them.
- Click **Import**. The IP addresses are assigned to the groups specified in the file. The icons on the My Organization tab update to reflect any changes to group type.

When you import a file with new group-IP pairs, the solution deletes all IP addresses previously assigned to an IP-based group.

When the process is complete, as new computers are integrated into Advanced EPDR, they move to the relevant groups based on their IP address.

Exporting IP-based assignment rules

To export a file with IP-based assignment rules, follow the steps below:

- Click the context menu of a group from which you want to export IP-based rules, and select the option **Export IP-based assignment rules**. A CSV file downloads with the IP-based assignment rules defined for the group and its subgroups.
- The CSV file has the format specified in section **Importing IP-based assignment rules to existing groups**.

Moving computers from one group to another

You have several options to move one or more computers to a group:

Moving groups of computers to groups

- Select the group **All** in order to list all managed computers, or use the search tool to locate a specific group of computers you want to move.
- In the list of computers, select the checkboxes next to the computers you want to move.
- Click the ⋮ icon to the right of the search bar. A drop-down menu appears with the option **Move to**. Click it to show the target group tree.
- Select the target group you want to move the computers to.

Moving a single computer to a group

There are three ways to move a single computer to a group:

- Follow the steps described above for moving groups of computers, but simply select a single computer.
- Find the computer that you want to move and click the ⋮ menu icon to its right.
- From the details page of the computer that you want to move:
    - From the panel with the list of computers, click the computer you want to move in order to display its details.

- Find the **Group** property and click **Change**. A window opens with the target group tree.
- Select the target group to move the computer to. Click **OK**.

Moving computers from an Active Directory group

A computer that belongs to an Active Directory group is synchronized with your Active Directory server and cannot be moved to another Active Directory group through Advanced EPDR. To do this, you must move the computer in Active Directory and then wait up to one hour for Advanced EPDR to synchronize the change. However, computers belonging to an Active Directory group can be moved to a native group.

If you move a computer from an Active Directory group to a native group, any changes made to the company's Active Directory groups will not be reflected in the web console. See ***Active Directory groups*** *for more information.*

Moving computers to an Active Directory group

You cannot move a computer from a native group to a specific Active Directory group. You can only return a computer to the Active Directory group that it previously belonged to. To do this, click the computer's context menu and select **Move to Active Directory path**.

Returning multiple computers to their Active Directory group

To return multiple computers to their original Active Directory group, click the context menu of an Active Directory group and select **Retrieve all computer residing on this Active Directory branch**. All computers in the group that you moved to other groups return to their original Active Directory group.

Filtering results by groups

The feature for filtering results by groups displays in the console only the information generated by the computers on the network that belong to the groups selected by the administrator. This is a quick way to establish a filter that affects the entire console (lists, dashboards, and settings) and helps to highlight data of interest to the administrator.

Configuring the filter by groups

To configure the filtering of results by groups, follow the steps below:

- Click the relevant button from the top menu. A window with the group tree is displayed.
- Select the groups you want to see from the computer tree and click **OK**.

The console only displays information for the computers from the selected groups.

Figure 8.4: Filtering results by groups

Filters do not affect task visibility, email alerts, or scheduled executive reports.

Filtering groups

In very large IT infrastructures, the group tree may contain a large number of nodes distributed at multiple levels, making it difficult to find specific groups. To filter the group tree and show only those groups that match the characters entered:

- Click the icon at the top of the group tree. A text box appears.
- Type the letters of the name of the group you want to find. All groups whose name starts with, ends with, or contains the character string entered are shown.
- After you have completed your search, select the group you are interested in and click the icon to show the full group tree again, maintaining your selection.

Available lists for managing computers

Computers list

Accessing the list

- From the top menu, select **Computers**. The left pane shows the computer or folder tree. The right pane shows a detailed table of the managed computers on the network.
- Click an item from the group tree or filter tree on the left. The right pane updates with details of the selected item.

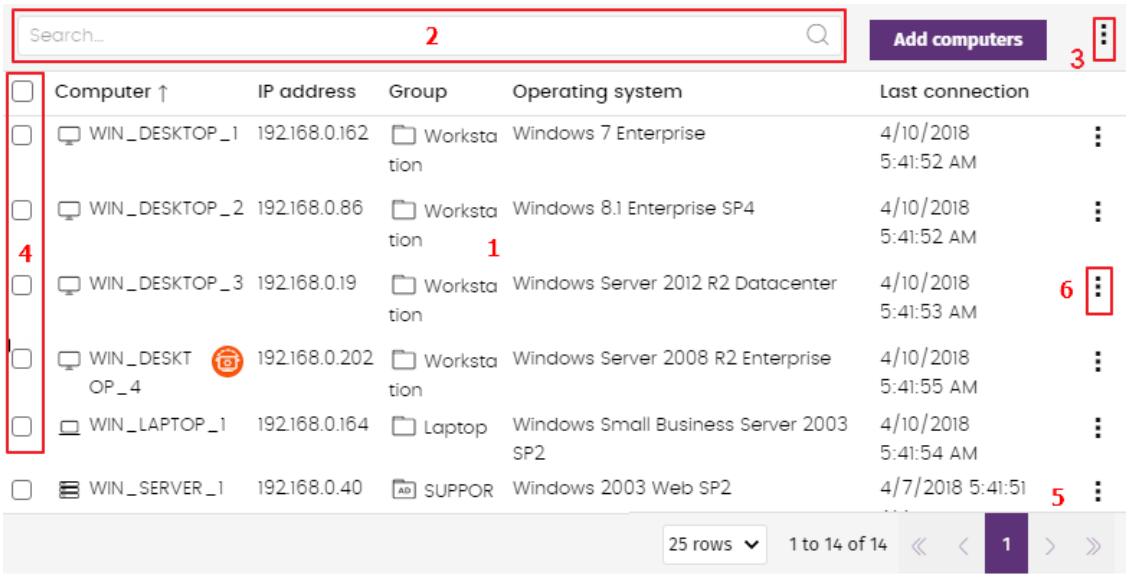


Figure 8.5: Computers list

Required permissions

No additional permissions are required to access the **Computers list**.

Computers

The computer list shows the workstations and servers that belong to the group or filter you select in the computer tree. It also provides management tools you can use on individual computers or on multiple computers at the same time.

The items that appear in the computer list are these:

- **(1)** List of computers that belong to the selected branch.
- **(2)** Search tool: Find computers by their name, description, IP address, last logged-in user, or MUID (computer ID used in Cytomic Orion). It supports partial matches. Search terms are not case-sensitive.
- **(3)** General context menu: Apply an action to multiple computers.
- **(4)** Computer selection checkboxes.
- **(5)** Pagination controls at the bottom of the pane.
- **(6)** Context menu for each computer.

You can configure the computer list to adapt the data shown to your needs.

To add or remove columns in the table, click the context menu in the upper-right corner of the page. Select **Add or remove columns**. A dialog box opens that shows the available columns and a **Default columns** link to reset the list to its default values.

Use the context menu to export the computer list. The exported file can contain all data in the computer list (see **Fields displayed in the exported file**) or a shortened version of it (see **Fields**

displayed in the shortened exported file). The latter option is very useful when there is a large number of computers.

- Click the icon to show the list options.
- Click the  icon to export the computer list or a shortened version of it.

You can see this detailed information for each computer:

Field	Description	Values
Computer	Computer name and type.	Character string: •  Workstation or server •  Laptop •  Mobile device (Android smartphone or tablet)
Computer status	Agent reinstallation: •  Reinstalling the agent. •  Error reinstalling the agent. Protection reinstallation: •  Reinstalling the protection. •  Error reinstalling the protection. •  Pending restart. Computer isolation status: •  Computer in the process of being isolated. •  Isolated computer. •  Computer in the process of stopping being isolated.	Icon

Field	Description	Values
	"RDP attack containment" mode: •  Computer in "RDP attack containment" mode. •  Ending "RDP attack containment" mode. Verbose mode •  Computer in Verbose mode.	
IP address	The computer primary IP address.	IP address
Last logged-in user	Names of the user accounts that have an active session on the computer.	Character string
Description	Description assigned to the computer.	Character string
Group	Folder within the Advanced EPDR group tree to which the computer belongs, and its type.	Character string: •  Group •  IP-based group •  Active Directory AD or root domain •  Organizational unit •  Group tree root
Active Directory path	Full path to the computer in the company Active Directory.	Character string
Domain	Windows domain the computer belongs to.	Character string
Operating system	Name and version of the operating system installed on the computer.	Character string
Last	Date when the computer status was last sent to	Date

Field	Description	Values
connection	the Cytomic cloud.	

Table 8.3: Fields in the Computers list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	Comma-separated list of the IP addresses of all cards installed on the computer.	Character string
Public IP address	IP address of the last device (router/proxy/VPN endpoint) that connected the customer network to the Internet.	IP address
Physical addresses (MAC)	Comma-separated list of the physical addresses of all cards installed on the computer.	Character string
Domain	Windows domain the computer belongs to.	Character string
Active Directory	Full path to the computer in the company Active Directory.	Character string
Group	Folder within the Advanced EPDR group tree to which the computer belongs.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string

Field	Description	Values
Last bootup date	Date when the computer was last booted.	Date
Installation date	Date when the Advanced EPDR software was successfully installed on the computer.	Date
Last connection	Last time the computer connected to the cloud.	Date
Platform	Type of operating system installed.	• Windows • Linux • macOS
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Virtual machine	Shows whether the computer is physical or virtual.	Boolean
Is a non-persistent computer	Shows whether the operating system of the virtual machine resides on a storage device that persists between restarts or reverts to its original state instead.	Boolean
Protection version	Internal version of the protection module installed on the computer.	Character string
Last update on	Date when the protection was last updated.	Date
Licenses	Licensed product.	Advanced EPDR
Network settings	Name of the network settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the network settings profile.	Character string
Security for	Name of the security settings profile applied to the workstation or server.	Character string

Field	Description	Values
workstations and servers		
Settings inherited from	Name of the folder from which the device inherited the security settings profile.	Character string
Security for Android devices	Name of the security settings profile applied to the mobile device.	Character string
Settings inherited from	Name of the folder from which the device inherited the security settings profile.	Character string
Security for iOS devices	Name of the security settings profile applied to the mobile device.	Character string
Settings inherited from	Name of the folder from which the device inherited the security settings profile.	Character string
Per-computer settings	Name of the settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the settings profile.	Character string
Cytomic Data Watch	Name of the personal data monitoring (Cytomic Data Watch) settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the personal data monitoring settings profile.	Character string
Patch management	Name of the patching (Cytomic Patch) settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the patching settings profile.	Character string

Field	Description	Values
Encryption	Name of the encryption (Cytomic Encryption) settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the encryption settings profile.	Character string
Authorized software	Name of the Authorized Software module settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the Authorized Software settings profile.	Character string
Program blocking	Name of the program blocking settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the program blocking settings profile.	Character string
Indicators of attack (IOA)	Name of the Indicators of Attack (IOA) settings profile applied to the computer.	Character string
Settings inherited from	Name of the folder from which the computer inherited the Indicators of Attack (IOA) settings profile.	Character string
Isolation status	Shows the isolation status of the computer.	• Isolated • Isolating • Stopping isolation • Not isolated
"RDP attack containment" mode	Status of the "RPD attack containment" mode.	Boolean

Field	Description	Values
Description	Description assigned to the computer.	Character string
Last logged-in user	Comma-separated names of the user accounts that have an interactive session active on the Windows computer.	Character string
Requested action	Requested action that is pending execution or is in progress.	• Restart • Protection reinstallation • Agent reinstallation
Requested action failed	Type of error reported by the requested action.	• Wrong credentials • Discovery computer not available • Unable to connect to the computer • Operating system not supported • Unable to download the agent installer • Unable to copy the agent installer • Unable to uninstall the agent • Unable to install the agent • Unable to register the agent • Action requires input from the user
Last proxy used	Access method used by Advanced EPDR the last time it connected to the Cytomic cloud. This data is not updated immediately. It might take up to 1 hour for the correct value to show.	Character string

Field	Description	Values
Shadow Copies	Shows the feature status: • Enabled • Disabled • **Error 2010**: The Shadow Copies service could not be enabled. • **Error 2011**: An error occurred creating the last Shadow Copy.	Enumeration
Last copy	Date and time the last copy was made.	Date

Table 8.4: Fields in the Computers list exported file

Fields displayed in the shortened exported file

When you select **Reduced export**, a file is generated that contains this information:

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
IP address	Comma-separated list of the IP addresses of all cards installed on the computer.	Character string
Public IP address	IP address of the last device (router/proxy/VPN endpoint) that connected the customer network to the Internet.	IP address
Physical addresses (MAC)	Comma-separated list of the physical addresses of all cards installed on the computer.	Character string
Domain	Windows domain the computer belongs to.	Character string
Active Directory	Full path to the computer in the company Active Directory.	Character string

Field	Description	Values
Last seen in Active Directory	Date when the computer was last seen in Active Directory.	
Group	Folder in the Advanced EPDRgroup tree to which the computer belongs.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
Last bootup date	Date when the computer was last booted.	Character string
Installation date	Date when the Advanced EPDR software was successfully installed on the computer.	Date
Last connection	Last time the computer connected to the cloud.	Date
Platform	Type of operating system installed.	• Windows • Linux • macOS
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Virtual machine	Shows whether the computer is physical or virtual.	Boolean
Is a non-persistent computer	Shows whether the operating system of the virtual machine resides on a storage device that persists between restarts or reverts to its original state instead.	Boolean
Protection version	Internal version of the protection module installed on the computer.	Character string
Last update on	Date when the protection was last updated.	Date
Licenses	Licensed product.	Advanced EPDR
Isolation status	Shows the isolation status of the computer.	• Isolated

Field	Description	Values
		• Isolating • Stopping isolation • Not isolated
"RDP attack containment" mode	Status of the "RPD attack containment" mode.	Boolean
Description	Description assigned to the computer.	Character string
Last logged-in user	Comma-separated names of the user accounts that have an interactive session active on the Windows computer.	Character string
Requested action	Requested action that is pending execution or is in progress.	• Restart • Protection reinstallation • Agent reinstallation
Requested action failed	Type of error reported by the requested action.	• Wrong credentials • Discovery computer not available • Unable to connect to the computer • Operating system not supported • Unable to download the agent installer • Unable to copy the agent installer • Unable to register

Field	Description	Values
		the agent • Action requires input from the user
Last proxy used by the agent	Access method used by Advanced EPDR the last time it connected to the Cytomic cloud. This data is not updated immediately. It might take up to 1 hour for the correct value to show.	Character string
Shadow Copies	Shows the feature status: • **Enabled** • **Disabled** • **Error 2010**: The Shadow Copies service could not be enabled. • **Error 2011**: An error occurred creating the last Shadow Copy.	Enumeration
Last copy	Date and time the last copy was made.	Date

Table 8.5: Fields in the Computers list shortened exported file

Filter tools

Field	Description	Values
Computer	Computer name.	Character string.

Table 8.6: Filters available in the Computers list

Management tools

To access the management tools:

- Select one or more computers using the checkboxes **(4)**. The search tool **(2)** hides and the action bar **(7)** appears.

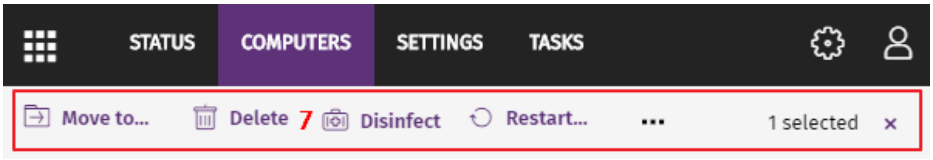


Figure 8.6: Action bar

Select the checkbox in the table header **(4)** to select all computers on the current page of the list. The **Select all xx rows in the list** option appears, which enables you to select all computers on the list regardless of the page you are on.

- Click the context menu **(6)** for a computer or mobile device.

Action	Description
Move to	Opens a dialog box that shows the group tree. Select the group you want to move the computer to. The computer inherits the settings profiles assigned to the target group. For more information, see **Creating and managing settings profiles** on page **294**.
Move to Active Directory path	Moves the computer to a group that corresponds with its organizational unit in Active Directory.
Delete	Deletes the computer from the console and uninstalls the Advanced EPDR endpoint software. For more information, see **Uninstalling the software** on page **182**.
Scan now	For an introduction to scan tasks, see **On-demand computer scanning and disinfection** on page **879**. For a full description, see **Tasks** on page **909**.
Schedule scan	For an introduction to scan tasks, see **On-demand computer scanning and disinfection** on page **879**. For a full description, see **Tasks** on page **909**.
Restart	Restarts the computer. For more information, see **Computer restart** on page **888**.
Isolate computer	Blocks all communications established from and to an at-risk computer, except for those required to connect to the Cytomic cloud. For more information, see **Isolating one or more computers from the organization network** on page **890**.

Action	Description
Stop isolating the computer	Restores all communications to and from the computer. For more information, see **Stopping isolation** on page **890**.
View available patches	Opens the **Available patches** list filtered for the selected computer. See **Available patches** on page **483**.
Schedule patch installation	For more information about how to install patches on Windows computers, see **Cytomic Patch (Updating vulnerable programs)** on page **435**.
View computer inventory	Opens the **Files with personal data** list filtered for the selected computer. See **Files with personal data** on page **417**.
Remote control	Starts a remote connection to the selected computer. See **Remote computer control** on page **892**.
Verbose mode	Enables Verbose mode to generate extended telemetry. See **Verbose mode** on page **359**.
Disable Verbose mode	Disables Verbose mode to generate standard telemetry. See **Verbose mode** on page **359**.**Verbose mode** on page **359**
End "RDP attack containment" mode	Manually end the blocking of RDP connections. See **Manual termination of RDP attack containment mode** on page **620**.
Reinstall protection (requires restart)	Reinstalls the security software if a malfunction occurs. For more information, see **Remote reinstallation** on page **186**.
Reinstall agent	Reinstalls the agent if a malfunction occurs. For more information, see **Remote reinstallation** on page **186**.
Selected	Undoes the current selection.

Action	Description
Report a problem	Sends a report to Cytomic technical support to diagnose problems with the computer.

Table 8.7: Computer management tools

My lists panel

Accessing the My lists panel

- Go to top menu **Status**. Click **Add** in the **My lists** section in the side panel. A window appears with all available lists.
- From the **General** group, select the **Hardware**, **Software**, or **Computers with duplicate name** list.

*See **Managing lists** on page **48** for more information about the types of lists and how to work with them.*

For more information about the fields as well as the filter and search tools implemented in each list, see the chapter on the group the list belongs to.

Required permissions

No additional permissions are required to access the **My lists** panel.

Hardware

Shows the hardware components installed on each computer on the network. Each hardware component is shown independently each time it is detected on a computer.

Field	Description	Values
Computer	Name and type of computer that contains the hardware component.	Character string: • Workstation or server. • Laptop. • Mobile device

Field	Description	Values
		(Android smartphone or tablet).
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
CPU	Make and model of the microprocessor installed on the computer. The number of installed cores is shown in brackets.	Character string
Memory	Total amount of RAM memory installed.	Character string
Disk capacity	Sum of the capacity of all the internal hard disks connected to the computer.	Character string
Last connection	Date when the Advanced EPDR status was last sent to the Cytomic cloud.	Date
Context menu	Management tools. See **Management tools** for more information.	

Table 8.8: Fields in the Hardware list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string

Field	Description	Values
Public IP address	IP address of the last device (router/proxy/VPN endpoint) that connected the customer network to the Internet.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string
Group	Folder in the Advanced EPDR group tree that the computer belongs to.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
Last connection	Date when the Advanced EPDR status was last sent to the Cytomic cloud.	Date
Platform	Type of operating system installed.	• Windows • Linux • macOS • Android
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
System	Name of the computer's hardware model.	Character string
CPU-N	Model, make, and characteristics of CPU number N.	Character string
CPU-N Number of cores	Number of cores in CPU number N.	Numeric value
CPU-N Number of logical processors	Number of logical cores reported to the operating system by the Hyper-Threading/SMT (simultaneous multithreading) system.	Numeric value
Memory	Sum of all the RAM memory banks installed on the	Character string

Field	Description	Values
	computer.	
Disk-N Capacity	Total space on internal storage device number N.	Character string
Disk-N Partitions	Number of partitions on internal storage device number N reported to the operating system.	Numeric value
TPM spec version	Versions of the APIs compatible with the TPM chip.	Character string
BIOS - Serial number	The computer's BIOS serial number.	Character string

Table 8.9: Fields in the Hardware exported file

Filter tool

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Platform	Operating system type.	• Windows • Android

Table 8.10: Filters available in the Hardware list

Software

Shows all programs installed on the computers on the network. For each package, the solution reports the number of computers that have it installed, as well as the software version and vendor.

Click any of the software packages to open the **Computers** list filtered by the selected package. The list shows all computers on the network that have that package installed.

Field	Description	Values
Name	Name of the software package found on the network.	Character string

Field	Description	Values
Publisher	Software package vendor.	Character string
Version	Internal version of the software package.	Character string
Computers	Number of computers that have the package installed.	Numeric value

Table 8.11: Fields in the Software exported file

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Name	Name of the software package found on the network.	Character string
Publisher	Software package vendor.	Character string
Version	Internal version of the software package.	Character string
Computers	Number of computers that have the package installed.	Numeric value

Table 8.12: Fields in the Software exported file

Fields displayed in the detailed Excel export file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Computer	Computer that contains the package found.	Numeric value
Name	Name of the software package found on the network.	Character string
Publisher	Software package vendor.	Character string

Field	Description	Values
Installation date	Date the software was installed.	Date
Size	The size of the installed software.	Numeric value
Version	Internal version of the software package.	Character string
Group	Folder in the Advanced EPDR group tree that the computer belongs to.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string

Table 8.13: Fields in the detailed export file

Filter tool

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Platform	Operating system type.	• Windows • Linux • macOS • Android

Table 8.14: Filters available in the Software list

Computer list page

Click any of the rows in the list to display a list of computers filtered by the selected software. See **Computers** for more information.

Computers with duplicate name

Shows computers on the network with the same name and belonging to the same domain. Where computers have the same name, Advanced EPDR considers the computer that has most recently connected to the Cytomic cloud to be the only correct one. This computer is not shown in the list.

To delete duplicate computers, select them using the relevant checkboxes and click **Delete** from the toolbar. A window is shown asking you if you wish to uninstall the Advanced EPDR agent.

> *Deleting computers from the **Computers with duplicate name** list without uninstalling the Advanced EPDR agent removes them from the Advanced EPDR console. However, those computers reappear in the Advanced EPDR console the next time they connect to the cloud. To avoid deleting multiple computers if you are not sure which ones are true duplicates, we recommend that you do not remove the agent from the computers and see which ones reappear in the console.*

Field	Description	Values
Computer	Computer name and type.	Character string: • Workstation or server • Laptop. • Mobile device (Android smartphone or tablet).
IP address	The computer's primary IP address.	Character string
Group	Folder in the Advanced EPDR group tree that the computer belongs to.	Character string
Operating system	Name of the operating system installed on the computer, internal version, and patch status.	Character string
Last connection	Date when the Advanced EPDR status was last sent to the Cytomic cloud.	Date

Table 8.15: Fields in the Computers with duplicate name list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the administrator.	Character string
Group	Folder in the Advanced EPDR group tree that the computer belongs to.	Character string
Agent version	Internal version of the agent installed on the computer.	Character string
Protection version	Internal version of the protection module installed on the computer.	Character string
Installation date	Date when the Advanced EPDR software was successfully installed on the computer.	Date
Last connection date	Date when the Advanced EPDR status was last sent to the Cytomic cloud.	Date
Platform	Type of operating system installed.	• Windows • Linux • macOS • Android

Field	Description	Values
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Active Directory	Full path to the computer in the company's Active Directory.	Character string
Last logged-in user	Names of the user accounts that have an active session on the computer.	Character string
Last bootup date	Date when the computer was last booted.	Date

Table 8.16: Fields in the Computers with duplicate name exported file

Filter tool

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Platform	Operating system type.	• All • Windows • Linux • macOS • Android
Last connection	Date when the Advanced EPDR status was last sent to the Cytomic cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30

Field	Description	Values
		days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago

Table 8.17: Filters available in the Computers with duplicate name list

Computer details page

Click any of the rows in the list to open the computer details page. See **Computer details** for more information.

Computer details

When you select a device from the list of computers, a page opens and shows details of the hardware, software, and security settings of the computer.

To show or hide the general details section and notifications, click or .

The details page is divided into these sections:

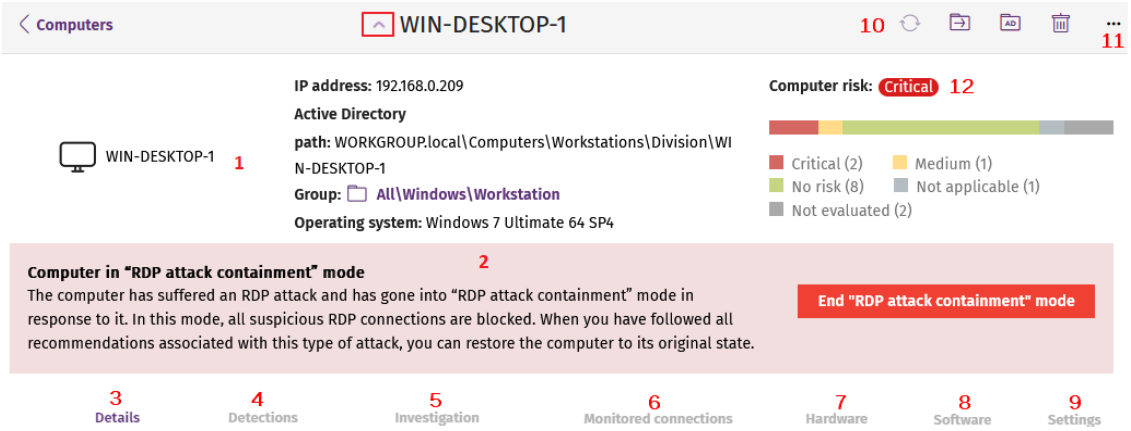


Figure 8.7: Computer overview

- **General (1)**: Information to help you identify the computer.
- **Notifications (2)**: Notifications that might indicate potential problems.
- **Details (3)**: Lists a summary of the hardware, software, and security settings of the computer.

- **Detections (4)**: Indicates the security status of the computer.
- **Investigation (5)**: Opens the Cytomic Orion investigation console to list the telemetry collected for the computer. See **Investigation section (5)**.
- **Monitored connections (6)**: Lists inbound connections detected on the computer. See **Endpoint Access Enforcement settings options** on page **519**.
- **Hardware (7)**: Lists hardware installed on the computer, its components and peripherals, as well as resource consumption and use.
- **Software (8)**: Lists software packages installed on the computer, as well as versions and changes.
- **Settings (9)**: Lists security settings and other settings assigned to the computer.
- **Toolbar (10)**: Includes buttons for each action you can take for managed computers.
- **Hidden icons (11)**: Based on the size of the screen, some tools might be hidden in an options menu.
- **Computer risk (12):** Risk information for the computer, including the risk level. See **Risk assessment module lists** on page **731**.

General section (1)

Contains the following information for all types of devices:

Field	Description
Computer	Computer name and icon indicating the computer status.
IP address	The computer's IP address.
Last logged-in user	Last logged-in user on the computer.
Description	Computer description assigned by the network administrator.
Group	Folder in the group tree to which the computer belongs.
Active Directory path	Full path to the computer in the company's Active Directory.
Domain	Domain the computer belongs to.
Operating system	Full version of the operating system installed on the computer.

Field	Description
Last connection	Date when the client software last connected to the Advanced EPDR cloud.
Computer risk	Distribution graph that shows the overall risk level for the computer and the risks detected on it. See **Risk assessment module lists** on page **731**.

Table 8.18: Fields in the General section of a computer's details

General section for mobile devices

With mobile devices, the General **(1)** and Computer notifications **(2)** sections are replaced with the anti-theft dashboard, from which you can take remote actions on managed devices.

*In the case of iOS devices, the actions you can take vary depending on whether the mobile device is enrolled in an MDM solution or not. See **Installation on iOS systems** on page **154**.*

*See **Anti-theft** on page **365** for more information about how to enable the anti-theft feature for mobile devices and configure private mode.*

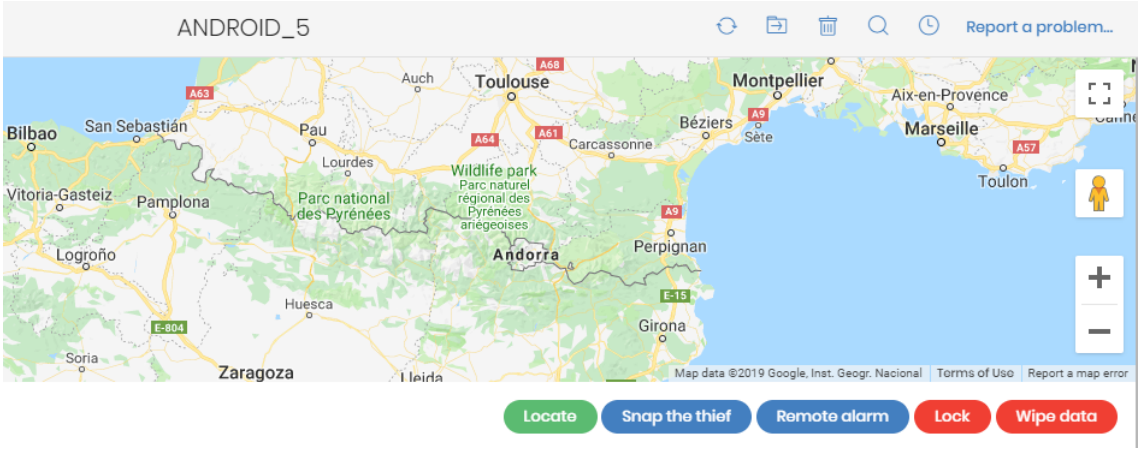


Figure 8.8: Anti-theft dashboard for mobile devices

The available actions are:

Action	Description
Locate	Advanced EPDR uses the device GPS to locate it. If this feature is unavailable,

Action	Description
	it tries to locate the device through Wi-Fi or the carrier communication infrastructure. • **With private mode enabled**: The console opens a window that prompts you to enter the code entered by the device user to enable private mode. When you enter the correct code, Advanced EPDR gets the device coordinates and shows the device location on the map. • **With private mode disabled**: The Advanced EPDR server gets the device coordinates and shows the device location on the map.
Snap the thief	This option is not available on iOS devices. When anti-theft is enabled, you can take a photo of the person using the Android device. The feature shows a window where you can enter an email address to send a photo of the potential thief to. Specify when you want the photo to be taken: • **Now**: The Advanced EPDR agent immediately takes a photo from the device and sends it to the specified address. • **When the screen is touched**: The Advanced EPDR agent takes a photo and sends it to the specified address when the user or potential thief touches the device screen.
Remote alarm	Shows a window where you can send a remote alarm and message to the mobile device. By default, the alarm sounds immediately, even if the device is locked. The screen shows the message and phone number you specify. To prevent an alarm sound, select the **Don't play any sound** checkbox.
Lock	Locks the mobile phone to prevent it from being used in the event of loss or theft, and requires the user to enter the PIN specified in the administrator console to open the device. Even though the administrator console always requires the user to enter the unlock PIN when you enable this feature, the behavior varies depending on the Android or iOS version used by the device. **Android**: • **Versions lower than 7**: The web console prompts you to create a PIN, which is then used to lock the device. • **Versions 7 to 10**: If a PIN was never created, the web console prompts you to create one and uses it to lock the phone. If a PIN was previously created by

Action	Description
	the user, it is used to lock the phone, regardless of the PIN you specify in the console. • **Versions 11 or higher**: If a PIN was previously created by the user, it is used to lock the phone, regardless of the PIN you specify in the console. If a PIN was never created, the device screen turns off and there is no lock PIN. **iOS**: • **Versions 13 or higher**: If a PIN was previously created by the user, it is used to lock the phone, regardless of the PIN you specify in the console. If a PIN was never created, the device screen turns off and there is no lock PIN.
Wipe data	This option deletes all device contents and applications and returns the device to factory settings.

Table 8.19: Actions supported by the anti-theft module for mobile devices

Computer notifications section (2)

These notifications describe problems encountered on computers with regard to the operation of Advanced EPDR and provide instructions for resolving them.

Occasionally, notifications **(1)** are accompanied by codes **(2)**.

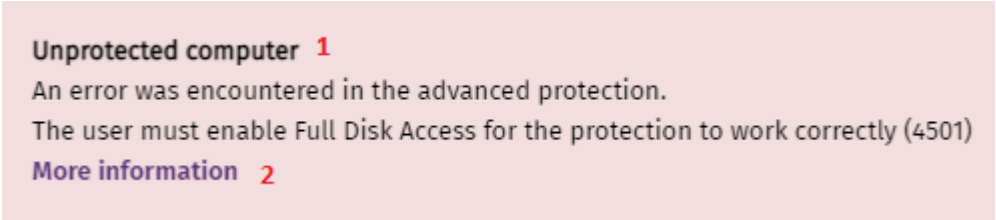


Figure 8.9: Unprotected computer notification and associated code

Each code is related to an error that occurs before or during the installation of the protection on computers. For more information about these codes, see **https://www.pandasecurity.com/en/support/card?id=700031**.

These tables list the types of notifications generated and recommended actions.

Isolated computers

Notification	Description	Reference
Isolated computer	The administrator has isolated the computer and all connections have been blocked except for those	For more information, see

Notification	Description	Reference
	required by Advanced EPDR to work correctly.	**Computer isolation** on page **888**.
We're trying to isolate this computer	The Advanced EPDR server has attempted to isolate the computer but cannot because the computer is offline or turned off.	For more information, see **Offline computers** on page **665**.
We're trying to stop isolating this computer	The Advanced EPDR server cannot stop the isolation command for the computer because the computer is offline or turned off.	For more information, see **Offline computers** on page **665**.

Table 8.20: Notifications related to the computer isolation feature

Computers in containment mode

Notification	Description	Reference
Computer in "RDP attack containment" mode	The computer has received a high number of failed RDP connection attempts, and all RDP connections have been blocked to contain the attack.	See **Detection and protection against RDP attacks** on page **617**
We're trying to end the "RDP attack containment" mode on this computer.	The administrator has manually ended the "RDP attack containment" mode on the computer, but the operation is not yet complete. This could be because the computer is turned off, offline, pending restart, or the action is in progress.	See **Detection and protection against RDP attacks** on page **617**

Table 8.21: Notifications related to the attack containment feature

Licenses

Notification	Description	Reference
Computer without a license	There are no available licenses to assign to the computer. Release an assigned license or purchase more Advanced EPDR licenses.	For more information, see **Releasing licenses** on page **192**.
	There are free licenses but none of them have been assigned to this computer.	For more information, see **Assigning licenses** on page **191**.

Table 8.22: Notifications related to license assignment

Computer in Audit mode

Notification	Description	Reference
Computer in Audit mode	Enabling Audit mode for a settings profile does not change the overall status of the protections applied to the computers that receive the settings. Nor does it change the configuration of the protections in the web console. Threats continue to be detected and reported, but they are not blocked or deleted.	For more information, see **Audit mode** on page **359**

Table 8.23: Notification related to the Audit mode

Protection software installation errors

*Errors that occur during the protection software installation process are shown with an error code, its associated extended error code, and an extended error subcode, where available. For more information, see table **Fields displayed in the exported file** on page **685**.*

Notification	Description	Reference
Unprotected computer	There was an error during installation of	For more information, see **Product features and requirements** on page **932**.

Notification	Description	Reference
	the security product on the computer. With errors whose origin is known, a description of the cause is displayed. If the origin is unknown, the associated error code is displayed.	
	A reboot is required to complete the installation due to a previous uninstallation.	For more information, see **Computer restart** on page **888**.
	The agent does not have the permissions required on macOS computers.	For more information, see **Requirements for macOS platforms** on page **944**.
	Error when installing the protection on macOS 13 Ventura. The user must allow EndpointProtectionService from Login Items.	For more information, see **Requirements for macOS platforms** on page **944**.
	Unsupported Linux kernel.	For more information, see **https://www.pandasecurity.com/en/support/card?id=700031**.
	Unsupported Unbreakable Enterprise Kernel (UEK) release.	For more information, see **https://www.pandasecurity.com/en/support/card?id=700031**.
Error installing Cytomic Data Watch	There was an error during installation of Cytomic Data Watch	For more information, see **Cytomic Data Watch requirements** on page **374**.

Notification	Description	Reference
	on the computer.	
Error installing the protection and Cytomic Data Watch	There was an error during installation of the protection and the module on the computer.	For more information, see **Product features and requirements** on page **932** and **Cytomic Data Watch requirements** on page **374**.
Error installing the patch manager	There was an error during installation of the patch management module.	For more information, see **Make sure that Cytomic Patch works correctly** on page **440**.
Error installing the encryption module	There was an error during installation of the encryption module.	For more information, see **Cytomic Encryption minimum requirements** on page **545**.
Error installing the Cytomic agent	Wrong credentials.	For more information, see **Offline computers** on page **665**.
	The discovery computer is not available.	For more information, see **Security module panels/widgets** on page **661**, and **Designating a discovery computer** on page **122**.
	Unable to connect to the target computer because it is turned off or does not comply with the hardware or network requirements.	For more information, see **Security module panels/widgets** on page **661**, and **Product features and requirements** on page **932**.
	The computer operating system is not supported.	For more information, see **Product features and requirements** on page **932**.
	Unable to download the agent installer due	For more information, see **Product features and requirements** on page **932**.

Notification	Description	Reference
	to a network error.	
	Unable to copy the agent installer due to low free disk space on the computer.	For more information, see **Product features and requirements** on page **932**.
	Unable to copy the agent installer because the target computer is turned off or does not meet the remote installation requirements.	For more information, see **Offline computers** on page **665**, and **Product features and requirements** on page **932**.
	Unable to register the agent.	For more information, see **Offline computers** on page **665**, and **Product features and requirements** on page **932**.
Error communicating with servers	The computer cannot connect to one or more servers in the Cytomic cloud.	For more information, see **Product features and requirements** on page **932**.

Table 8.24: Notifications related to the installation of the Advanced EPDR software

Protection software reinstallation errors

*Errors that occur during the protection software reinstallation process are shown with an error code, its associated extended error code, and an extended error subcode, where available. For more information, see table **Table 20.24:** on page **688**.*

Notification	Description	Reference
Pending protection reinstallation	The administrator requested reinstallation of the security product. Reinstallation is incomplete because the computer is off or offline, or there is	See **Offline computers** on page **665** and **Remote reinstallation**

Notification	Description	Reference
	still time before the forced restart.	**requirements** on page **186**.
Pending agent reinstallation	The administrator requested reinstallation of the agent. Reinstallation is not complete because the computer is off or offline, or there is still time before the forced restart.	See **Offline computers** on page **665** and **Remote reinstallation requirements** on page **186**.
Error installing the Cytomic agent	Wrong credentials.	For more information, see **Offline computers** on page **665**.
	The discovery computer is not available.	For more information, see **Offline computers** on page **665**.
	Unable to connect to the computer. It is off or offline, or does not meet remote installation requirements.	See **Offline computers** on page **665** and **Remote reinstallation requirements** on page **186**.
	The operating system is not supported. It does not meet remote installation requirements.	See **Remote reinstallation requirements** on page **186**.
	Unable to download the agent installer to the target computer. The computer is turned off or does not meet remote installation requirements.	See **Offline computers** on page **665** and **Remote reinstallation requirements** on page **186**.
	Unable to copy the agent installer to the target computer. It is turned off or does not meet remote installation requirements.	See **Offline computers** on page **665** and **Remote reinstallation requirements** on page **186**.

Notification	Description	Reference
	Unable to uninstall the agent from the target computer. It is turned off or does not meet remote installation requirements.	See **Offline computers** on page **665** and **Remote reinstallation requirements** on page **186**.
	Unable to install the agent on the target computer. It is turned off or does not meet remote installation requirements.	See **Offline computers** on page **665** and **Remote reinstallation requirements** on page **186**.
	Unable to register the agent because the computer is turned off or does not meet remote installation requirements.	See **Offline computers** on page **665** and **Remote reinstallation requirements** on page **186**.
	Action requires input from the user.	See **Offline computers** on page **665** and **Remote reinstallation requirements** on page **186**.

Table 8.25: Notifications related to the reinstallation of the Advanced EPDR agent

Advanced EPDR software issues

Notification	Description	Reference
Unprotected computer	An error was encountered in the antivirus and advanced protections. Restart the computer to fix the problem.	See **Computer restart** on page **888**.
Cytomic Data Watch error	An error was encountered in Cytomic Data Watch. Restart the computer to fix the problem.	See **Computer restart** on page **888**.
Error encrypting the computer	Unable to encrypt the computer due to an error.	See **Computer restart** on page

Notification	Description	Reference
		888.

Table 8.26: Notifications related to Advanced EPDR software issues

Pending user or administrator action

Notification	Description	Reference
Encryption pending user action	The user must restart the computer or enter the relevant encryption credentials to complete the encryption process.	See **Encryption and decryption on Windows computers** on page **546** and **Encryption and decryption on macOS computers**
Pending restart	The administrator has requested that the computer be restarted but it has not restarted yet as it is offline or the time period for a forced reboot has not ended yet.	See **Offline computers** on page **665**.
Reinstalling the protection.	The administrator has requested that the computer protection be reinstalled but the operation is not yet complete because the computer is turned off or offline, the amount of time to wait before the reinstallation is forced has not passed, or the reinstallation is in progress.	See **Remote reinstallation** on page **186**
Unprotected computer	The antivirus and advanced protections are disabled. Enable the protection.	See **Manual and automatic assignment of settings profiles** on page **296**, **Creating and managing settings profiles** on page **294**, and **Advanced protection** on page **333**.
Computer offline for N days	The computer is turned off or does not meet the network access requirements.	See **Product features and requirements** on page **932**

Notification	Description	Reference
Outdated protection	The protection requires the local user to manually restart the computer to complete the installation.	This is only on computers with the Home and Starter versions of Windows.
Connection problems with the Cytomic servers	The computer cannot successfully connect to the servers that store the security intelligence.	See **Product features and requirements** on page **932**
The administrator has changed the protection status from the computer local console	The administrator has changed the protection settings from the agent installed on the workstation or server. The current settings do not match the settings defined from the web console.	
Cannot upgrade this computer's protection to the latest version	The new versions of the protection require that the operating system recognize SHA-256 signed drivers. This computer does not support that signature format and therefore the installed protection cannot be upgraded to the latest version	See **Support for SHA-256 driver signing** on page **943**.

Table 8.27: Notifications related to lack of user or administrator action

Computer with out-of-date protection

Notification	Description	Reference
Outdated protection	A reboot is required to complete the protection update process.	For more information, see **Computer restart** on page **888**.
	An error occurred during the update process. Make sure the computer meets the hardware and network requirements.	See **Product features and requirements** on page **932** and the amount of available disk space in the **Hardware section (7)**.
	Updates are disabled for the computer. Assign the computer a	See **Protection engine updates** on page **204**.

Notification	Description	Reference
	settings profile with updates enabled.	
Malware and threat knowledge out of date	Knowledge updates are disabled for this computer. Assign the computer a settings profile with updates enabled.	See **Knowledge updates** on page **206**.

Table 8.28: Notifications related to out-of-date Advanced EPDR software

Mobile device notifications

Notification	Description	Reference
The iOS device has been jailbroken	The device has been jailbroken and allows the installation of unsigned apps. The device is exposed to confidential data leaks or removal of the security software.	Contact the user.
iOS or Android device with permission problems	The device user has not granted permissions required by Advanced EPDR, affecting its performance.	See **Requirements for iOS platforms** on page **950** and **Requirements for Android platforms** on page **949**

Table 8.29: Mobile device notifications

Details section (3)

The information on this tab is divided into three sections:

- **Computer**: Information about the device settings. This information is provided by the Cytomic agent.
- **Security**: The status of the Advanced EPDR protection modules.
- **Data protection** (Windows computers only): The status of the modules that protect the data stored on computers.

Computer

Field	Description
Risk	For Android devices, distribution graph that shows the overall risk level for the device and the risks detected on it. See **Risk assessment module lists** on page **731**.
Name	Computer name.
Description	Descriptive text provided by the administrator.
IP addresses	List of all the IP addresses (primary addresses and aliases).
Public IP address	IP address of the last device (router/proxy/VPN endpoint) that connected the customer network to the Internet.
Physical addresses (MAC)	Physical addresses of the network interface cards installed.
Domain	Windows domain the computer belongs to. This is empty if the computer does not belong to a domain.
Active Directory path	Path to the computer in the company's Active Directory.
Group	Group in the group tree that the computer belongs to. To change the computer's group, click **Change**.
Operating system	Operating system installed on the computer.
Virtual machine	Shows whether the computer is physical or virtual.
Is a non-persistent desktop	Shows whether the operating system of the virtual machine resides on a storage device that persists between restarts or reverts to its original state instead.
Licenses	Cytomic product licenses installed on the computer. See **Licenses** on page **189** for more information.

Field	Description
Agent version	Internal version of the Cytomic agent installed on the computer.
Last bootup date	Date when the computer was last booted.
Installation date	Date when the computer's operating system was last installed.
Last proxy used	Access method used by Advanced EPDR the last time it connected to the Cytomic cloud. This data is not updated immediately. It might take up to 1 hour for the correct value to show.
Last connection with the Cytomic infrastructure	Date when the client software last connected to the Cytomic cloud. The communications agent connects at least every four hours.
Last settings check	Date Advanced EPDR last connected to the Cytomic cloud checking for changes to the settings.
Shadow Copies	Shows the feature status: • Enabled • Disabled • Error code
Last copy	Shows the date and time of the last copy made.
Last logged-in user	Names of the user accounts that have an active session on the computer.

Field	Description
Remote control	Shows the feature status: • **Enabled** • **Disabled** • **Installation error**: The remote control module reported an error in the installation process. • **No license**: The security software does not have a Advanced EPDR license assigned. • **No information**: The agent has not yet sent information about the module status to the server.

Table 8.30: Fields in the Computer section

Security

This section shows the status (Enabled, Disabled, Error) of the Advanced EPDR technologies that protect the computer against malware.

Field	Description
Advanced protection	Protection against advanced threats, APTs, and exploits.
File antivirus	Protection for the file system.
Anti-theft	Actions for mitigating data exposure in the event of theft of a mobile device. This feature is not available for iOS devices not installed with an MDM solution. See **Installation on iOS systems** on page **154**.
Mail antivirus	Protection for the protocols used for sending and receiving email messages.
Web browsing antivirus	Protection against malware downloaded from web pages. This feature is not available for iOS devices not installed with an MDM solution. See **Installation on iOS systems** on page **154**.
Firewall	Protection for the network traffic generated by applications.

Field	Description
Device control	Protection from infections stemming from external storage devices or devices that enable computers to connect to the Internet without passing through the organization's communications infrastructure (modems).
Web access control	Protection that enables you to prevent access to unauthorized web pages. This feature is not available for iOS devices not installed with an MDM solution. See **Installation on iOS systems** on page **154**.
Patch management	Installation of patches and updates for Windows, macOS, and Linux operating systems and third-party applications. Detection of the patch status of the computers on the network and removal of problematic patches.
Patch installation	Indicates whether patch installation is allowed or denied on the computer, or whether the computer is a test computer for patch installation. For more information, see **Cytomic Patch features**
Program blocking	Blocking of the execution of programs considered dangerous or not compatible with the organization activity by the administrator.
Last checked	Date when Cytomic Patch last queried the cloud to check whether new patches had been published.
Protection version	Internal version of the protection module installed on the computer.
Knowledge update date	Date when the signature file was last downloaded to the computer.
Hard disk encryption (Mac computers only)	Encryption module status: • **Not available:** The computer is not compatible with Cytomic Encryption. • **No information**: The computer has not yet sent any information about the encryption module. • **Enabled**: The computer has a settings profile assigned to encrypt its storage devices and no errors have occurred. • **Disabled**: The computer has a settings profile assigned to decrypt its storage devices and no errors have occurred.

Field	Description
	• **Error installing**: Error downloading or installing the executables required to manage the encryption service if they were not already installed on the computer. • **No license**: The computer does not have a Advanced EPDR license assigned. **Get recovery key**: Opens a dialog box that shows the ID of the recovery key associated with the computer and the corresponding recovery key. For more information, see **Obtaining a recovery key** on page **551**. Encryption process status: • **Unknown**: There are disks whose status is unknown. • **Unencrypted disks**: For the computer encryption process to start, the user must enter administrator credentials. • **Encrypted disks**: All disks compatible with the encryption technology are encrypted. • **Encrypting**: At least one disk is currently in the encryption process. • **Decrypting**: At least one disk is currently in the decryption process. • **Encrypted by the user**: The user encrypted all of the disks. • **Encrypted by the user (partially)**: The user encrypted some of the disks.
Authentication method (Mac computers)	• **Password:** While booting, the computer requests a PIN or password for authentication.
Connection to knowledge servers	Status of the connection between the computer and the Cytomic servers. In case of errors, links are shown to support pages with information about the requirements that must be met.

Table 8.31: Fields in the Security section

Data protection (Windows)

This section shows the status of the modules that protect the data stored on the computer.

Field	Description
Personal data monitoring	Monitors files containing data that could identify users or company customers (Cytomic Data Watch module).

Field	Description
Allow data searches on this computer	Shows whether the computer has a settings profile assigned that enables it to receive searches for files and report their results.
Personal data inventory	Provided that content-based searches of files are allowed, Cytomic Data Watch parses all files contained in the supported storage media to retrieve their content and generate a database.
Indexing status	• Not indexed • Indexed • Indexed (text only) • Indexed (all content) • Indexing
Hard disk encryption	Encryption module status: • **Not available:** The computer is not compatible with Cytomic Encryption. • **No information**: The computer has not yet sent any information about the encryption module. • **Enabled**: The computer has a settings profile assigned to encrypt its storage devices and no errors have occurred. • **Disabled**: The computer has a settings profile assigned to decrypt its storage devices and no errors have occurred. • **Error**: The settings configured by the administrator do not allow an authentication method supported by Cytomic Encryption to be applied on the operating system version installed on the computer. • **Error installing**: Error downloading or installing the executables required to manage the encryption service if they were not already installed on the computer. • **No license**: The computer does not have a Advanced EPDR license assigned. **Get recovery key**: Opens a dialog box that shows the IDs of the computer encrypted disks. Click an ID to show the relevant recovery key. For more information, see **Obtaining a recovery key** on page **551**. Encryption process status:

Field	Description
	• **Unknown**: There are disks whose status is unknown. • **Unencrypted disks**: Some of the disks compatible with the encryption technology are neither encrypted nor in the process of being encrypted. **Unencrypted disks**: Some of the disks compatible with the encryption technology are neither encrypted nor in the process of being encrypted. • **Encrypted disks**: All disks compatible with the encryption technology are encrypted. • **Encrypting**: At least one disk is currently in the encryption process. • **Decrypting**: At least one disk is currently in the decryption process. • **Encrypted by the user**: The user encrypted all of the disks. • **Encrypted by the user (partially)**: The user encrypted some of the disks.
Authentication method	• **Unknown**: The authentication method is not compatible with those supported by Cytomic Patch. • **Security processor (TPM).** • **Security processor (TPM) + Password** • **Password**: Authentication method based on a PIN, extended PIN, or passphrase. • **USB drive**: Authentication method based on a USB drive. • **None**: None of the drives compatible with the encryption technology is encrypted or in the process of being encrypted.
Encryption date	Date when the computer was fully encrypted for the first time.
Removable storage drive encryption	Encryption module status: • **Not available:** The computer is not compatible with Cytomic Encryption. • **No information**: The computer has not yet sent any information about the encryption module. • **Enabled**: The computer has a settings profile assigned to encrypt its storage devices and no errors have occurred. • **Disabled**: The computer has a settings profile assigned to decrypt its

Field	Description
	storage devices and no errors have occurred. • **Error**: The settings configured by the administrator do not allow an authentication method supported by Cytomic Encryption to be applied on the operating system version installed on the computer. • **Error installing**: Error downloading or installing the executables required to manage the encryption service if they were not already installed on the computer. • **No license**: The computer does not have a Advanced EPDR license assigned. **View encrypted devices on this computer:** Opens a dialog box that shows the IDs of the computer encrypted external storage media. Click an ID to show the relevant recovery key. See **Obtaining a recovery key** on page **551**.

Table 8.32: Fields in the Data Protection section

Detections section (4) for Windows, Linux, and macOS computers

Shows counters associated with the computer's security and patch level through the following widgets:

Panel	Description
Detections by advanced security policies	See **Detections by advanced security policies** on page **672**.
Malware activity	See **Malware/PUP activity** on page **667**.
Currently blocked programs being classified	See **Currently Blocked Programs Being Classified panel** on page **790**.
Programs blocked by the administrator	See **Programs blocked by the administrator** on page **575**.
PUP activity	See **Malware/PUP activity** on page **667**.
Exploit activity	See **Exploit activity** on page **669**.

Panel	Description
Threats detected by the antivirus	See **Threats detected by the antivirus** on page **675**.
Available patches	See **Available patches** on page **467**.
Available patches trend	See **Available patches trend** on page **464**.
End-of-Life programs	See **End-of-Life programs** on page **462**.
Detected indicators of attack (IOA)	See **Detected indicators of attack (IOA)** on page **652**.
Detections trend	See **Detections trend** on page **648**.

Table 8.33: List of widgets available in the Detections section

Detections section (4) for Android and iOS devices

Shows counters associated with the device's security through the following widgets:

Panel	Description
Threats detected by the antivirus	See **Threats detected by the antivirus** on page **675**.

Table 8.34: List of widgets available in the Detections section

Investigation section (5)

This section shows the telemetry collected on the computer so you can investigate the source and scope of attacks.

*For more information about the meaning of the fields in the telemetry data, see **Format of the events contained in telemetry data** on page **957**.*

You can use these tools to view the telemetry:

- **Investigation console**
- **Advanced SQL queries**
- **Graphs**

You can use one or more tools. The tab bar shows the tools used in the session. When you select the **Investigation** tab, the console automatically opens the **Investigation console** tool for the managed computer. To use another tool, select the relevant tab. To add a tool, click the + icon.

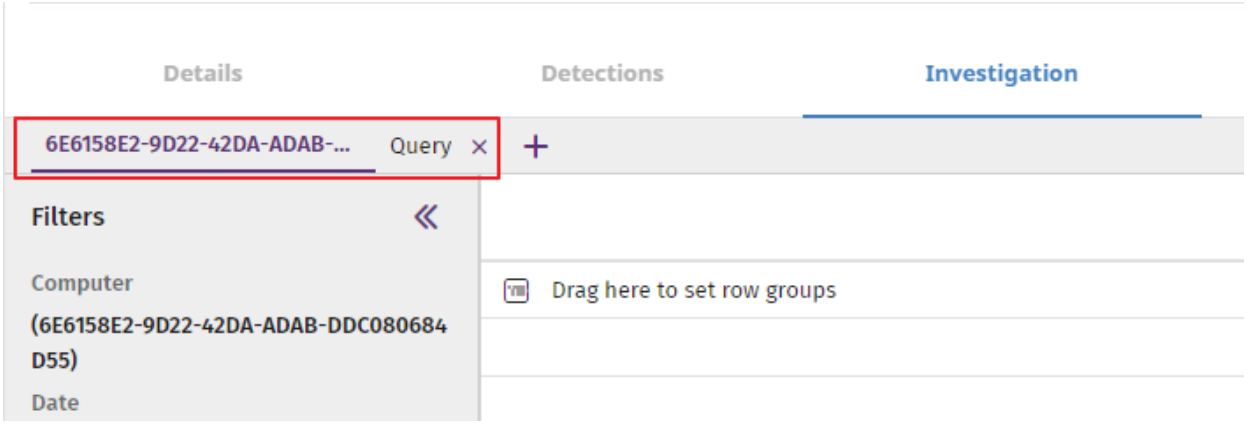


Figure 8.10: Tab bar with the investigation console and advanced SQL query open tools

Investigation console

The Cytomic Orion investigation console shows a list of all events logged on the computer over a one-day period. You can change the start date to up to seven days earlier to see telemetry recorded in previous days.

> *For more information about the Cytomic Orion investigation console, see **Investigation Console Structure**.*

Opening a new investigation console

As your investigation progresses, you might need to open more investigation consoles for other computers on the network**Database schema**

To open a new investigation console:

- Select the **Investigation** tab for the selected computer. The Cytomic Orion console opens.
- Click the + icon. The context menu opens.
- Select **Computer investigation**. The **Investigate computer** dialog box opens.

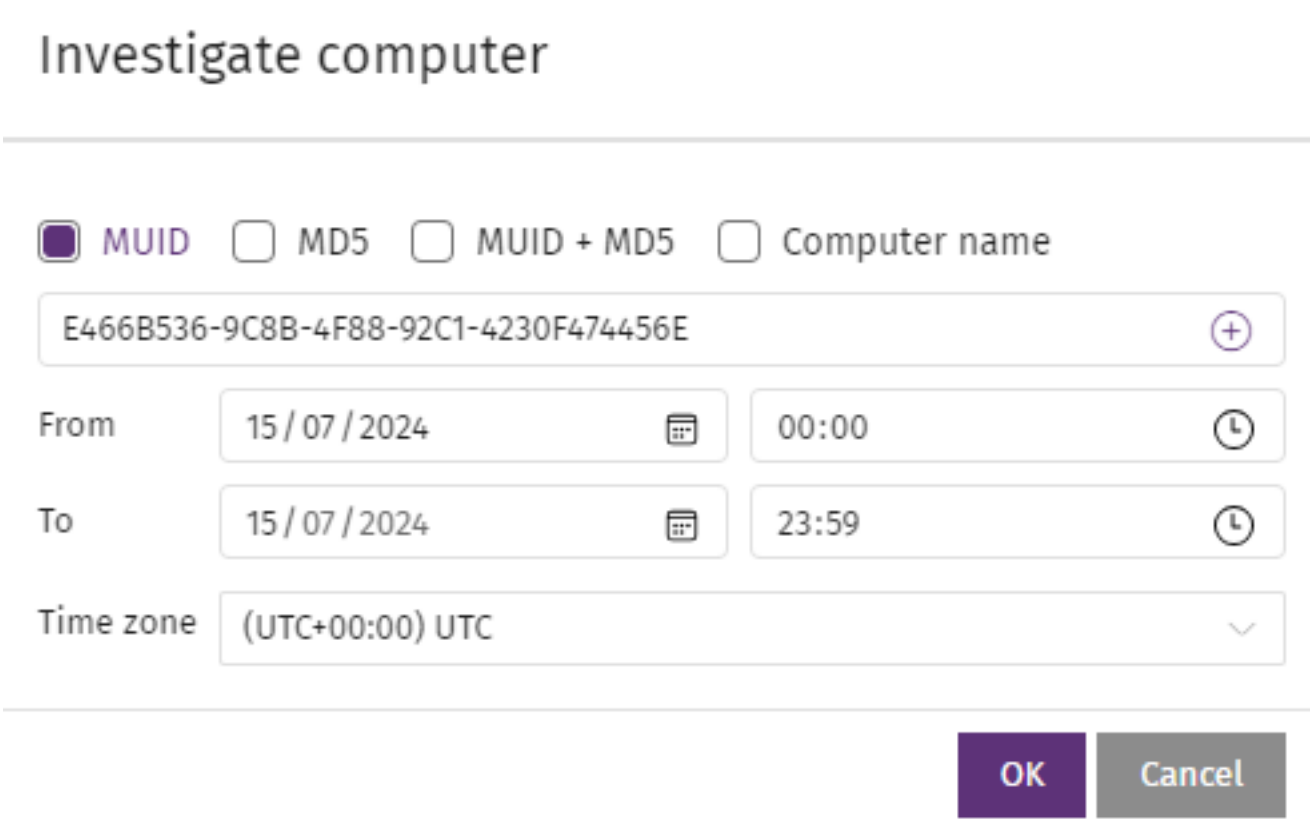


Figure 8.11: Dialog box to select the new computer you want to investigate

- To investigate all events logged on a computer over a one-day period:
  - Select **MUID** or **Computer name** (the advanced SQL query tool works with MUIDs. See **Device ID (MUID)**).
  - In the text box, type the **Computer name** or **MUID**.
  - Select the time period for which the investigation console will retrieve data from the data lake. You can change the start date to up to seven days earlier to see telemetry recorded in previous days. The longest supported time period is one day.
  - Select a time zone for the time period.
  - Click **OK**. A new tab appears that shows the investigation console configured to show telemetry for the selected computer.
- To investigate a file when you do not know the computer that contains it:
  - Select **MD5**. In the text box, enter the file MD5.
  - Click **OK**. A new tab appears that shows the investigation console. The investigation console has two panes.
  - From the left pane, select the computer you want to investigate. The right pane shows all events related to the file on the computer.
- To investigate a file when you know the computer that contains it:

- Select **MUID + MD5**. In the text boxes, type the computer MUID and the file MD5.
- Click **OK**. The investigation console opens and shows all events related to the file on the computer.

Advanced SQL queries

You can navigate the data lake to find specific events for a selected computer or any other computer on the managed network using the computer MUID. With the advanced SQL query tool, you can access telemetry recorded on the current day, as well as the seven previous days. To do this, you must use SQL and know the database schema used. See **Database schema**

To access the advanced SQL query tool:

- Select the **Investigation** tab for the selected computer. The Cytomic Orion investigation console opens.
- Click the + icon. The context menu opens.
- Select **Advanced SQL query**. The advanced SQL query tool opens.

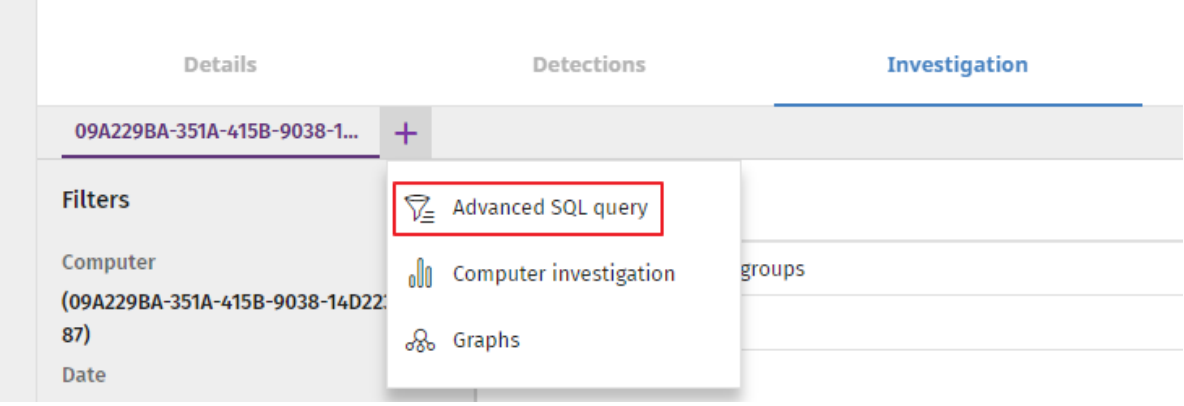


Figure 8.12: Investigation drop-down menu.

For more information about how to use the advanced SQL query tool, see **Advanced SQL Query Module**.

> *Some features of the advanced SQL query tool are only available to customers who access the tool directly through the Cytomic Orion console.*

For more information about the syntax of the SQL type used in Cytomic Orion, see **Advanced Query Module SQL Syntax**.

Database schema

When you access the advanced SQL query tool from Advanced EPDR, the events logged on the computer are stored in two tables:

- **Telemetry**: Stores the telemetry logged on computers.
- **Indicators**: Shows the indicators logged on computers. Indicators are grouped. For more information about the grouping algorithm, see **Indicator Grouping**.

The **EventType** field in the **Telemetry** table indicates the type of event stored in the corresponding row. For more information about the types of events, see **Format of the events contained in telemetry data** on page **957**.

Device ID (MUID)

The advanced SQL query tool shows events from the data lake just as they are stored in the database. Some tables store references to computers on the network by using the computer MUID (Machine Universal Identifier). To get a computer name from the computer MUID, search for the MUID in the Advanced EPDR console. See **Computers**.

Graphs

Graphs use nodes and arrows to provide a graphical representation of the processes discovered in your analysis and the relationship between them. The information shown on a graph is equivalent to the information shown in the investigation console or in advanced queries, but organized and presented in a clearer, easier-to-interpret way.

Opening a graph

- Select the **Investigation** tab for the selected computer. The Cytomic Orion investigation console opens.
- Click the + icon. The context menu opens.
- Select **Graphs**. The **New graphical investigation** dialog box opens and shows a list of all graph templates defined.
- Select a template based on the type of data you want the graph to show. For more information about the available templates, see **Information Contained in Graphs**. If the template requires parameters, a dialog box opens for you to enter the necessary information.

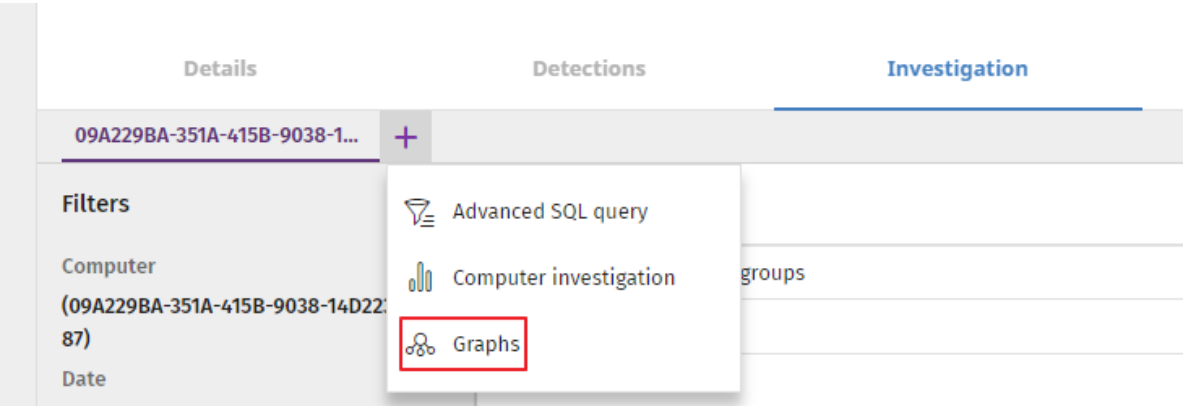


Figure 8.13: Investigation drop-down menu.

For more information about graphs, see ***Graphs****.*

Monitored connections (6)

Accessing the list

To access the list:

- From the top menu, select **Computers**.
- From the computer tree, select a group that contains computers with the Endpoint Access Enforcement feature enabled.
- From the computer list, select a computer. Select the **Monitored connections** tab.

Required permissions

Permission	Access to lists
View detections and threats	Monitored connections

Table 8.35: Permissions required to access the Monitored Connections list

Monitored connections

This list shows information about inbound connections detected on the computer that meet the conditions you configured in the Endpoint Access Enforcement policy. See **Endpoint Access Enforcement settings** on page **518**.

For more information about the data in the list, see ***Endpoint Access Enforcement module lists*** *on page* ***531****.*

Hardware section (7)

This tab shows information about the hardware resources installed on the computer:

Field	Description	Values
CPU	Information about the computer microprocessor, along with a line chart that shows CPU usage at different time intervals based on your selection.	• 5-minute intervals over the last hour. • 10-minute intervals over the last 3 hours.

Field	Description	Values
		• 40-minute intervals over the last 24 hours.
Memory	Information about the memory chips installed, along with a line chart that shows memory usage at different time intervals based on your selection.	• 5-minute intervals over the last hour. • 10-minute intervals over the last 3 hours. • 40-minute intervals over the last 24 hours.
Disk	Information about the mass storage system, along with a pie chart that shows the current percentage of free/used space.	• Device ID • Size • Type • Partitions • Firmware revision • Serial number • Name
BIOS	Information about the BIOS installed on the computer.	• Version • Manufacture date • Serial number • Name • Manufacturer
TPM	Information about the security chip located on the computer motherboard. For Advanced EPDR to use the TPM chip, it must be enabled, activated, and owned.	• **Manufacturer version**: Internal version of the chip. • **Spec version**: Supported API versions. • Version • Manufacturer • **Activated**: The TPM chip is ready to receive commands. This is used on

Field	Description	Values
		systems with multiple TPM chips. • **Enabled**: The TPM chip is ready to work as it has been enabled in the BIOS. • **Owned**: The operating system can interact with the TPM chip.

Table 8.36: Fields in the Hardware section of a computer details

Software section (8)

This tab provides information about the software packages installed on the computer, the Windows operating system updates, and a history of all software installations and uninstallations.

Filter tool

To perform a search, type a software package name or publisher in the **Search** text box. Press **Enter**. This information appears for each program found:

Field	Description
Name	Name of the installed program.
Publisher	Company that developed the program.
Installation date	Date when the program was last installed. With iOS devices enrolled in an MDM solution, this field indicates the date when apps were first seen on the device. See **Deploying and installing the iOS agent** on page **157**. This information is not available for iOS devices not enrolled in an MDM solution. Devices enrolled in the Cytomic MDM solution send the server a daily report that includes the third-party apps they have installed.
Size	Program size.

Field	Description
Version	Internal version of the program.

Table 8.37: Fields in the Software section of a computer details

- To narrow your search, select the type of software you want to find from the drop-down menu:
    - Programs only
    - Updates only
    - All software

Installations and uninstallations

- To show a history of all software changes made to the computer, click the **Installations and uninstallations** link:

Field	Description
Event	•  Software uninstallation. •  Software installation.
Name	Name of the installed program.
Publisher	Company that developed the program.
Date	Date the program was installed or uninstalled.
Version	Internal version of the program.

Table 8.38: Fields in the Installations and Uninstallations section

Settings section (9)

This tab shows the various settings profiles assigned to the computer and enables you to edit and manage them:

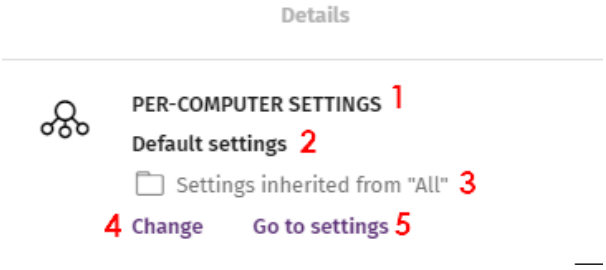


Figure 8.14: Example of inherited and manually assigned settings profiles

- **(1) Settings type**: Indicates the type of settings profile assigned to the computer. For more information about the types of settings available in Advanced EPDR, see **Introduction to the various types of settings profiles** on page **289**.
- **(2) Settings profile name.**
- **(3) Method used to assign the settings profile**: Directly assigned to the computer or inherited from a parent group.
- **(4) Button to change the settings profile assigned to the computer**.
- **(5) Button to edit the settings profile**.

> *For more information about how to create and edit settings profiles, see* ***Creating and managing settings profiles*** *on page* ***294***.

Action bar (10)

This resource groups together multiple actions you can take on the managed computers on your network:

Action	Description
Move to	Moves the computer to a standard group.
Move to Active Directory path	Moves the computer to its original Active Directory group.
Delete	Releases the Advanced EPDR license and removes the computer from the web console.
Scan now	Enables you to run a scan task immediately. For more information, see **On-demand computer scanning and disinfection** on page **879**.

Action	Description
Schedule scan	Enables you to schedule a scan task. For more information, see **On-demand computer scanning and disinfection** on page **879**.
Isolate computer	Prevents the computer from establishing external communications to help you perform forensic analysis tasks on compromised computers. For more information, see **Isolating one or more computers from the organization network** on page **890**.
Stop isolating the computer	Restores communications with other computers. For more information, see **Stopping isolation** on page **890**.
View available patches	Opens the **Available patches** list which shows patches that are pending installation on the computer. See **Cytomic Patch module lists** on page **477**.
Schedule patch installation	Creates a task that installs all released patches missing from target computers. For more information, see **Download and install patches** on page **442**.
Remote control	Runs remote control tools. See **Remote computer control** on page **892**.
Restart	Restarts the computer immediately. For more information, see **Computer restart** on page **888**.
Reinstall protection (requires restart)	Reinstalls the security software if a malfunction occurs. See **Remote reinstallation** on page **186**.
Reinstall agent	Reinstalls the agent if a malfunction occurs. See **Remote reinstallation** on page **186**.
Report a	Creates a support ticket for the Cytomic support department. For more

Action	Description
problem	information, see **Reporting a problem** on page **906**.

Table 8.39: Actions available from a computer details page

Hidden icons (11)

Depending on the size of the screen and the number of icons to show, some icons might be hidden under the ... icon. Click it to show the remaining icons.

Chapter 9

Managing settings

Settings, also called "settings profiles" or simply "profiles", offer administrators a simple way of establishing security, productivity, and connectivity parameters for the computers managed through Advanced EPDR.

Chapter contents

Strategies for creating settings profiles

Administrators can create as many settings profiles with different settings as necessary to manage network security for different types of computers and devices. We recommend that you create separate settings profiles for groups of computers with similar protection needs.

- Computers used by people with different levels of IT knowledge require different levels of permissiveness with respect to the running of software, access to the Internet, or to peripherals.
- Users with different tasks to perform and therefore with different needs require settings that allow access to different resources.
- Users who handle confidential or sensitive information require greater protection against threats and attempts to steal the organization's intellectual property.
- Computers in different offices require settings that allow them to connect to the Internet using a variety of communication infrastructures.
- Critical servers require specific security settings.

Overview of assigning settings profiles to computers

In general, assigning settings profiles to computers is a four-step process:

1. Creation of groups of similar computers or computers with identical connectivity and security requirements.
2. Assigning computers to the corresponding groups.
3. Assigning settings profiles to groups.
4. Deployment of settings profiles to network computers.

All these operations are performed from the group tree, which is accessed from the **Computers** menu at the top of the console. The group tree is the main tool for assigning settings profiles quickly and to large groups of computers.

Therefore, administrators must put similar computers in the same group and create as many groups as there are different types of computers on the network.

For more information about the group tree and how to assign computers to groups, see ***The Computer tree panel*** *on page* ***213****.*

Immediate deployment of settings profiles

After a settings profile is assigned to a group, it is applied to the computers in the group immediately and automatically, in accordance with the inheritance rules described in section **Indirect assignment of settings profiles: the two rules of inheritance**. These settings are applied to computers in just a few seconds.

For more information about how to disable the immediate deployment of settings profiles, see ***Configuring real-time communication*** *on page* ***317***.

Multi-level tree

In medium-sized and large organizations, there can be a wide range of settings profiles. To make it easier to manage large networks, Advanced EPDR enables you to create multi-level group trees so that you can manage all computers on the network with sufficient flexibility.

Inheritance

In large networks, it is highly likely that the administrator wants to reuse existing settings profiles already assigned to groups higher up in the group tree. The inheritance feature enables you to assign a settings profile to a group, applying it automatically to all groups below it in order to save time.

Manual settings

To prevent settings profiles from being applied to all lower levels in the group tree, or to assign settings profiles different from the inherited ones to a certain computer on a branch of the tree, you can manually assign settings profiles to groups or individual computers.

Default settings

Initially, all computers in the group tree inherit the settings profile established for the **All** root node. This node comes with a series of default settings created in Advanced EPDR with the purpose of protecting all computers from the outset, even before the administrator accesses the console to configure a security settings profile.

Introduction to the various types of settings profiles

A security settings profile is a group of settings for a specific security area that you use to configure the endpoint security product and specify how it operates on your network computers and devices. You assign profiles to one or more groups and all computers and devices in the groups receive the settings in the profile.

This is an introduction to the different types of settings profiles supported by Advanced EPDR.

Advanced EPDR enables you to configure these aspects of the service:

Settings	Description
Users	Manage the user accounts that can access the management console,

Settings	Description
	the actions they can take (roles), and their activity. For more information, see **Accessing, controlling, and monitoring the management console** on page **61**.
Per-computer settings	Specify how often to install Advanced EPDR updates on workstations and servers. You can also define settings to prevent tampering and unauthorized uninstallation of the protection software. For more information, see **Configuring the agent remotely** on page **307**.
Remote control	Specify access to user computers from the Cytomic Orion threat hunting product. For more information, see **Remote computer control** on page **892**.
Network settings	Specify the language of Advanced EPDR installed on workstations and servers. You can also define the type of connection to the Cytomic cloud. For more information, see **Configuring the agent remotely** on page **307** .
Network services	Specify how Advanced EPDR communicates with computers on the network: • **Proxy**: Define computers that act as a proxy to enable isolated computers with Advanced EPDR installed to access the cloud. For more information, see **Cytomic proxy role** on page **308**. • **Cache**: Define computers that act as a cache for signature files, security patches, and other components used to update the Advanced EPDR software installed on other computers and devices on the network. For more information, see **Cache role** on page **310**. • **Discovery**: Define computers that discover unprotected computers on the network. For more information, see **Discovery computer role** on page **312**.
VDI environments	Define the maximum number of computers that can be simultaneously active in a non-persistent virtualization environment.
My alerts	Configure alerts to send to the network administrator by email. For more information, see **Alerts** on page **855**.
Workstations and servers	Define how Advanced EPDR protects the computers on your network against threats and malware. For more information, see **Security settings**

Settings	Description
	for workstations and servers on page **327**.
IOC gallery	Import and export IOCs to and from the protection product and search protected computers for indicators of compromise. For more information, see **Detection and management of IOCs** on page **587**.
Indicators of attack (IOA)	Detect sophisticated infection strategies that use multiple attack vectors and operating system tools for extended periods of times. For more information, see **Indicators of attack settings** on page **609**.
Program blocking	Specify how Advanced EPDR must behave to block the execution of certain programs. For more information, see **Program blocking settings** on page **573**.
Authorized software	Prevent unknown programs in the process of classification from being blocked. For more information, see **Authorized software settings** on page **581**.
Mobile devices	Protect tablets and smartphones against threats, malware, and theft. For more information, see **Security settings for mobile devices** on page **363**.
Patch management	Specify when the protection software searches for new patches and software updates for the Windows operating systems and third-party applications installed across the network. For more information, see **Cytomic Patch (Updating vulnerable programs)** on page **435**.
Endpoint Access Enforcement	Monitor inbound connections to computers on the corporate network. Allow or block connections based on the security status of the connecting computer. For more information, see **Endpoint Access Enforcement settings** on page **518**.
Cytomic Data Watch	Monitor the personal data stored on the storage systems on your network. For more information, see **Cytomic Data Watch (Personal data monitoring)** on page **371**.
Encryption	Encrypt the content of your computer internal and external storage devices. For more information, see **Cytomic Encryption (Device encryption)** on page **539**.

Settings	Description
MDR	Describe the customer IT infrastructure a partner must monitor and protect from malware attacks and external threats. These settings can be accessed only if the customer has purchased the MDR service from a partner. For more information, see **MDR service settings** on page **657**.

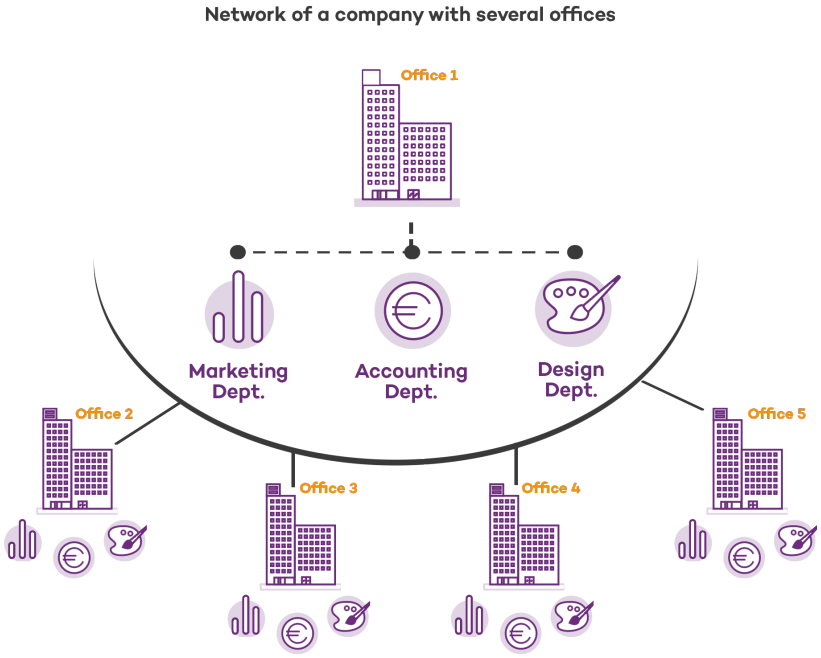
Table 9.1: Description of the types of settings profiles available in Advanced EPDR

Modular vs. monolithic settings profiles

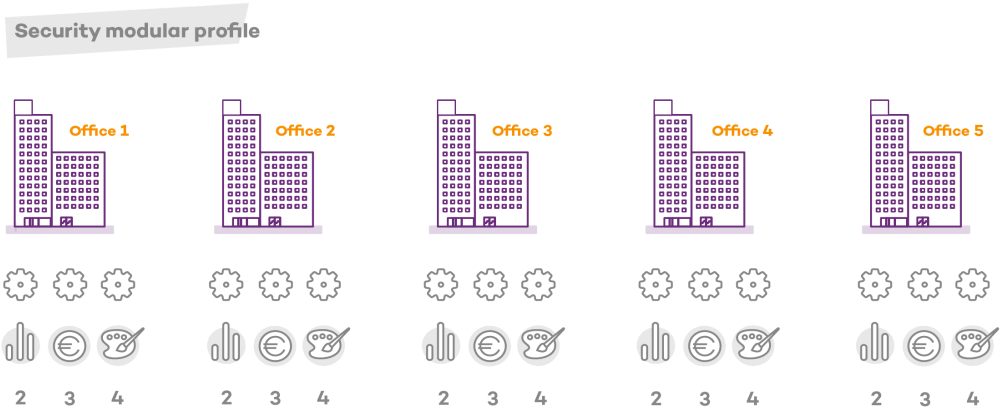
By supporting different types of profiles, Advanced EPDR uses a modular approach to creating and deploying the settings you want to apply to managed computers. The reason for using this modular approach and not just a single, monolithic profile that covers all the settings is to reduce the number of profiles created in the management console. This in turn reduces the time that administrators have to spend managing the profiles created. Modular profiles are lighter than monolithic profiles, which would result in numerous large and redundant settings profiles with little differences between each other.

Case study: Creating settings profiles for multiple offices

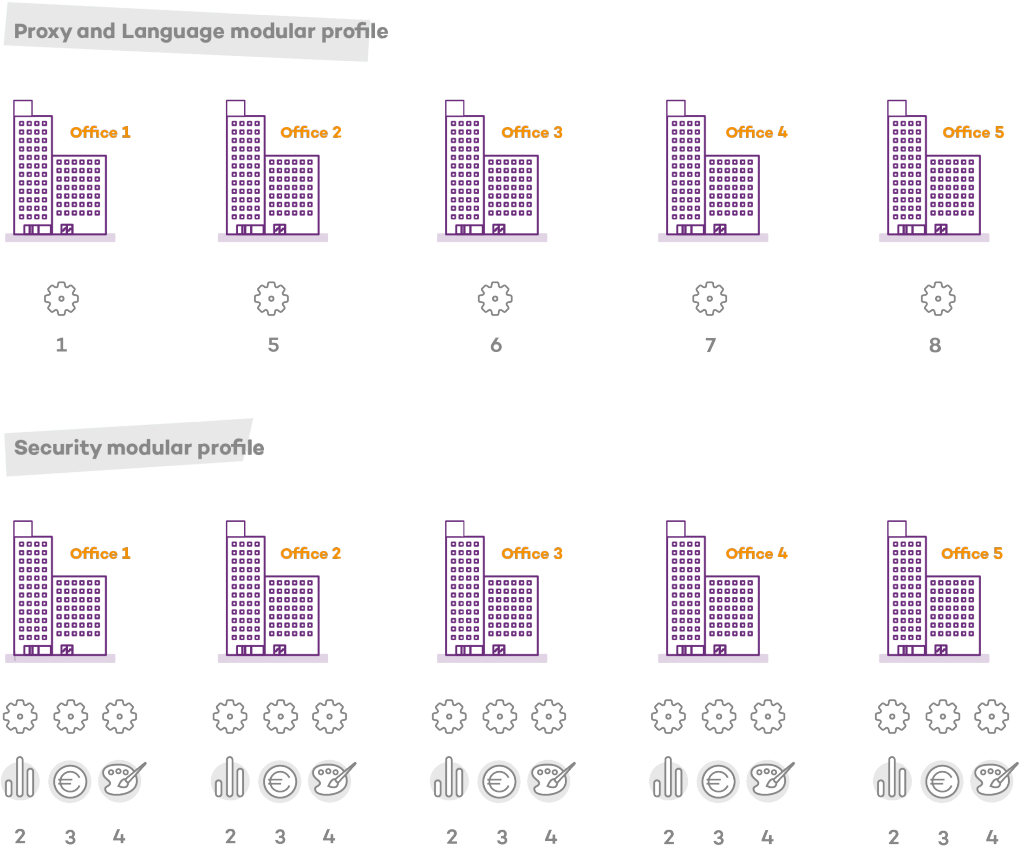
This example uses a company with five offices, each with a different communications infrastructure and therefore different proxy settings. Also, each office requires three different security settings profiles: one for the Design department, one for the Accounting department, and one for Marketing.



Using monolithic profiles, the company would require 15 different settings profiles (5 offices x 3 security settings profiles in each office = 15) to adapt to the needs of all three departments in the company offices.



However, because Advanced EPDR separates the proxy settings from the security settings, the number of profiles needed is reduced (5 proxy profiles + 3 department profiles = 8) as the security profiles for each department in one of the offices can be reused and combined with the proxy profiles in other offices.



Creating and managing settings profiles

From the top menu, select **Settings** to create, copy, and delete settings profiles.

The left pane shows the available types of security settings **(1)**. The right pane shows the settings profiles already created for the selected type **(2**), and buttons to add **(3)**, copy **(4)**, and delete profiles **(5)**. To search for a settings profile, type the name in the **Search** box **(6)**.

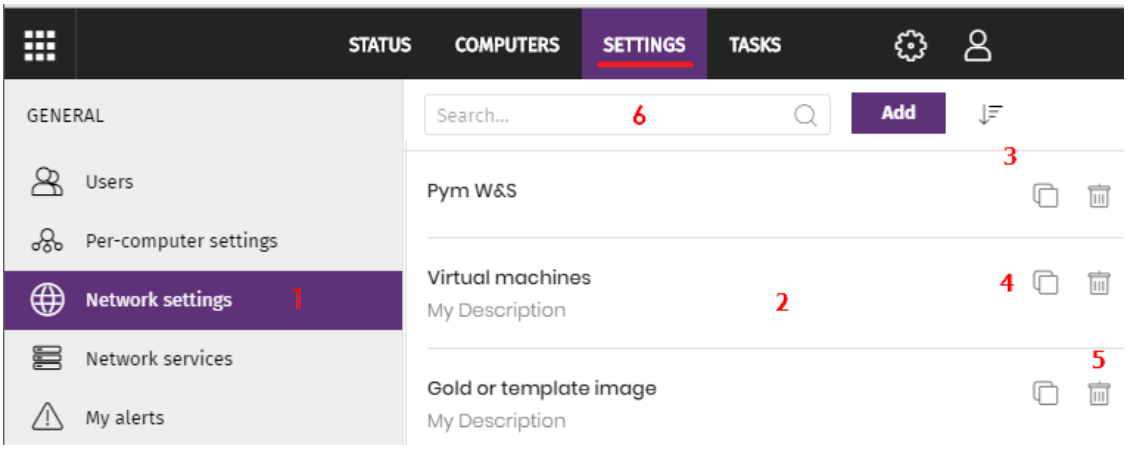


Figure 9.1: Page for creating and managing settings profiles

> *Settings profiles created from CYTOMIC Nexus and inherited from a service provider account display with a green CYTOMIC Nexus. When you point the mouse to the label, this message appears: "These settings are managed from CYTOMIC Nexus". Settings profiles created from CYTOMIC Nexus are read only. You can edit only their recipients. For more information, see section Settings management for Cytomic-based products in the* ***Panda Partner Center*** *Administration Guide.*

Creating a settings profile

Click **Add**. The **Add Settings** page opens. All profiles have a name and a description, which appear in the list of settings profiles.

To create a settings profile, bear in mind these limitations regarding permissions and visibility:

- To create a settings profile, the user account must have the relevant permission assigned. See **Understanding permissions** on page **72**.
- To assign recipients to a settings profile, the user account must have visibility of the computers to assign. See **Managing roles and permissions** on page **69**

Listing and sorting settings profiles

To see settings profiles of a specific type, the user account must have at least read permissions. See **Understanding permissions** on page **72**.

Click the  icon **(7)** to expand a context menu with these sort options:

- Sorted by creation date
- Sorted by name
- Ascending
- Descending

Copying a settings profile

To copy a settings profile, click the **(4)** icon. All settings are copied, except for the content of the **Recipients** field, which is empty.

To copy a settings profile, the user account must have the relevant edit permission assigned. See **Understanding permissions** on page **72**.

Editing a settings profile

When you edit an existing settings profile, your endpoint security product automatically applies your changes to computers on the network that use that settings profile.

- To edit a settings profile, select it. The **Edit settings** page opens.
- To save your changes, click **Save**.

To edit a settings profile, bear in mind these limitations regarding permissions and visibility:

- The user account must have the relevant edit permission assigned. See **Understanding permissions** on page **72**.
- To add recipients to a settings profile, the user account must have visibility of the relevant computers. See **Managing roles and permissions** on page **69**
- To remove recipients, the user account must have visibility of the relevant computers. See **Managing roles and permissions** on page **69**

Deleting a settings profile

To delete a settings profile, click the **(5)** icon. You cannot delete a settings profile that is assigned to a device or computer.

To delete a settings profile, the user account must have the relevant permission assigned. See **Understanding permissions** on page **72**.

Manual and automatic assignment of settings profiles

After you create a settings profile, you can assign it to one or more computers in two different ways:

- Manually (directly).
- Automatically (indirectly) through inheritance from a group to subgroups, computers, and devices.

Both strategies complement each other. It is highly advisable that administrators understand the advantages and limitations of each one in order to define the most simple and flexible computer structure possible to minimize the workload of daily maintenance tasks.

Manual/direct assignment of settings profiles

Consists of directly assigning settings profiles to computers or groups. It is the administrator who manually assigns a profile to a computer or computer group.

After you create a settings profile, there are many ways to manually assign it:

- From the **Computers** menu at the top of the console, from the group tree in the left panel.
- From the target computer's details, accessible from the **Computers** list.
- From the profile when it is created or edited.

*For more information about the group tree, see **Group tree** on page **222**.*

From the group tree

To assign a settings profile to a computer group:

- Click the **Computers** menu at the top of the console. From the left panel, select a filter or group.
- Click the group's context menu.
- Click **Settings**. A window opens with the profiles already assigned to the selected group and the type of assignment:
- **Manual/Direct assignment**: The text **Directly assigned to this group** is displayed.
- **Inherited/Indirect assignment**: The text **Settings inherited from** is displayed, followed by the name and full path of the group the settings profile is inherited from.

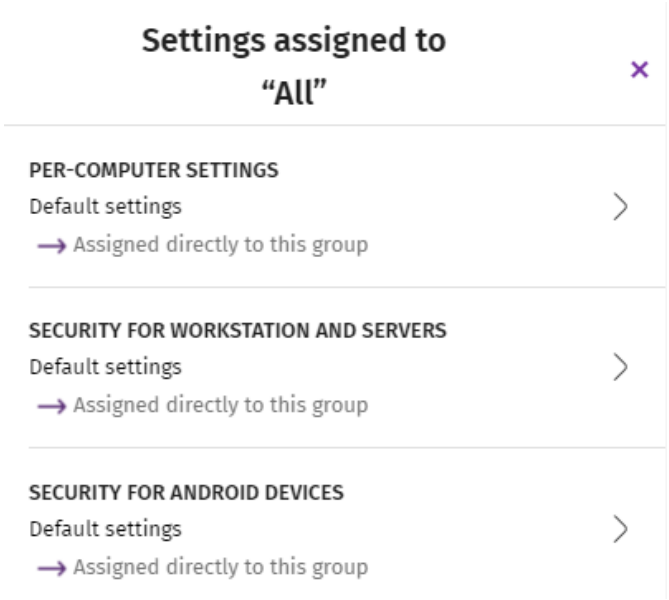


Figure 9.2: Example of inherited and manually assigned settings profiles

Select one of the available types of settings profiles. Select the specific settings profile to apply. Click **OK**. The profile is immediately deployed to all members of the group and its subgroups.

From the Computers list panel

To assign a settings profile to a specific computer or device:

- Go to the **Computers** menu at the top of the console. From the left panel, select the filter or group that contains the computer you want to assign the settings to. From the list of computers, select the computer. The computer details page opens.
- Select the **Settings** tab. A window opens with the profiles already assigned to the selected computer and the type of assignment:
    - **Manual/Direct assignment**: The text **Directly assigned to this group** is displayed.
    - **Inherited/Indirect assignment**: The text **Settings inherited from** is displayed, followed by the name and full path of the group the settings profile is inherited from.
- Select one of the available types of settings profiles. Select the specific settings profile to apply. Click **OK**. The profile is immediately applied to the computer.

From the settings profile

The fastest way to assign a settings profile to several computers belonging to different groups is from the settings profile itself.

To assign a settings profile to multiple computers or computer groups:

- Go to the **Settings** menu at the top of the console. From the left panel, select the type of settings you want to assign.

- Select a settings profile from the list. Click **Recipients**. The **Recipients** page opens. This page is divided into two sections: **Computer groups** and **Additional computers**.
- Click the ⊕ buttons to add individual computers or computer groups to the settings profile.
- Click **Back**. The profile is assigned to the selected computers and the settings are applied immediately.

> *If you remove a computer from the list of computers assigned to a settings profile, it re-inherits the security settings profile from the group it belongs to. A warning message is displayed in the management console before the computer is removed and the changes are applied.*

Indirect assignment of settings profiles: the two rules of inheritance

Indirect assignment of settings profiles takes place through inheritance, which enables automatic deployment of a settings profile to all computers below the node to which the settings were initially assigned.

The following is a description of the rules that govern the interaction between the two ways of assigning profiles (manual/direct and automatic/inheritance):

Automatic inheritance rule

A computer or computer group automatically inherits the settings of its parent group (the group above it in the hierarchy).

The settings are manually assigned to the parent group and automatically deployed to all child nodes (computers and computer groups with computers inside).

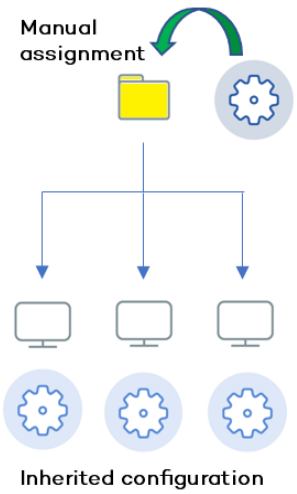


Figure 9.3: Inheritance/indirect assignment

Manual priority rule

Manually assigned settings take precedence over inherited settings.

When you manually assign a new settings profile to a group, all computers and devices below that group use the manually assigned settings, not the inherited or default ones.

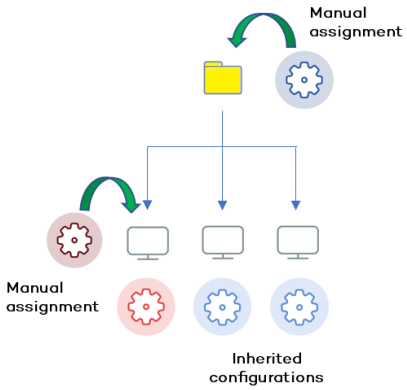


Figure 9.4: Precedence of manually assigned settings over inherited settings

Inheritance limits

Manually assigned settings override inherited settings from the higher-level group. That is, settings assigned to a group (manual or inherited) apply to all subgroups, computers, and devices unless manually assigned settings apply.

When the solution encounters manually assigned settings, that group and all of its subgroups, computers, and devices receive the manually assigned settings and not the original inherited ones.

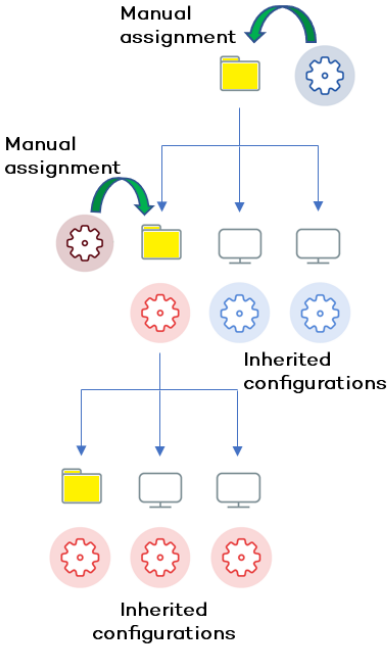


Figure 9.5: Inheritance limits

Overwriting settings

Manually assigned settings take precedence over inherited settings. When you manually assign a new settings profile to a group, all computers and devices below that group use the manually assigned settings, not the inherited or default ones.

Bearing that in mind, changes you make to settings in a higher-level group affect the groups, computers, and devices that inherit the settings differently, based on whether they have existing manually assigned or inherited settings. There are two scenarios:

- **Subgroups and computers with no manually assigned settings**: When you change settings in a group that are inherited by subgroups and computers that have no manual settings applied, the new settings automatically apply to all subgroups, computers, and devices in the group.
- **Subgroups and computers with manually assigned settings**: When you change settings in a group that are inherited by subgroups and computers that have manually assigned settings applied, any subgroups or computers with manually assigned settings do not inherit the new settings, regardless of the level.

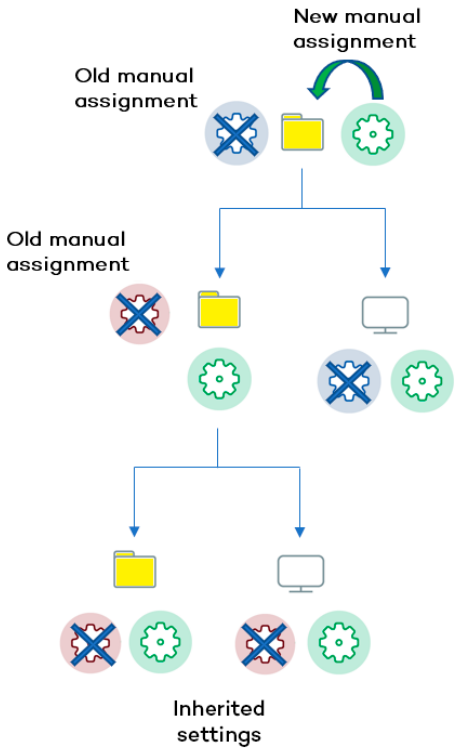


Figure 9.6: Overwriting manual settings

The solution prompts you to specify whether to **inherit the settings** or **keep the manually assigned settings**.

Make all inherit these settings

> *Be careful when you choose this option as this action is irreversible! When you select this option, all manually assigned settings below the parent node are removed and all groups and computers inherit the new settings. The wayAdvanced EPDR behaves might change on many computers on the network.*

The new directly assigned settings propagate through inheritance across the entire tree, overwriting the previously assigned settings up to the last-level child nodes.

Keep all settings

When you select this option, new settings apply only to groups and computers that do not have manually assigned settings.

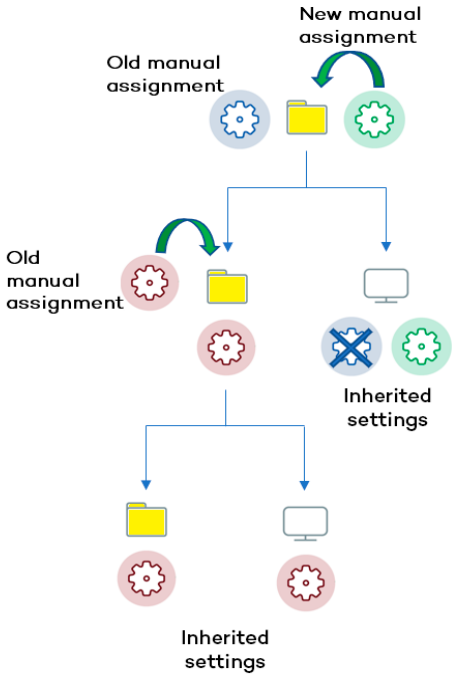


Figure 9.7: Keeping manual settings

Existing manual settings are retained and the application of new inherited settings stops at the first group or computer with manually configured settings.

Deleting manually assigned settings and restoring inheritance

To restore inheritance to a group or computer with manually assigned settings, you must delete the manually assigned settings:

- Go to the **Computers** menu at the top of the console. From the left panel, click the group with manually assigned settings that you want to delete.

- Click the branch's context menu icon and select **Settings**. A pop-up window opens with the profiles assigned to the group. Select the manually assigned profile you want to delete.
- A list is shown with all available settings profiles and the **Inherit from parent group** button. Click **Inherit from parent group**. The manually assigned settings are removed. The group inherits profile settings from the specified group.

Moving groups and computers

When you move computers from one branch in the tree to another, the way Advanced EPDR operates with respect to the settings profile to apply varies depending on whether the items moved are groups or individual computers.

Moving individual computers

All settings profiles that were manually assigned to the computer are kept. Inherited profiles are overwritten with the settings established in the new parent group.

Moving groups

A dialog box appears with the following question: "**Do you want the settings inherited by this group to be replaced by those in the new parent group?**"

- If the answer is **YES**, the process is the same as when you move a single computer: The manual settings are kept and the inherited settings are overwritten with those established in the parent node.
- If the answer is **NO**, both the manual settings and the original inherited settings of the group are kept.

Exceptions to indirect inheritance

All computers that are integrated into a native group in the web console automatically receive, from Advanced EPDR, the network settings assigned to the target group by means of the standard indirect assignment/inheritance mechanism. However, if a computer is a member of an Active Directory or IP-based group, you must manually assign network settings. This change in the way network settings are assigned results in a change in behavior if that computer is moved from an Active Directory or IP-based group to another group: It does not automatically inherit the network settings assigned to the target group, but retains its own.

This particular behavior of the inheritance feature is due to the fact that, in midsize and large companies, the department that manages security might not be the same as the one that manages the company's Active Directory. Therefore, a group membership change made by the technical department that maintains the Active Directory could inadvertently change network settings in the Advanced EPDR console and leave the protection agent installed on the affected computer without connectivity and full protection. To prevent settings changes when a computer

changes groups in the Advanced EPDR console because of a group change in Active Directory, you must manually assign network settings.

Settings profiles inherited from a partner

Partners are companies or organizations that deliver and manage security solutions remotely for their customers.

There are two types of partners:

- Resellers who assign products to their customers and manage them remotely.
- Companies that delegate security service management to each department, but also want to centrally oversee compliance of the protection policies that are common to the entire company.

To manage the protection software remotely, partners send settings profiles to their customers. These profiles appear in the management console with the CYTOMIC Nexus label.

Features of the settings profiles inherited from a partner

By default, you cannot edit or delete the settings profiles you inherit from a partner in the management console. Only if the partner marks them as editable can you modify certain aspects of their configuration. For more information, see **Exclusions set by a partner** on page **331** and **Software authorized by a partner** on page **582**.

Requirements

To receive settings profiles from a partner, follow these steps:

- From the top menu, select **Settings (1)**. From the left panel, select **Users (2).**
- Select the **Users** tab. Select **Allow my reseller to access my console (3)**.

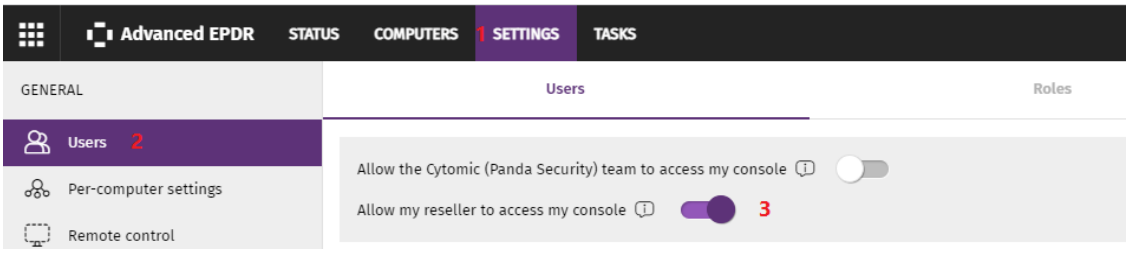


Figure 9.8: Option **Allow my reseller to access my console**

Viewing assigned settings profiles

The management console provides four methods of displaying the settings profiles assigned to a group or a single computer:

- From the group tree.
- From the Settings menu at the top of the console.
- From a computer's **Settings** tab.
- From the exported list of computers.

Viewing settings profiles from the group tree

- Click the **Computers** menu at the top of the console. Click the tab from the left panel to show the group tree.
- Click the context menu of the relevant branch. Select **Settings** from the pop-up menu displayed. A window opens with the settings profiles assigned to the folder.

The following is a description of the information displayed in the window:

- **Settings type**: Indicates the settings class the profile belongs to.
- **Name of the settings profile**: Name given by the administrator when configuring the profile.
- **Inheritance type**:
  - **Settings inherited from...:** The settings profile was assigned to a higher-level folder and every computer on the current branch has inherited it.
  - **Directly assigned to this group**: → The settings profile applied to the computers was manually assigned to the folder by the administrator.

Viewing settings profiles from the Settings menu at the top of the console

Go to the **Settings** menu at the top of the console. Select a type of settings from the left menu.

Select a settings profile from the list.

If the settings profile is assigned to one or more computers or groups, the **View computers** button is displayed.

Click the **View computers** button. The **Computers** page opens, with a list of all computers with the settings profile assigned, regardless of whether it was assigned individually or through computer groups. At the top of the page you can see the filter criteria used to generate the list.

Viewing settings profiles from a computer's Settings tab

Go to the **Computers** menu at the top of the console. Select a computer from the right panel. Click it to view its details. Go to the **Settings** tab to see the profiles assigned to the computer.

Viewing settings profiles from the exported list of computers

From the computer tree (group tree or filter tree), click the general context menu and select **Export**.

*See **Fields displayed in the exported file** on page **232** for more information.*

Chapter 10

Configuring the agent remotely

Administrators can configure various aspects of the Cytomic agent installed on the computers on their network from the web console:

- Define a computer's role towards the other protected workstations and servers.
- Protect the Advanced EPDR client software from unauthorized tampering by hackers and advanced threats (APTs).
- Define the visibility of the agent on the workstation or server, and the language it is displayed in.
- Configure the communications established between the computers on the network and the Cytomic cloud.
- Apply an additional layer of protection for VPN connections between remote computers and corporate networks.

Chapter contents

Configuring the Cytomic agent role

The Cytomic agent installed on the Windows computers on your network can have three roles:

- Proxy
- Discovery computer
- Cache

To assign a role to a computer with the Cytomic agent installed, select **Settings** from the top menu. Select **Network services** from the side menu. Four tabs appear: **Advanced EPDR proxy**, **Cache**, **Discovery**, and **Network Access Enforcement**.

Only computers that use the Windows operating system can take on the Proxy, Cache, or Discovery Computer roles.

Cytomic proxy role

To access the Cytomic cloud, the security software installed on computers requires access to the Internet. Isolated computers can access the Internet through the organization corporate proxy. If there is no corporate proxy, Advanced EPDR enables you to add or designate more than one computer on the network as a Cytomic proxy.

Computers designated as a Cytomic proxy can listen to requests from other computers and redirect them to the Cytomic cloud using a valid connection.

We recommend that you configure a Cytomic proxy only to enable isolated computers (those without an Internet connection, either direct or through a corporate proxy) to access the Cytomic cloud. A Cytomic proxy does not provide all the features of a corporate proxy and is designed only to access resources hosted in the Cytomic cloud.

Cytomic proxy computers can serve a variable number of devices, depending on the hardware resources installed. As a general rule, a proxy computer can serve a maximum of 100 computers.

Limitations of Cytomic proxy computers

For security reasons, when Advanced EPDR has the Cytomic proxy role assigned, it can connect only to the Cytomic cloud. For this reason, there are certain limitations with regard to the items the security software can download when it is configured to access the Internet through a Cytomic proxy node:

- **Windows and macOS**:
  - The security software cannot download patches through Cytomic Patch, but can report patches that are pending installation. See **Download and install patches** on page **442**.
- **Linux**:
  - The security software cannot download patches through Cytomic Patch, but can report patches that are pending installation. See **Download and install patches** on page **442**.
  - If the security software needs to download packages from repositories that are not accessible to the Cytomic proxy, installation is not possible. See **Protection engine updates** on page **204**.

These limitations do not apply to the company corporate proxy.

Requirements for designating a computer as a Cytomic proxy

- Windows operating system and Advanced EPDR product installed.
- Support for the 8.3 filename format. For more information on file name requirements, see this MSDN article: **https://docs.microsoft.com/en- us/previous- versions/windows/it-pro/windows-server-2003/cc778996(v=ws.10)?redirectedfrom=MSDN**.
- TCP port 3128 must not be in use by other applications.
- Port 3128 must be open for inbound and outbound connections.
- The proxy computer name must be resolved from the computer that uses it.

Designating a computer as a Cytomic proxy

- From the top menu, select **Settings**. From the side menu, select **Network services**. Select the **Proxy** tab. A list appears and shows all computers that have been designated as a proxy.
- Click **Add proxy server**. A dialog box opens and shows all computers managed by Advanced EPDR that meet the requirements for acting as a proxy on the network.
- Use the search box to find a specific computer and click it to add it to the list of computers designated as a proxy.

Removing a Cytomic proxy

- From the top menu, select **Settings**. From the side menu, select **Network services**. Select the **Proxy** tab. A list appears and shows all computers that have been designated as a proxy.
- Next to the computer you want to remove from the list, click  .

For information about how to configure the use of a proxy computer, see ***Configuring proxies lists for Internet access****.*

Cache role

Advanced EPDR enables you to assign the cache role to one or more computers on your network. These computers automatically download and store all files required by other computers with Advanced EPDR installed. This saves bandwidth because not every computer has to separately download the updates they need. All updates are downloaded centrally and only once for all computers that require them.

Limitations of cache computers

For security reasons, when Advanced EPDR has the cache role assigned, it can connect only to the Cytomic cloud. For this reason, there are certain limitations with regard to the items the security software can download when downloads are configured to occur through a cache node:

- Linux computers cannot download update patches through Cytomic Patch. See **Download and install patches** on page **442**.
- Linux computers cannot download packages to install or update the security software. See **Protection engine updates** on page **204**.

Cached items

A computer designated with the cache role can cache these items:

- **Signature files**: Cached until they are no longer valid.
- **Installation packages**: Cached until they are no longer valid.
- **Update patches for** Cytomic Patch: Cached for 30 days.

Cache computer capacity

The capacity of a cache computer depends on the number of simultaneous connections it can accommodate and the type of traffic it manages (such as signature file downloads or installer downloads). A cache computer can serve approximately 1,000 computers simultaneously.

Designating a computer as a cache computer

- Go to the **Settings** menu at the top of the console. Select **Network services** from the menu on the left. Select the **Cache** tab.
- Click **Add cache computer**.
- Use the search tool at the top of the window to quickly find those computers you want to designate as cache computers.
- Select a computer from the list and click **OK**.

The selected computer then has the role of cache, and downloads all files required to keep its repository automatically synchronized. All other computers on the same subnet contact the cache computer to download updates.

Removing the cache role from a computer

Go to the **Settings** menu at the top of the console. Select **Network services** from the menu on the left. Select the **Cache** tab.

Click  next to the computer you want to remove from the list.

Specifying the storage drive

You can configure the Advanced EPDR agent to store cached items on a specific drive of the cache computer. To specify the cache drive:

- Go to the **Settings** menu at the top of the console. Select **Network services** from the menu on the left. Select the **Cache** tab.
- Select a computer from the list of cache computers. Click the **Change** link. A dialog box opens and shows the available drives.
- The following information is shown for each drive: volume name, mapped drive, free space, and total space.

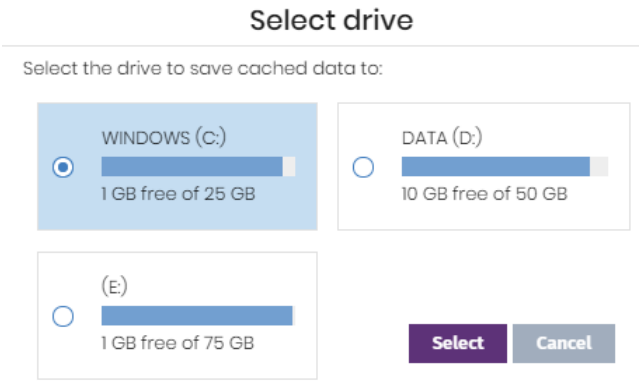


Figure 10.1: Volume selection window for a cache computer

- To view the space on a drive, point the mouse at the relevant bar. A tooltip shows the percentage of used and free space.
- Only drives with 1 GB or more of free space are available to store cached items. Select the drive where you want to store the cached items and click the **Select** button. Advanced EPDR starts to copy the cached items. When the process is complete, the items are deleted from their original location.

> *You can only select a drive on a computer which has reported its status to the Advanced EPDR server. If the drive has not reported its status, the drive that stores the Advanced EPDR installation files is selected by default. After the status has been reported, the **Change** link for the cache computer is shown, and you can select the storage drive. It might take several minutes for a computer to report its status.*

If there is not enough free space or a write error occurs when you select the drive, an error message appears below the cache computer and indicates the cause of the problem.

Discovery computer role

Click the **Settings** menu at the top of the console and select **Network services** from the menu on the left. You will find the **Discovery** tab, which is directly related to the installation and deployment of Advanced EPDR across a customer's network.

> *See **Viewing discovered computers** on page **125** for more information about the Advanced EPDR discovery and installation processes.*

Configuring proxies lists for Internet access

Advanced EPDR enables you to assign computers on the network one or more Internet connection methods, based on the resources available in the company's IT infrastructure.

There are two lists of connection methods:

- **Access list**: Contains the connection methods you configure.
- **Fallback list**: This is a non-editable list included by default in Advanced EPDR.

If a connection method appears in both lists, it is automatically removed from the fallback list.

Access list

This list contains the access methods you configure. The agent traverses the list from the start when it needs to connect to the Cytomic cloud. After it finds an access method that works, the agent continues to use it until it fails, at which point Advanced EPDR traverses the list from the start again until it finds one that works. If the solution reaches the end of the list without finding an access method that works, it searches for one in the fallback list. See **Fallback list**.

The connection types supported in the access list are:

Proxy type	Description
Do not use proxy	Direct access to the Internet. Computers access the Cytomic cloud directly to download updates and report their status. If you select this option, the Advanced EPDR software communicates with the Internet using the computer settings.
Corporate proxy	Access to the Internet through a proxy installed on the company's network. • **Address**: The proxy server IP address. • **Port**: The proxy server port. • **The proxy requires authentication**: Select this option if the proxy requires a user name and password. • **User name**: The user name of an existing proxy account. • **Password**: The proxy account password.
Automatic proxy discovery using the Web Proxy Auto-Discovery Protocol (WPAD)	Queries the network using DNS or DHCP to get the discovery URL that points to the PAC configuration file. Alternatively, you can directly specify the HTTP or HTTPS resource that hosts the PAC configuration file. This option is not supported on Linux. It is ignored. We recommend

Proxy type	Description
	that you do not use it for that operating system.
Advanced EPDR proxy	Access to the Cytomic cloud through a computer on the network with the Cytomic proxy role assigned. An access list can contain multiple Cytomic proxies. For more information about the access limitations of a Cytomic proxy and how to assign that role to a computer on the network, see **Cytomic proxy role**.

Table 10.1: Types of Internet access methods supported by Advanced EPDR

Configuring an access list

To configure an access list, create a **Network settings** profile:

- Click the **Settings** menu at the top of the console. Select **Network settings** from the side menu. Click the **Add** button or select an existing settings profile to edit it.
- In the **Proxy** section, click the icon. A window opens with a list of all available connection types.
- Select one of the connection types (**Types of Internet access methods supported by Advanced EPDR**) and click the **OK** button. The connection type is added to the list.
- To modify the order of the connection methods, select an item by clicking its checkbox and use the and arrows to move it up and down in the list.
- To delete a connection method, click the icon.
- To modify a connection method, select it by clicking its checkbox and click the icon. A window opens, where you can edit the method settings.

Fallback list

When the agent cannot connect to the Cytomic platform despite having tried all the connection methods in the access list you configured, it traverses the fallback list from the start. This list cannot be edited by you. After the Cytomic agent finds a connection method that works, it continues to use it until it fails, at which point the agent traverses the access list you configured from the start until it finds one that works. If none of the access methods in the access list or the fallback list works, the agent returns a communication error.

The fallback list is fixed and contains these access methods (not all access methods are available for all platforms):

- **Internet Explorer**: Advanced EPDR tries to retrieve the Internet Explorer proxy settings by impersonating the user account that logged in to the computer. This method is only available for Windows operating systems.
    - This method cannot be used if the proxy credentials have been explicitly defined.
    - If the Internet Explorer proxy settings have been configured using a proxy auto-config (PAC) file, the solution will obtain the URL of the configuration file only if the protocol for accessing the resource is HTTP or HTTPS.
- **Default proxy**: Advanced EPDR reads the operating system's default proxy settings.
- **WPAD**: Advanced EPDR uses DNS or DHCP to query the network and get the discovery URL that points to the proxy auto-configuration (PAC) file. This option is not supported on Linux.
- **Direct connection**: Advanced EPDR tries to connect directly to the Cytomic cloud.

Configuring downloads from cache computers

There are two ways to use computers with the cache role:

- **Automatic mode**: In this mode, a computer that starts a download uses cache computers found on the network that meet the requirements specified in section **Requirements for using a computer with the cache role assigned** . If multiple cache computers are found, the solution automatically balances the downloads so that a single cache computer is not overloaded.
- **Manual mode**: In this mode, you select the cache computers that download data from the Cytomic cloud. You order these computers in a list in the Network Settings. Manually selected cache computers differ from automatically selected ones in the following aspects:
    - When a computer has multiple cache computers assigned, it does not automatically share downloads among them.
    - If the first cache computer in the list is not available, the computer tries the next computer until it finds one that works. If it cannot find any available computers, the solution will try to access the Internet directly.

Requirements for using a computer with the cache role assigned

Automatic mode

- The computer with the cache role assigned and the computer that downloads items from it must be on the same subnet. If a cache computer has multiple network cards, it is able to act as a repository on each network segment to which it is connected.

We recommend that you designate a computer with the cache role on each network segment on the corporate network.

- All other computers automatically discover the presence of the cache computer and redirect their update requests to it.
- The cache computer must have a protection license assigned.
- The firewall must be configured to allow incoming and outgoing Universal Plug and Play (UPnP) and Simple Service Discovery Protocol (SSDP) traffic on:
    - UDP port 21226
    - TCP port 18226

Manual mode

- The computer with the cache role assigned and the computer that downloads items from do not need to be on the same subnet.
- The cache computer must have a protection license assigned.
- The firewall must be configured to allow incoming and outgoing traffic on:
    - UDP and TCP port 21226
    - TCP port 18226

Discovery of cache computers

When you designate a computer as cache, it broadcasts its status to the network segments to which its interfaces connect. All workstations and servers set to automatically detect cache computers receive the notification and connect to the cache computer. If there is more than one designated cache computer on a network segment, computers on the subnet connect to the most appropriate one based on the amount of free resources it has.

Occasionally, computers on the network set to automatically detect cache computers check whether there are new computers with the cache role.

Configuring the assignment method for cache computers

- Select the **Settings** menu at the top of the console. Select **Network settings** from the side menu. Select one of the existing settings profiles.
- Go to the **Cache** section. Select one of the following two options:
    - **Automatically use the cache computers seen on the network**: Computers that receive these settings automatically look for cache computers on their network segment.

- **Use the following cache computers (in order of preference)**: Click the ⊕ icon to add computers designated as a cache and set up a list of cache computers. Computers that receive these settings connect to the cache computers specified in the list.

Configuring real-time communication

Advanced EPDR communicates with the Cytomic platform in real time to retrieve the settings profiles configured for protected computers in the console. Therefore, only a few seconds pass between the time the administrator assigns a settings profile to a computer and the time it is applied.

Real-time communication between the protected computers and the Advanced EPDR server requires that each computer keep a connection open at all times. However, in organizations where the number of open connections might have a negative impact on the performance of the installed proxy, it may be advisable to disable real-time communication. The same applies to those organizations where the traffic generated when simultaneously pushing configuration changes to a large number of computers might impact bandwidth usage.

Requirements for real-time communication

- Real-time communications are compatible with all operating systems supported by Cytomic, except Windows XP and Windows 2003.
- If a computer accesses the Internet through a corporate proxy, the HTTPS connections must not be manipulated. Many proxies use Man-in-the-Middle techniques to scan HTTPS connections or work as cache proxies. When that happens, real-time communications do not work.

Disabling real-time communication

- Click the **Settings** menu at the top of the console. Select **Network settings** from the side menu. Click the **Add** button or select an existing settings profile to edit it.
- In the **Proxy** section, click **Advanced options**. Clear the **Enable real-time communication** checkbox.

If you disable real-time communication, your computers will communicate with the Advanced EPDR server every 15 minutes.

Configuring the agent language

To configure the language of the Cytomic agent for one or more computers, you must create a **Network settings** profile:

- Click the **Settings** menu at the top of the console. Select **Network settings** from the side menu. Click the **Add** button or select an existing settings profile to edit it.
- Go to the **Language** section and select a language from the list:
    - German
    - Spanish
    - Finnish
    - French
    - Hungarian
    - English
    - Italian
    - Japanese
    - Portuguese
    - Russian
    - Swedish

If the language is changed while the Advanced EPDR local console is open, the system will prompt the computer user to restart the local console. This does not affect the security of the computer.

Configuring the agent visibility

In those companies where the security service is 100% managed by the IT Department, there is no need for the Advanced EPDR agent icon to be shown in the notification area of managed computers. To show or hide the icon, follow the steps below:

- Click the **Settings** menu at the top of the console. Select **Per-computer settings** from the side menu.
- Click an existing settings profile or click **Add** to create a new one.
- Open the **Preferences** section and select or clear the **Show icon in the system tray** option.

Network Access Enforcement

Network Access Enforcement provides an extra layer of security when a user device (desktop, server, laptop, or mobile device) connects to your corporate network either remotely using a VPN connection or locally using a Wi-Fi connection.

The user device that tries to connect to the corporate network using a VPN or a Wi-Fi connection must meet a series of security requirements for the connection to be allowed. If it does not meet those requirements, the connection is rejected.

The Cytomic agent installed on the user device collects and sends the information that the Firebox or access point requires to verify that the device meets the necessary requirements.

Random UUID and authentication key generation

A UUID (Universal Unique Identifier) is a character string used to uniquely identify a device.

The Firebox or access point uses a UUID and authentication key to validate VPN or Wi-Fi network connections. Specify the same UUID-authentication key pair on the Firebox and in the Advanced EPDR console.

If you have not configured a UUID on a local-managed Firebox, you must generate one. UUID is an open format. To generate a random UUID, there are free tools available from vendors such as Microsoft or **https://www.uuidgenerator.net/**.

Use a long authentication key that includes uppercase, numeric, and special characters.

*For more information about the Firebox and the VPN connection settings, see **Network Access Enforcement Overview**.*

Requirements

For a user device to connect to the corporate network, it must meet these security requirements:

- It must have the security software installed, running, and correctly configured.
- You must have a valid UUID and authentication key configured on the device that validates the connection and in the Advanced EPDR console.
- **Operating system installed on the user device**:
  - Windows 8.1 or higher.
  - macOS Catalina 10.15 or higher.
  - Android 6 or higher.

> *With Android, unlike Windows or macOS, the Firebox console user cannot select the operating system version. On devices that run Android 6.0 or higher, Network Access Enforcement enables after they receive the relevant settings from the Cytomic servers.*

- **Open ports on the user device**: The Cytomic agent requires that TCP port 33000 be open to communicate with the device that validates the connection.
- **Security software settings**: Advanced EPDR advanced protection must be enabled in hardening or lock mode, or antivirus enabled and running.

> *Network Access Enforcement does not support Linux devices.*

Requirements verification

When a user device tries to connect to the corporate network, the device that validates the connection performs these actions:

- Requests information about the status of the protection installed on the user device.
- Verifies the account UUID and the authentication key are valid.
- Verifies the user device operating system against the operating systems defined in its settings.

If all requirements are met, the user device is allowed to access the corporate network. Otherwise, the connection is rejected.

> *By default, all devices are forced to comply with the security requirements to connect to the corporate network.*

Accessing the Network Access Enforcement settings

- From the side menu, select **Network services**.
- Select the **Network Access Enforcement** tab.
- To enable the protection, click the toggle.
- Enter the account UUID and the authentication key.
- Click **Save changes**.

Configuring security against protection tampering

To prevent unauthorized users from disabling the protection, Advanced EPDR enables you to set these limitations for the uninstallation and configuration of the security software on user computers:

- **Set a first authentication factor** (based on a password) to configure, disable, or uninstall the security software from the computer. Compatible with Windows and Linux computers.
- **Set a second authentication factor** (based on a QR code) to configure, disable, or uninstall the security software from the computer. Compatible with Windows and Linux computers. To use the second authentication factor, you must:
    - Have access to a smartphone or tablet with a built-in camera.
    - Download the WatchGuard AuthPoint app (or another authenticator app) for free from:
        - **iOS**: **https://apps.apple.com/app/watchguard-authpoint/id1335115425**
        - **Android**: **https://play.google.com/store/apps/details?id=com.watchguard.authpoint**
- **Enable anti-tamper protection**: Many advanced threats use techniques for disabling the security software installed on computers. Anti-tamper protection prevents tampering of the security software operation by enabling you to configure a password that prevents the software from being stopped, paused, or uninstalled. Compatible with Windows and Linux computers.
- **Enable protection when the computer starts in Safe Mode**: Some types of malware force Windows computers to restart in Safe Mode with networking enabled. In this mode, antivirus is automatically disabled and computers are vulnerable. You can configure Advanced EPDR to protect computers when they start in Safe Mode with networking enabled, so that all configured protections remain active and working normally. Compatible with Windows computers.

If a computer loses its license because it is manually removed or because it expires or is canceled, the anti-tamper protection and password-based uninstallation protection are disabled.

To configure security against tampering:

- From the top menu, select **Settings**. From the side menu, select **Per-computer settings**.
- Select an existing settings profile, or click **Add** to create a new profile.
- Select **Security against unauthorized protection tampering**:

- To **Request password to uninstall the protection from computers**, enable the toggle. In the **Password required to perform advanced management tasks locally from your computers** text box, type a password that is between 6 and 15 characters in length.
- To **Allow the protections to be temporarily enabled/disabled from the computers' local console**, enable the toggle. In the **Password required to perform advanced management tasks locally from your computers** text box, type a password that is between 6 and 15 characters in length.
- To **Enable Anti-Tamper protection (prevents users and certain types of malware from stopping the protections)**, enable the toggle. In the **Password required to perform advanced management tasks locally from your computers** text box, type a password that is between 6 and 15 characters in length.
- To **Enable protection when Windows computers start in Safe Mode**, enable the toggle. The protection starts working when a computer starts in Safe Mode with networking.
- To enable the second authentication factor, see **Enabling two-factor authentication (2FA)**.

Enabling two-factor authentication (2FA)

Generally, the security software is protected against tampering from third parties through a single password mechanism. Nevertheless, you can add an additional authentication factor for the security software. This additional authentication factor is obtained through a QR code generated in the console and which must be imported to the AuthPoint app or another app that generates authentication tokens.

To generate the QR code, Advanced EPDR requires a keyword. Each keyword generates a specific QR code.

After you enable two-factor authentication in a **Per-computer settings** profile, and the authenticator app reads the QR code, the administrator must provide both the password set in the console and the token generated by the authenticator app to uninstall the agent or change its settings.

Depending on the number of administrators who use the console, you can generate a single QR code for the entire account or multiple different codes. You can share a QR code to all **Per-computer settings** profiles in the account, to some profiles only, or even assign a unique QR code to each **Per-computer settings** profile.

Generating a unique QR code at account level

The QR code is automatically generated at account level and applied to all settings profiles that have the **Use a QR code shared across the entire account** setting enabled.

- From the top menu, select **Settings**. From the side menu, select **Per-computer settings**.
- Select an existing settings profile, or click **Add** to create a new profile.
- Select **Security against unauthorized protection tampering**.

- Select the **Enable Two-Factor Authentication (2FA)** toggle.
- Select **Use a QR code shared across the entire account**.
- Click **Show QR code**. A dialog box opens that shows the QR code generated for all the **Per-computer settings** profiles in the account.
- Scan the QR code in the AuthPoint app (or another authenticator app).
- Click **Close**.
- Click **Save**.

Generating a QR code for a single settings profile

The console prompts for a keyword to generate a QR code that is applied to a specific **Per-computer settings** profile.

- From the top menu, select **Settings**. From the side menu, select **Per-computer settings**.
- Select an existing settings profile, or click **Add** to create a new profile.
- Select **Security against unauthorized protection tampering**.
- Select the **Enable Two-Factor Authentication (2FA)** toggle.
- Select **Generate a QR code for this configuration**.
- Click **Generate code**.
- Enter a 6- to 20-character combination of letters and numbers for the QR code key. This QR code key (passphrase) is linked to the generated QR code. You can reuse the QR code key in other **Per-computer settings** profiles to enable two-factor authentication.
- Click **Generate code**.
- Click **Close**.
- Click **Save**.

Sharing a QR code to multiple settings profiles

To assign an existing QR code to another **Per-computer settings** profile:

- From the top menu, select **Settings**. From the side menu, select **Per-computer settings**.
- Select the settings profile from which you want to copy the QR code.
- Select **Security against unauthorized protection tampering**.
- In **Generate a QR code for this configuration**, click **Show QR code**. A dialog box opens and shows the QR code and the QR code key.
- Copy the QR code key to the clipboard.

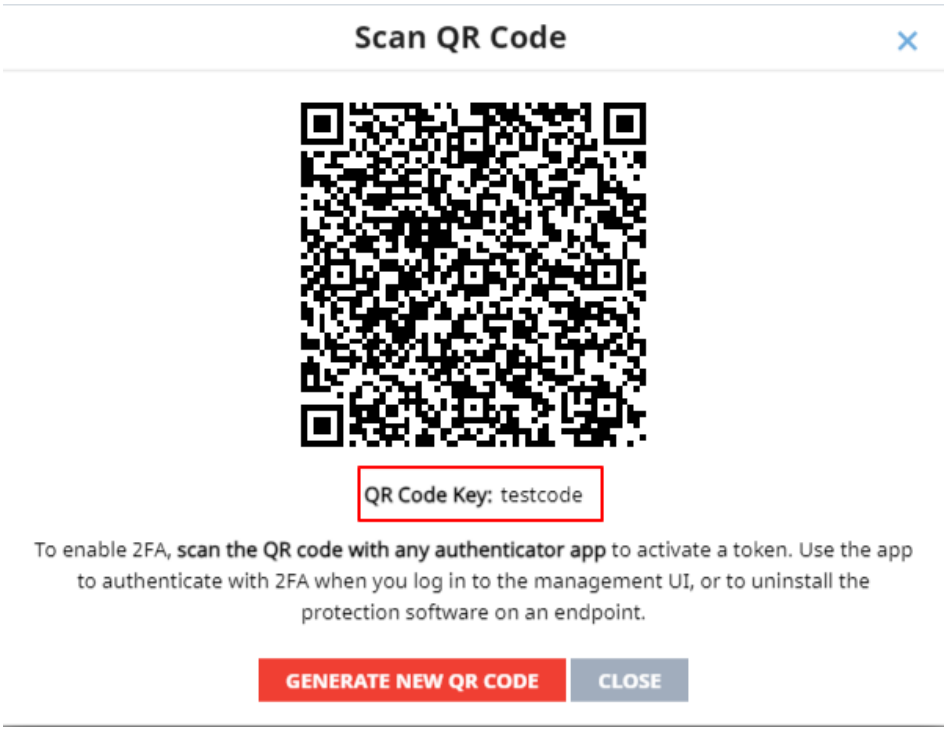


Figure 10.2: QR code and associated QR code key

- In the dialog box, click **Close**. On the settings profile page, click **Close**.
- Select the settings profile where you want to use the QR code you copied, or click **Add** to create a new profile.
- Select **Security against unauthorized protection tampering**.
- Select the **Enable Two-Factor Authentication** toggle.
- Select **Generate a QR code for this configuration**.
- Click **Generate code**.
- In the text box, paste the QR code key you copied.
- Click **Generate code**.
- Click **Close**.
- Click **Save**.

Exceptions when you copy a security settings profile with anti-tamper protection enabled

When you copy a settings profile with a password and/or two-factor authentication enabled, the security software behaves as described in **Copying a settings profile** on page **295**, except:

- The copied profile does not include the password specified in the **Password required to perform advanced management tasks locally from your computers** text box. The

administrator must enter a new password.

- If the administrator copies a settings profile inherited from a partner, Advanced EPDR automatically enables the **Generate a QR code for this configuration** option and generates a new QR code. It does not copy the password specified in the **Password required to perform advanced management tasks locally from your computers** text box.

Configuring shadow copies

Shadow copies is a technology included in Windows computers that can create a snapshot of computer files, even when they are in use.

From Advanced EPDR, you can remotely interact with the Windows Shadow Copies service on the computers on the network, using it as a remediation tool against ransomware attacks.

Characteristics of shadow copies in Advanced EPDR

Advanced EPDR complements the Shadow Copies service included in Microsoft Windows with additional features to protect user data from threats:

- Enables you to configure and manage a backup (snapshot) repository separately from other repositories the user might have created.
- Protects the service and the snapshots from changes made by threats or the user. This prevents the service from being stopped or the backup copies made by Advanced EPDR from being deleted.
- Enables you to specify the percentage of hard disk space to use for backup copies (this is 10% by default).
- Makes a backup copy of the files every 24 hours. The first copy is made when you enable the feature (it is disabled by default).
- Retains up to 7 copies of each file at a given time, depending on the free space allocated to the repository. If there is not enough space, older backup copies are deleted.

Requirements

- Operating system:
    - Windows Vista, Windows 7, or higher.
    - Windows 2003 Server 2012 or higher.
- Enough free disk space to make backup copies.
- Storage media identified by the operating system as fixed (internal and USB-connected hard disks) and NTFS disks.

Accessing the shadow copies feature

- From the top menu, select **Settings**. From the side menu, select **Per-computer settings**. A list opens and shows all created settings profiles.
- Select an existing settings profile or create a new one.
- In the **Shadow Copies** section, click the toggle to enable the feature. Specify the percentage of disk space you want to use for backup copies on user computers.

Although Advanced EPDR uses snapshots that are independent of the ones created by the user or the network administrator, all of them share the same settings. Additionally, the maximum space value you set for shadow copies in the management console has priority over other space settings established by the network administrator.

Using filters to find computers with shadow copies enabled

- From the top menu, select **Computers**.
- In the side panel, click the  icon. The filter tree appears.
- Select a folder. Click the icon. A context menu appears.
- Select **Add filter**. The **Add filter** dialog box opens.
- Configure the filter with these values:
  - **Category**: Computer
  - **Property**: Shadow Copies
  - **Operator**: Is equal to
  - **Value**: Enabled

*For more information, see **Configuring filters** on page **218**.*

Chapter 11

Security settings for workstations and servers

Configure security settings profiles for workstations and servers to define how Advanced EPDR protects the computers on your network against threats and malware.

Next is a description of the options available for configuring the security of your workstations and servers. We also provide practical recommendations on how to protect all computers on your network, without negatively impacting users' activities.

For additional information about the Workstations and servers module, see:

Creating and managing settings profiles *on page* ***294****: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*

Accessing, controlling, and monitoring the management console *on page* ***61****: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*

Chapter contents

Accessing the settings and required permissions

Accessing the settings

- Click the **Settings** menu at the top of the console. Select **Workstations and servers** from the side menu.
- Click the **Add** button. The **Workstations and servers** settings page opens.

Required permissions

Permission	Access type
Configure security for workstations and servers	Create, edit, delete, copy, or assign settings profiles for workstations and servers.
View security settings for workstations and servers	View the Workstations and servers settings profiles.

Table 11.1: Permissions required to access the Workstations and servers settings

Introduction to the security settings

The parameters for configuring the security of workstations and servers are divided into various sections. Click each of them to display a drop-down panel with the associated options. Next is a brief explanation of each section:

Section	Description
General	Configure updates, the removal of other security products, and file exclusions from scans.
Advanced protection	Configure the behavior of advanced protection and anti-exploit protection against APTs, targeted attacks, and advanced malware capable of leveraging exploits.
Antivirus	Configure parameters that control the traditional anti-malware protection against viruses and threats.

Section	Description
Firewall (Windows devices)	Configure parameters that control the firewall and the intrusion detection system (IDS) against network attacks.
Device control (Windows devices)	Configure parameters that control user access to the peripheral devices connected to the computer.
Web access control	Restrict access to web content categories and unknown pages.
Audit mode	Monitors the processes run on Windows, macOS, and Linux computers. It detects and reports threats, but does not block or delete them. Enabling Audit mode for a settings profile does not change the overall status of the protections applied to the computers that receive the settings. Nor does it change the configuration of the protections in the web console.

Table 11.2: Available modules in Advanced EPDR

Not all features are available for all supported platforms. This table provides a summary of the features in Advanced EPDR that are available for each supported platform:

Feature	Windows	macOS	Linux
Advanced protection	X		X
Anti-exploit protection	X		
Antivirus (1)	X	X	X
Firewall & Intrusion Detection System (IDS)	X		
Email protection	X		
Web protection	X	X	
Device control	X		
Web access	X	X	

Feature	Windows	macOS	Linux
Audit mode	X	X	X

Table 11.3: Supported security features by platform

General settings

The general settings enable you to configure how Advanced EPDR behaves with respect to updates, the removal of competitor products, and file and folder exclusions from scans.

Local alerts

Field	Description
Show malware, firewall, and device control alerts	In the text box, type a custom message to include in the alert. The Advanced EPDR agent will show a pop-up window with the content of the message. This feature is available for computers with a Windows, macOS, or Linux operating system installed.
Show an alert every time the web access control feature blocks a page	A pop-up window displays on the workstation or server every time Advanced EPDR blocks a web page. This feature is available for computers with a Windows or macOS operating system installed.

Table 11.4: Fields in the Local Alerts section

Updates

For more information about how to update the agent, the protection, and the signature file of the client software installed on user computers, see ***Product updates and upgrades*** *on page* ***203****.*

Uninstall other security products

For more information about how to configure the action to take if another security product is already installed on user computers, see ***Protection deployment overview*** *on page* ***104****.*

For a complete list of the competitor products that Advanced EPDR uninstalls automatically from user computers, see ***Supported uninstallers****.*

Files and paths excluded from scans

Configure items on your computers that you do not want the security software to block, delete, or disinfect when it scans for malware.

Exclusions disable antivirus and advanced protection for the specified files and file paths. Because this setting can cause potential security issues, we recommend that you only exclude files and paths to resolve performance problems.

Exclusions set by a partner

If your service provider changes the status of the settings profile from editable to non-editable, the exclusions you added no longer apply. Only the exclusions from the service provider apply. If the service provider changes the configuration again to be editable, then the exclusions you previously added are restored and applied..

Exclude the following disk files

Specify the files on the hard disk of your protected computers that you do not want Advanced EPDR to delete or disinfect.

We recommend that you use wildcards for Windows computers or substring matches for Linux/macOS computers as little as possible to be as specific as possible with regard to the files to exclude from scans.

Field	Description
Extensions	Specify the extensions of files you do not want to scan.

Field	Description

Folders	Specify the folders whose files you do not want to scan.
	Windows:
	• You can use variables in these cases:
	  • You can use system variables to exclude folders scanned by the antivirus module.
	  • You can use system and user variables to exclude folders monitored by the advanced protection module.
	• You cannot use user-created variables.
	• You cannot use willdcards.
	Linux/macOS:
	• You cannot use system or user variables.
	• You can specify partial paths.

Files	Specify the files you do not want to scan. **Windows:** • You can use the wildcard characters ? and * when you do not specify the path and you indicate the file name only. • You cannot use wildcards when you specify the full path to a file. • If you do not specify a file path, the file is excluded from scans in all folders where it is located. If you specify the path, the file is excluded from scans only in that folder. **Linux/macOS:** • You cannot use wildcard characters ? or *. • If you do not specify a file path, the file is excluded from scans in all folders where it is located. If you specify the path, the file is excluded from scans only in that folder. • You can specify the partial name of a file.

Table 11.5: Disk files you do not want Advanced EPDR to scan

To prevent advanced protection from blocking trusted software, even temporarily, and make sure that telemetry data is sent to Cytomic to analyze application behavior, we recommend that you use the authorized software module instead of exclusions. For more information, see ***Authorized software settings*** *on page* ***581***.

Example: Exclude files on Windows computers

To exclude file `C:\Users\mike\desktop\data.txt`:

- **Files** = `C:\Users\mike\desktop\data.txt` (recommended option).
- **Files** = `data.txt` (not recommended; this excludes all data.txt files regardless of their path).
- **Files** = `C:\Users\mike\desktop\data.*` (wrong; you cannot exclude files using widcards when you specify the path).

Example: Exclude paths on Windows computers

To exclude folder `C:\Users\mike\desktop\`:

- **Folders** = `C:\Users\mike\desktop\` (recommended option).
- **Folders** = `C:\Users\%USERNAME%\desktop\` (excludes the desktop folder for all of the computer users).
- **Folders** = `C:\Users\*\desktop\` (wrong; you cannot exclude folders using widcards in paths).

Example: Exclude files or folders on Linux/macOS computers

To exclude file `/home/mike/data.txt`:

- **Files** = `/home/mike/data.txt` (recommended option).
- **Folders** = `/home/$USER/` (wrong; you cannot use environment variables).
- **Files** = `/home/mike/*.txt` (wrong; you cannot use wildcards).
- **Files** = `mik` (not recommended, this excludes all files whose name or path contains the `mik` substring).

Exclude the following email attachments

Specify email attachments with specific file extensions that you do not want to scan.

Advanced protection

Features by platform

The advanced protection features available vary for each platform.

Feature	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Behavior: Operating mode	X		
Behavior: Detect malicious activity	X	X	
Anti-exploit protection, including code injection and vulnerable driver detection	X (Not available on Windows ARM systems)		
Windows Anti-Malware Scan Interface (AMSI) technology (available in Antivirus)	X		
Advanced security policies and blocked programs	X		
Network attack protection	X		
Privacy	X	X	X
Network usage	X	X	X

Table 11.6: Advanced protection supported features by platform

Behavior

Advanced protection enables the monitoring of the processes run on Windows, macOS, and Linux computers and the sending of all generated telemetry to the Cytomic cloud. This information is incorporated into the investigation processes that classify files as goodware or malware, without ambiguity or classifying files as suspicious. Thanks to this technology, it is possible to detect unknown malware and advanced threats such as APTs on Windows and Linux computers.

Along with these advanced detection features, Cytomic provides a service called Zero-Trust Application Service for Windows computers, which classifies all files found on the customer IT network, leaving no unknown files.

Operating mode (Windows computers only)

Field	Description
Audit	Allows execution of unknown programs, and disinfects or deletes known malware depending on the settings of the antivirus module. See **Antivirus**.
Hardening	Allows execution of unknown programs already installed on user computers. Blocks unknown programs that originate from an untrusted source (such as the Internet, external storage drives, or other computers on the network) until a classification is returned. Disinfects or deletes programs classified as malware.
Lock	Prevents execution of all unknown programs pending classification. Deletes or disinfects programs already classified as malware.

Table 11.7: Advanced protection operating modes for Windows computers

- **Report blocking to computer users**: Shows a message in a pop-up alert on the user computer when:
    - Advanced protection blocks a file.
    - A blocked program is reclassified as goodware, and the user can use it.
- **Add the following custom message to alerts (optional)**: Specify a custom message to include in the alert.
- To enable users to decide whether to run blocked items, enable **Give computer users the option to run unknown blocked programs (recommended for advanced users and administrators only)**.

Detect malicious activity (Linux computers only)

Advanced EPDR sends the telemetry received from the monitored Linux workstations and servers to the Cytomic cloud. With this information, Advanced EPDR generates contextual rules to stop advanced threats.

Field	Description
Audit	Reports threats detected through contextual rules, but does not block them.
Block	Reports and blocks threats detected through contextual rules. Unless you are sure that the detected malicious activity is a legitimate action, it is recommended that you change the setting to Block mode.

Field	Description
Do not detect	Malware found through contextual rules is not detected or reported.

Table 11.8: Linux protection operating modes

Advanced security policies

Advanced security policies enable you to detect and block suspicious scripts and unknown programs that use advanced infection techniques on Windows computers. This type of malware is a growing threat to the security of systems.

To enable advanced security policies, click the **Enable advanced policies** toggle and configure each of the policies listed in **Table 11.9:** with one of these options:

- **Do not detect**: Does not detect the policy or generate any feedback for users or administrators.
- **Audit**: Detects the policy and generates feedback for the administrator in lists and dashboard widgets. See **Malware and network visibility** on page **661**.
- **Block**: Advanced EPDR prevents the program from running.

Advanced security policies include:

Fields	Description
PowerShell with obfuscated parameters	Detects the number of times the PowerShell interpreter received suspicious parameters that could result in the execution of dangerous operations on the protected computer. This option requires that you enable the anti-exploit protection.
PowerShell run by the user	Detects the number of attempts to run a monitored PowerShell script by an interactive account capable of executing dangerous operations on the protected computer. This option requires that you enable the anti-exploit protection.
Unknown scripts	Detects and/or blocks attempts to run a script that the Cytomic security intelligence team has not classified as safe. This policy helps: • Provide visibility into scripts run on the network. • Secure servers where program execution is restricted. • Prevent the spread of malware on the network if infection is suspected.

Fields	Description
	If you think the security software is generating false positives, consider the possibility of excluding the file from scans. See **Files and paths excluded from scans**.
Locally compiled programs	Detects the number of attempts to run a program that is unknown to the Cytomic security intelligence team because it was compiled on the user computer.
Documents with macros	Detects the number of attempts to open a Microsoft Office document with macros.
Registry modification to run when Windows starts	Detects the number of times a program tried to add a Windows registry key to gain persistence on the computer and to load with the operating system on every system start.

Table 11.9: Advanced security policies in Advanced EPDR

Block programs

To increase the security of Windows computers on the network, you can prevent the use of programs you consider dangerous or suspicious.

These programs include:

- Programs which, due to the way they run, use too much bandwidth or establish too many connections, negatively impacting company connectivity if run simultaneously by multiple users.
- Programs that enable users to access contents that might contain security threats.
- Programs that enable users to access contents not related to company activity and which might affect user performance.

To create a new settings profile or edit an existing profile, enter this information:

Fields	Description
Names of the programs to block	Names of the files that you want Advanced EPDR to prevent from running. You can paste a list of file names separated by line breaks.
MD5 or SHA-256 codes of the	MD5 or SHA-256 codes of the files that you want Advanced EPDR to prevent from running. You can paste a list of MD5 or SHA-256 codes

Fields	Description
programs to block	separated by line breaks.

Table 11.10: Configuring a Block Programs security policy

To **Notify computer users about blocked applications**, enable the toggle. A pop-up message shows on user computers when they try to run a blocked application. In the text box, enter a custom message to show users when Advanced EPDR blocks a program.

Anti-exploit

Anti-exploit technology is not available on Windows ARM systems.

Anti-exploit protection automatically blocks attempts to exploit vulnerabilities found in the active processes on user computers, in most cases without requiring user intervention.

How anti-exploit protection works

Network computers might run trusted processes that include bugs. Although legitimate, these processes are vulnerable because they sometimes do not correctly interpret data received from users or other processes.

If a vulnerable process receives malicious inputs from a hacker, a malfunction can occur that enables the attacker to inject malicious code into areas of memory that the vulnerable process manages. The injected code can cause the compromised process to execute actions it was not programmed for and compromise computer security.

The anti-exploit protection included in Advanced EPDR detects attempts to inject malicious code into vulnerable processes run by users, and neutralizes them based on the exploit detected:

Exploit blocking

The security software detects the injection attempt while it is still in progress. Because the injection process does not complete, the targeted process is not compromised and there is no risk to the computer. The exploit is neutralized without the need to end the affected process or restart the computer, and there are no data leaks from the affected process.

The user of the targeted computer receives a block notification, based on the settings configured by the administrator.

Exploit detection

The security software detects the injection after it takes place. Because the vulnerable process already contains malicious code, the security software must end the process before it performs actions that might put computer security at risk.

Regardless of the time between exploit detection and when the compromised process ends, Advanced EPDR reports that the computer was at risk. The level of risk depends on the time passed before the process stopped and on the type of malware. Advanced EPDR can either end a compromised process automatically to minimize the negative effects of an attack, or prompt the user to end the process and remove it from memory.

If you configure compromised processes to be automatically ended, users could lose information handled by the affected processes. However, by delegating the decision to the user, you enable them to save work or critical information before the compromised process stops.

If it is not possible to end a compromised process, the user is prompted to restart the computer.

Vulnerable driver blocking

Drivers supplied by legitimate vendors might contain vulnerabilities that malware could exploit to infect a computer or disable the security software.

These drivers are not malicious in themselves and can be installed on computers without posing a security threat. Therefore, initially they are not detected as malware.

The anti-exploit protection included in Advanced EPDR blocks the use of vulnerable drivers, except when the driver loads at operating system startup.

Anti-exploit technology compatibility

Cytomic follows all standards recommended by OS manufacturers to make sure its security products are compatible with other antivirus and EDR solutions. Anti-exploit technology is typically implemented with hooks. If more than one solution uses anti-exploit technology, they could be incompatible. We recommend that you only enable one anti-exploit technology.

In Advanced EPDR, the technologies that use hooks are:

- Anti-exploit
- Advanced code injection
- Advanced IOAs. See **Compatibility of advanced IOAs with third-party security solutions** on page **613**.

Anti-exploit protection settings

Code injection

- To enable anti-exploit protection, enable the toggle.
- **Code injection exclusions**: You can exclude processes that are incompatible with anti-exploit protection. To exclude a process, type its name in the **Excluded processes** text box and press **Enter**.

If authorized by a partner, you can add exclusions but you cannot delete or edit the list of exclusions defined by the partner. For more information, see ***Exclusions set by a partner****.*

- **Operating mode (Windows computers only)**

Field	Description
Audit	Reports exploit detections in the management console, but does not take action against them or display information to the user.
Block	Blocks exploit attacks. In some cases, it might be necessary to end the compromised process. • **Report blocking to the computer user**: The user receives a notification, and the compromised process is automatically ended if required. • **Ask the user for permission to end a compromised process**: Prompts users to end a compromised process should it be necessary. This enables users to, for example, save their work or critical information before the compromised process is stopped. Every time a compromised computer needs to restart, the user must provide confirmation, regardless of whether the **Ask the user for permission to end a compromised process** toggle is enabled.

Table 11.11: Advanced EPDR advanced anti-exploit protection operating modes

Many exploits continue to run malicious code until the relevant process ends. An exploit does not appear as resolved in the Exploit Activity panel on the Security dashboard in the web console until the compromised program terminates.

Vulnerable driver.

- To enable blocking of vulnerable drivers, enable the **Detect drivers with vulnerabilities** toggle.
- **Operating mode (Windows computers only)**

Field	Description
Audit	Reports detections in the Cytomic management console, but does not take action against them.

Field	Description
Block	Reports detections in the Cytomic management console, blocks drivers from loading, and shows an alert on the affected computer.

Table 11.12: Vulnerable driver blocking operating modes in Advanced EPDR

Network attack protection

Many security incidents begin with attacks that exploit vulnerabilities in Internet-exposed services. If malicious actors achieve their goal and infect computers in your organization, you must stop the attack.

Network attack protection scans network traffic in real time to detect and stop threats. It prevents network attacks that attempt to exploit vulnerabilities in services that are open to the Internet and in the internal network.

For more information about network attack protection detections, see **https://www.pandasecurity.com/en/support/card?id=700145**.

Field	Description
Block	Blocks traffic in a network attack. This is the default option.
Audit	Reports network attacks in the management console, but does not take action against them or display information to the user.

Table 11.13: Network attack protection operating modes in Advanced EPDR

Privacy

Advanced EPDR collects the name and full path of the files it sends to the Cytomic cloud for analysis, as well as the name of the logged-in user. This information is used in the reports and forensic analysis tools shown in the management console. If you do not want this information sent, clear the relevant checkbox in the **Privacy** section.

Network usage

Advanced EPDR compresses and sends every unknown executable file found on user computers to the Cytomic cloud for analysis. The maximum size of the compressed file that the agent sends for analysis is 50 MB.

This behavior is configured so that it has no impact on the customer's network bandwidth.

- The security software only sends a maximum 50 MB of files to the cloud each hour for each agent.
- The agent sends each unknown file once only for all customers who use Advanced EPDR.
- The security software implements bandwidth management mechanisms to prevent intensive usage of network resources

To configure the maximum number of MB that an agent can send each hour, type a value in the corresponding box. Click **OK**. To establish unlimited transfers, set the value to 0.

Antivirus

This section enables you to configure the general behavior of the signature-based antivirus engine.

Field	Description
File antivirus	Enable or disable the antivirus protection for the file system.
Mail protection	Enable or disable the antivirus protection for the mail client installed on user computers. Advanced EPDR detects threats received over the POP3 protocol and encrypted variants.
Web browsing antivirus	Enable or disable the antivirus protection for the web browser installed on user computers. Advanced EPDR detects threats received over the HTTP protocol and encrypted variants.

Table 11.14: Antivirus protection modules available in Advanced EPDR

When Advanced EPDR detects malware or the Cytomic anti-malware laboratory identifies a suspicious file, Advanced EPDR takes one of these actions:

- **Known malware files when disinfection is possible**: Replaces the infected file with a clean copy.
- **Known malware files when disinfection is not possible**: Makes a copy of the infected file and deletes the original file.

AMSI (AntiMalware Scan Interface) technology

The Windows AntiMalware Scan Interface (AMSI) is a versatile interface that allows your applications and services to integrate with any anti-malware product that is present on a computer. AMSI provides enhanced malware protection for your users and their data, applications, and workloads.

For more information, see ***https://learn.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal****.*

This feature is only available for computers with a Windows operating system installed.

To enable or disable AMSI technology, enable the **Enable advanced scanning with AMSI** toggle.

Exclusions

You can add exclusions for programs that might cause performance issues when you enable advanced scanning with AMSI. In the text box, type the names of the programs and press Enter. For more information about how the console behaves when you edit exclusions for a settings profile managed by a partner, see **Exclusions set by a partner**.

Threats to detect

Configure the types of threats that Advanced EPDR searches for and removes from the file system, mail client, and web client installed on user computers.

Field	Description
Detect viruses	Detects files that contain patterns classified as dangerous.
Detect hacking tools and PUPs	Detects unwanted programs (such as programs with intrusive ads and browser toolbars) and tools used by hackers to gain access to your system.
Block malicious actions	Enables anti-exploit and heuristic technologies that analyze process behavior locally and detect suspicious activity.
Detect phishing	Detects fraudulent emails and websites.
Do not detect threats at the following addresses and domains	Type IP addresses and domains you want to exclude from phishing scans, separated by commas. This text box is not case-sensitive. Access is allowed to all addresses that start with the specified IP addresses and domains, even if the full URL is longer.
Create Decoy Files to help detect	Creates decoy files as bait on computers. These files are permanently monitored by Advanced EPDR. When there is an attempt to modify a decoy file, the security software identifies the process as ransomware and

Field	Description
ransomware	ends the process.

Table 11.15: Malware types detected by the Advanced EPDR antivirus protection

File types

Specify the types of files to be scanned by Advanced EPDR:

Field	Description
Scan compressed files on disk	Decompresses compressed files and scans their contents for malware.
Scan compressed files in emails	Decompresses email attachments and scans their contents for malware.
Scan all files regardless of their extension when they are created or modified (Not recommended)	Many types of data files do not pose a threat to the security of computer networks. When you enable this option, the security software scans all files when they are created or modified. For best performance, we recommend that you do not enable this option.

Table 11.16: File types scanned by the Advanced EPDR antivirus protection

Firewall (Windows computers)

Advanced EPDR monitors the communications sent and received by each computer on the network, blocking all traffic that matches the rules defined by you. This module is compatible with both IPv6 and IPv4 and includes multiple tools for filtering network traffic:

- **System rules**: Describe communication characteristics (ports, IP addresses, protocols, etc.), allowing or denying the data flows that match the configured rules.
- **Program rules**: Allow or prevent the programs installed on users' computers from communicating with other computers.
- **Intrusion detection system**: Detects and rejects malformed traffic patterns that can affect the security or performance of protected computers.

Operating mode

This is defined through the option **Let computer users configure the firewall**:

- **Enabled (user- mode or self- managed firewall)**: Enables users to manage the firewall protection from the local console installed on their computers.
- **Disabled (administrator- mode firewall)**: You configure the firewall protection of all computers on the network through settings profiles.

Network types

Laptops and mobile devices can connect to networks with different security levels, from public Wi-Fi networks, such as those in Internet cafés, to managed and limited-access networks, such as those found in companies. You have two options to set the default behavior of the firewall protection: manually select the type of network that the computers in the configured profile usually connect to, or let Advanced EPDR select the most appropriate network type.

Network type	Description
Public network	Networks in public places such as airports, Internet cafés, and universities. Computers are not visible to other users on the network and some programs have limited access to the network. Limitations must be established on the way protected computers are used and accessed, especially with regard to file, resource, and directory sharing. Cytomic rules are enabled or disabled according to the administrator's criteria.
Trusted network	Home or office networks when you know and trust the other users and devices on the network. Computers are visible to other computers and devices on the network. Cytomic rules are not applied, so there are no restrictions on sharing files, resources, or directories.
Detect automatically	The network type (public or trusted) is selected automatically based on the rules you specify. Click the link **Configure rules to determine when a computer is connected to a trusted network**.

Table 11.17: Network types supported by the firewall

Advanced EPDR behaves differently and applies different predetermined rules automatically depending on the type of network selected. These predetermined rules are referred to as 'Cytomic rules' in the Program rules and Connection rules sections.

Each network interface on a computer has a specific type of network assigned to it. Computers with multiple network interfaces can have different network types assigned, and different firewall rules for each network interface.

Configuring rules for trusted access

Advanced EPDR enables you to add and configure rules to determine whether a computer is connected to a **trusted network**. If none of these conditions is met, then the network type selected for the network interface is **public network**.

To be considered on a trusted network, the computer must be able to resolve a domain previously defined on an internal DNS server. If the computer can connect to the DNS server and resolve the configured domain, then it is connected to the company network, and the firewall assumes the computer is connected to a trusted network.

Next is a configuration example:

- In this example, the organization's primary DNS zone is "`mycompany.com`".
- Add a Type A record with the "`firewallcriterion`" name to the primary zone of your organization's internal DNS server ("`mycompany.com`"). You do not need to specify an IP address because it is not used to validate the criterion.
- Based on these settings, "`firewallcriterion.mycompany.com`" is the domain that Advanced EPDR tries to resolve in order to check that it is connected to the company's network.
- Restart the DNS server if required and make sure "`firewallcriterion.mycompany.com`" is resolved successfully from all segments of the internal network with the tools `nslookup`, `dig`, or `host`.
- From the Advanced EPDR console, click the link **Configure rules to determine when a computer is connected to a trusted network**. A dialog box opens. Enter the following data:
  - **Criterion name**: Type a name for the rule you want to add.. For example "`myDNScriterion`".
  - **DNS server**: Type the IP address of the DNS server in your company network that can resolve DNS requests.
  - **Domain**: Type the domain to send to the DNS server for resolution. Enter "`firewallcriterion.mycompany.com`".
- Click **OK** and **Save**. Click **Save** again.
- After the criterion has been configured and applied, the computer tries to resolve the "`firewallcriterion.mycompany.com`" domain on the specified DNS server every time an event occurs on the network interface (connect, disconnect, IP address change, etc.). If DNS resolution succeeds, the settings assigned to the trusted network are assigned to the network interface used.

Program rules

In this section you can configure program rules to control which programs can communicate with the local network and Internet.

To build an effective protection strategy, follow these steps in the order listed:

1. **Set the default action**.

Action	Description
Allow	Implements a permissive strategy based on always accepting connections for all programs for which you have not configured a specific rule in step 3. This is the default, basic mode.
Deny	Implements a restrictive strategy based on always denying connections for all programs for which you have not configured a specific rule in step 3. This is an advanced mode, as it requires adding rules for every frequently used program. Otherwise, they will not be allowed to communicate, affecting their performance.

Table 11.18: Types of default actions supported by the firewall for the programs installed on computers

2. **Enable or disable Cytomic rules.**

This only applies if the computer is connected to a public network.

3. **Add rules to define the specific behavior of your applications**.

Figure 11.1: Edit controls for connection rules

You can change the order of the program rules, as well as adding, editing, or removing them by using the Up **(1)**, Down **(2)**, Add **(3)**, Edit **(4)**,and Delete **(5)** buttons on the right. Use the checkboxes **(6)** to select the rules you want to apply each action to.

Complete the following fields to create a rule:

- **Description**: Type a description of the new rule.
- **Program**: Select a program you want to configure connection options for.
- **Connections allowed for this program**: Select an option to specify whether to allow or deny connections for the program:

Field	Description
Allow inbound and outbound connections	The program can connect to the local network and Internet. Also, other programs or users can connect to it. There are certain types of programs that need these permissions to work correctly: file sharing programs, chat

Field	Description
	applications, Internet browsers, etc.
Allow outbound connections	The program can connect to the local network and Internet, but does not accept inbound connections from other users or applications.
Allow inbound connections	The program accepts connections from programs or users from the local network and Internet, but is not allowed to establish outbound connections.
Deny all connections	The program cannot connect to the local network or Internet.

Table 11.19: Communication modes for allowed programs

- **Advanced permissions**: Specify parameters of the traffic you want to allow or deny.

Field	Description
Action	Defines the action that Advanced EPDR takes when the examined traffic matches the rule. • **Allow**: Allows the traffic. • **Deny**: Blocks the traffic. It `drops` the connection.
Direction	Sets the traffic direction for connection protocols such as TCP. • **Outbound**: Traffic from the user's computer to another computer on the network. • **Inbound**: Traffic to the user's computer from another computer on the network.
Zone	Applies only if the zone matches the zone configured in **Network types**. Rules whose **Zone** is set to **All** are applied at all times irrespective of the network type configured in the Firewall settings.
Protocol	Establish the layer 3 protocol for the traffic generated by the program you want to control: • All • TCP

Field	Description
	• UDP
IP	• **All**: The rule does not take into account the connection source and target IP addresses. • **Custom**: Specify the source or target IP address of the traffic to control. You can enter multiple addresses, separated by commas (,). To specify a range, use a hyphen (-). From the drop-down menu, select if the IP addresses are IPv4 or IPv6. You cannot mix different types of IP addresses in the same rule. • **Ports**: Specify the communication port. Select **Custom** to enter multiple ports, separated by commas (,). To specify a range, use a hyphen (-).

Table 11.20: Advanced communication options for allowed programs

Connection rules

Connection rules define traditional TCP/IP traffic filtering. Advanced EPDR extracts the values of fields in the headers of each packet sent and received by protected computers and checks them against the predefined rules and any custom rules you create If the traffic matches any of the rules, the solution takes the specified action.

Connection rules affect the entire system (regardless of the process that manages them). They have priority over program rules that control the connection of programs to the Internet and local network.

To build an effective strategy to protect the network against dangerous and unwanted traffic, follow these steps in the order listed:

1. **Specify the firewall's default action in the Program rules section**.

Action	Description
Allow	Implements a permissive strategy based on always accepting all connections for which you have not configured a specific rule in step 3. This is the default, basic configuration mode: All connections for which there is not an existing rule are automatically accepted.

Action	Description
Deny	Implements a restrictive strategy based on always denying all connections for which you have not configured a specific rule in step 3. This is an advanced mode: All connections for which there is not an existing rule are automatically denied.

Table 11.21: Types of default actions supported by the firewall for the programs installed on users' computers

2. **Enable or disable Cytomic rules.**

This only applies if the computer is connected to a public network.

3. **Add rules that describe specific connections along with the associated action**.

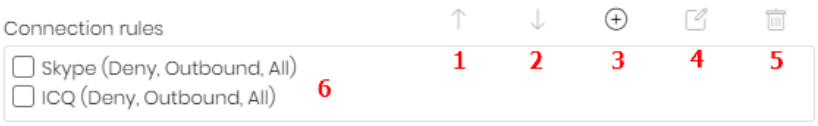


Figure 11.2: Edit controls for connection rules

You can change the order of the firewall connection rules, as well as adding, editing, or removing them by using the Up **(1)**, Down **(2)**, Add **(3)**, Edit **(4)**, and Delete **(5)** buttons to their right. Use the checkboxes **(6)** to select the rules you want to apply each action to.

The order of the rules in the list is not random. They are applied in descending order. If you change the position of a rule, you also change its priority.

The following is a description of the fields found in a connection rule:

Field	Description
Name	Type a name for the rule.
Description	Type a description of the traffic filtered by the rule.
Direction	Sets the traffic direction for connection protocols such as TCP. • **Outbound**: Outbound traffic. • **Inbound**: Inbound traffic.
Zone	The rule only applies if the value specified here matches the network type configured in **Network types**. If you select **All**, then the rule applies at all times, regardless of the network type configured.
Protocol	Select the traffic protocol. The options vary for the protocol you select:

Field	Description

	• **TCP, UPD, TCP/UDP**: Define TCP and/or UDP rules, including local and remote ports.
	  • **Local ports**: Select the connection port used on the user's computer. Select **Custom** to enter multiple ports separated by commas (,) or a range separated with a hyphen (-).
	  • **Remote ports**: Select the connection port used on the remote computer. Select **Custom** to enter multiple ports separated by commas (,) or a range separated with a hyphen (-).
	• **ICMP services**: Create rules that describe ICMP messages, indicating their type and subtype.
	• **ICMPv6 services**: Create rules that describe ICMP messages over IPv6, indicating their type and subtype.
	• **IP Types**: Select the higher-level protocols you want to apply the rule to.

IP addresses	Specify the source or target IP address of the traffic to control. You can enter multiple addresses, separated by commas. To specify a range, use a hyphen (-). From the drop-down menu, select if the IP addresses are IPv4 or IPv6. You cannot mix different types of IP addresses in the same rule.
MAC addresses	Specify the source or target MAC address of the traffic to control.

Table 11.22: Settings options for connection rules

The source and target MAC addresses included in packet headers are overwritten every time the traffic goes through a proxy, router, etc. The data packets reach their destination with the MAC address of the last device that handled the traffic.

Block intrusions

The intrusion detection system (IDS) enables you to detect and reject malformed traffic specially crafted to impact the security and performance of protected computers. This traffic can cause malfunction of user programs, lead to serious security issues, and allow remote execution of applications by hackers, data theft, etc.

The following is a description of the types of malformed traffic supported and the protection provided:

Field	Description
IP Explicit Path	Rejects IP packets that contain an explicit source route field. These packets are not routed based on their target IP address. Routing information is defined beforehand.
Land Attack	Stops denial-of-service attacks that use TCP/IP stack loops. Detects packets with identical source and target addresses.
SYN Flood	This attack type launches TCP connection attempts to force the targeted computer to commit resources for each connection. The protection establishes a maximum number of open TCP connections per second to prevent saturation of the computer under attack.
TCP Port Scan	Detects if a host tries to connect to multiple ports on the protected computer in a specific time period. The protection filters both the requests to open ports and the replies to the malicious computer. The attacking computer is unable to obtain information about the status of the ports.
TCP Flags Check	Detects TCP packets with invalid flag combinations. It acts as a complement to the protection against port scanning. It blocks attacks such as "SYN&FIN" and "NULL FLAGS". It also complements the protection against OS fingerprinting attacks as many of those attacks are based on replies to invalid TCP packets.
Header Lengths	• **IP**: Rejects inbound packets with a IP header length that exceeds a specific limit. • **TCP**: Rejects inbound packets with a TCP header length that exceeds a specific limit. • **Fragmentation Overlap**: Checks the status of the packet fragments to be reassembled at the destination, which protects the system against memory overflow attacks due to missing fragments, ICMP redirects masked as UDP, and computer scanning.
UDP Flood	Rejects UDP streams to a specific port if the number of UDP packets exceeds a preconfigured threshold in a particular period.
UDP Port	Protects the system against UDP port scanning attacks.

Field	Description
Scan	
Smart WINS	Rejects WINS replies that do not correspond to requests sent by the computer.
Smart DNS	Rejects DNS replies that do not correspond to requests sent by the computer.
Smart DHCP	Rejects DHCP replies that do not correspond to requests sent by the computer.
ICMP Attack	• **Small PMTU**: Detects invalid MTU values used to generate a denial-of-service attack or slow down outbound traffic. • **SMURF**: Attacks involve sending large amounts of ICMP (echo request) traffic to the network broadcast address with a source address spoofed to the victim's address. Most computers on the network will reply to the victim, which multiplies traffic flows. The solution rejects unsolicited ICMP replies if they exceed a certain threshold in a specific time period. • **Drop Unsolicited ICMP Replies**: Rejects all unsolicited and expired ICMP replies.
ICMP Filter Echo Request	Rejects ICMP echo request packets.
Smart ARP	Rejects ARP replies that do not correspond to requests sent by the protected computer to avoid ARP cache poisoning scenarios.
OS Detection	Falsifies data in replies to the sender to trick operating system detectors. It prevents attacks on vulnerabilities associated with the operating system. . This protection complements the TCP Flag Checker.

Table 11.23: Supported types of malformed traffic

Do not block intrusions from the following IP addresses:

Enables you to exclude certain IP addresses and/or IP address ranges from the detections made by the firewall.

Device control (Windows computers)

This feature enables you to control the behavior of protected Windows computers when they connect to a removable or mass storage device:

- From the top menu, select **Settings**.
- From the side menu, select **Workstations and servers**. A page opens that shows all settings profiles created so far.
- Select an existing security settings profile to edit, or in the upper-right corner of the page, click **Add** to create a new profile.
- Select **Device control**.
- Enable the **Enable device control** toggle.
- For each type of device, specify the authorized use:
    - **Removable storage drives and CD/DVD drives**: Choose among **Block**, **Allow read access**, or **Allow read & write access**.
    - **Bluetooth devices, mobile devices, imaging devices, and modems**: Choose among **Allow** and **Block**.
- To **Disable AutoPlay on removable storage devices**, enable the toggle. The Windows operating system blocks the `autorun.inf` file on storage devices and does not automatically run the predefined application or action. Neither does it show the menu with the available actions for the device.

Allowed devices

This section enables you to configure an allowlist of specific devices you want to allow despite belonging to a blocked device category.

- Click the ⊕ icon in the **Allowed devices** section to show a list of all devices connected to the computers on your network.
- Select the devices you want to exclude from the configured general blocking rules.
- Use the 🗑 button to delete existing exclusions.

Exporting and importing a list of allowed devices

Use the **Export** and **Import** options available from the context menu ⋮.

Determining a device unique ID

To manage a specific device without having to wait for a user to connect it to their computer, or to exclude it manually, you need to determine the device ID:

- Open Windows Device Manager. Select the device you want to obtain the ID for. Right-click the device name and select **Properties**.
- Select the **Details** tab.
- From the **Property** drop-down list, select **Device Instance Path**. The **Value** box shows the device unique ID.

If no value appears in Device Instance Path, you are not able to obtain the device ID. You can instead use the Device Hardware ID to identify it:

- To show the Device Hardware ID, from the **Property** drop-down list, select **Hardware IDs**.

> *A device Hardware ID does not identify it uniquely. It identifies all devices of the same hardware type.*

In a text file, add the IDs of the devices you want to allow, as indicated in **Exporting and importing a list of allowed devices**

Renaming devices

The name assigned to a computer devices by Advanced EPDR can sometimes lead to confusion or prevent you from correctly identifying them. To resolve this, you can assign a custom name for a device:

- In the **Allowed devices** list, select the computer or device.
- Click the icon. A dialog box opens for you to enter a new name for the device.
- Click **OK**. The **Allowed devices** list updates with the new name.

Web access control

With this protection, you can limit access to specific web content categories and individual URLs to optimize network bandwidth and increase business productivity.

To enable or disable it, click the **Enable Web access control** toggle.

Limitations with HTTP/3 (QUIC) protocol

Because the security software does not inspect the HTTP/3 (QUIC) protocol, the web access control feature does not support browsers with that protocol.

To resolve this issue, use one of these options:

Add a filter rule from the Advanced EPDR console to block traffic on port 80, port 8080, and port 443

> *This procedure is effective on Windows devices only.*

- From the top menu, select **Settings**. From the side menu, select **Workstations and servers**. A page opens that shows all settings profiles created so far.
- Select an existing security settings profile to edit, or in the upper-right corner of the page, click **Add** to create a new profile. The **Add settings** or **Edit settings** page opens.
- Select the **Firewall (Windows computers)** section. The settings associated with the firewall appear.
- Click **Enable the firewall** (if it is disabled).
- In **Connection rules**, click the ⊕ icon to create a new filter rule.
- In the **Name** and **Description** fields, enter a name for the filter rule and a description (optional).
- In the **Action** field, select **Deny**.
- In the **Direction** field, select **Outbound**.
- In the **Zone** field, select the type of network for which you want to apply the block rule on the user computer. See **Network types**.
- In the **Protocol** field, select **UDP**.
- In the **Remote ports** field, select **Custom**. A new field appears.
- In the **Custom** field, add port 80, port 8080, and port 443 separated by a comma.
- Click **OK**. Click **Save**. The settings profile is saved and automatically sent to all computers that have it assigned.

After the firewall rule is applied to the computers on the network, the user browser cannot send requests that use the UDP protocol on port 80, 8080, or 443. This forces the browser to send its requests with the TCP protocol on port 80, which corresponds to HTTP/2.

*For more information about how to create firewall rules in Advanced EPDR, see **Connection rules**.*

Disable HTTP/3 (QUIC) protocol in browsers on user devices

Browser settings can vary for different versions.

- Google Chrome
  - In the browser address bar, type **chrome://flags**.
  - Disable the **Experimental QUIC protocol** option.

- Microsoft Edge
    - In the browser address bar, type **edge://flags/**.
    - Disable the **Experimental QUIC protocol** option.
- Mozilla Firefox
    - In the browser address bar, type **about:config**.
    - Disable the **network.http.http3.enabled** option.
- Opera
    - In the browser address bar, type **opera://flags/#enable-quic**.
    - From the **Experimental QUIC protocol** drop-down menu, select **Disabled**.

Configuring time periods for the web access control feature

This option enables you to limit access to certain website categories and denied sites during business hours and authorize it during non-business hours and weekends.

To configure Internet access time limits, select the **Enable only during the following times** option.

Specify when you want to enable web access control. On the calendar, select the days and hours when you want to enable it.

- Click the day to select the whole day.
- Click and drag the squares to select multiple days and times.
- To select every day of the month, click the **Select all** button.
- Click **Clear** to disable web access control for all of the times selected.

Denying access to specific web pages

Advanced EPDR groups the web pages it classifies into 160 content categories. To deny access to a certain type of web content category, select it from the list.

If a user visits a web page that belongs to one of the forbidden categories, a warning page appears that indicates that access is denied and the reason.

Denying access to pages categorized as unknown

To deny access to pages characterized as unknown, enable the **Deny access to pages categorized as unknown** toggle.

Internal and intranet sites accessible on ports 80 and 8080 could be categorized as unknown. To avoid this, add exclusions for internal pages you want to allow.

List of allowed/denied addresses and domains

You can set a list of pages that are always allowed (allowlist) or blocked (blocklist), regardless of the category that they belong to:

- In the text box, enter the URL of the relevant IP address or domain.
- Click **Add**.
- Use the **Delete** and **Clear** buttons to edit the list according to your needs.
- Click **OK** to save the settings.

To add multiple similar domains to a list without having to specify each domain separately, you can add the part of the domain names that is common to all of them. The wildcard character (*) is not supported.

For example, **https://www.mydomain.com/test** represents these domains (among others):

- https://www.mydomain.com/test/test2.htm
- https://www.mydomain.com/testing.htm
- https://www.mydomain.com/test/test2/

Database of URLs accessed from computers

Each computer on the network keeps a database of the URLs accessed from it. This database is located in:

```
%programdata%\Panda Security\Security Protection\urlcounters.dg
```

This database is in SQLite3 format and can only be accessed from the computer for a period of 30 days.

The data stored is this:

- User ID.
- Protocol (HTTP or HTTPS).
- Domain.
- URL
- Returned category.
- Action (Allow/Deny).
- Date accessed.
- Access count (by category and domain).

Audit mode

Audit mode monitors the processes run on Windows, macOS, and Linux computers, and detects and notifies threats.

Enabling Audit mode for a settings profile does not change the overall status of the protections applied to the computers that receive the settings. Nor does it change the configuration of the protections in the web console. Threats continue to be detected and reported, but they are not blocked or deleted.

We recommend that you limit the use of Audit mode as much as possible to minimize the time your computers are exposed to the threats detected.

To enable Audit mode:

- Select **Settings** from the top menu. Select **Workstations and servers** from the side menu.
- Select the settings profile for which you want to enable Audit mode. To create a settings profile, see **Creating and managing settings profiles** on page **294**.
- Select **Audit mode**. Enable the toggle.
- Click **Save**. A message appears at the top of the **Edit settings** page, indicating that you have enabled Audit mode for the settings profile and the risk it entails.

Viewing computers in Audit mode

The **Protection status** widget shows the number of computers that have Audit mode enabled. Click the text on the widget to go to the **Risks by computer** list filtered by the **Audit mode enabled** risk.

For more information, see **Security module panels/widgets** on page **661** and **Risk assessment module lists** on page **731**.

Verbose mode

Verbose mode enables a small number of computers on the network to generate extended telemetry for a limited period of time. You can then analyze this information to evaluate which security software components are in use when an IOA is generated.

Verbose mode is essentially used to evaluate the capabilities of security software in a test environment, where attacks on the IT infrastructure are simulated.

To see both normal and extended telemetry, see the **Investigation section (5)** on page **275**.

Verbose mode requirements and limitations

Verbose mode collects a large quantity of telemetry from all computers configured in this mode and sends it to the cloud. To avoid impacting performance, Advanced EPDR implements these restrictions:

- Maximum number of computers simultaneously configured in Verbose mode: 20 computers.
- Maximum duration of Verbose mode: 7 days.
- Verbose mode can only be enabled on computers in Audit mode.
- Verbose mode is only available on Windows computers.

The requirements for assigning Verbose mode to a computer are:

- **Configure security for workstations and servers** permission. See **Managing roles and permissions** on page **69**
- Audit mode assigned. See **Audit mode**.

Enabling and disabling Verbose mode

> *Make sure the computer has a **Workstations and servers** settings profile assigned and Audit mode enabled. If the computer does not meet this requirement, Verbose mode is not available. See **Audit mode**.*

To enable Audit mode:

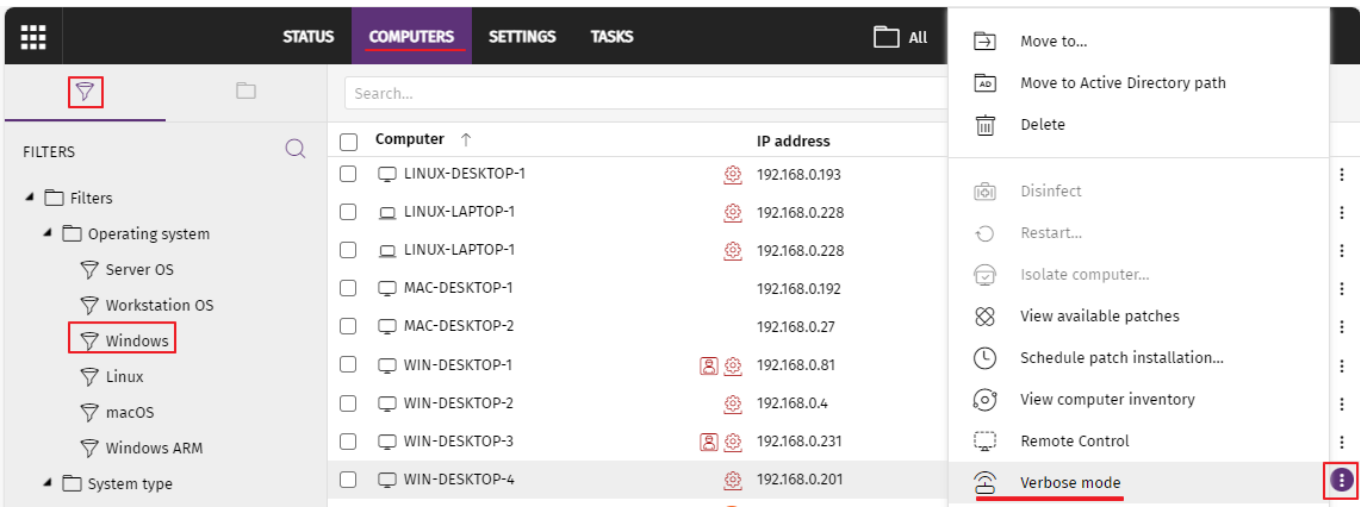


Figure 11.3: List of computers filtered by Windows platform

- From the top menu, select **Computers**. The **Computers** page opens.
- From the side panel, select the **Filters** tab . A list opens that shows all configured filters.
- Select a filter that shows Windows computers (for example **Windows**). The list updates to show all managed computers.
- To open the context menu for the computer where you want to configure Verbose mode, click the icon.
- Select **Verbose mode** . The **Enable Verbose mode** dialog box opens.
- From the drop-down menu, select the duration of Verbose mode.
- Click **Enable Verbose mode**. The icon appears next to the computer in the list.

To disable Verbose mode:

- From the top menu, select **Computers**. The **Computers** page opens.
- Select a filter that shows Windows computers (for example **Windows**). The list updates to show all managed computers.
- Click the icon for the computer on which you want to disable Verbose mode. The icon appears next to the computer.
- Select **Disable Verbose mode** . The icon disappears.

Viewing computers in Verbose mode

Computers in Verbose mode appear in the list with the icon.

To list only computers in Verbose mode, create a filter:

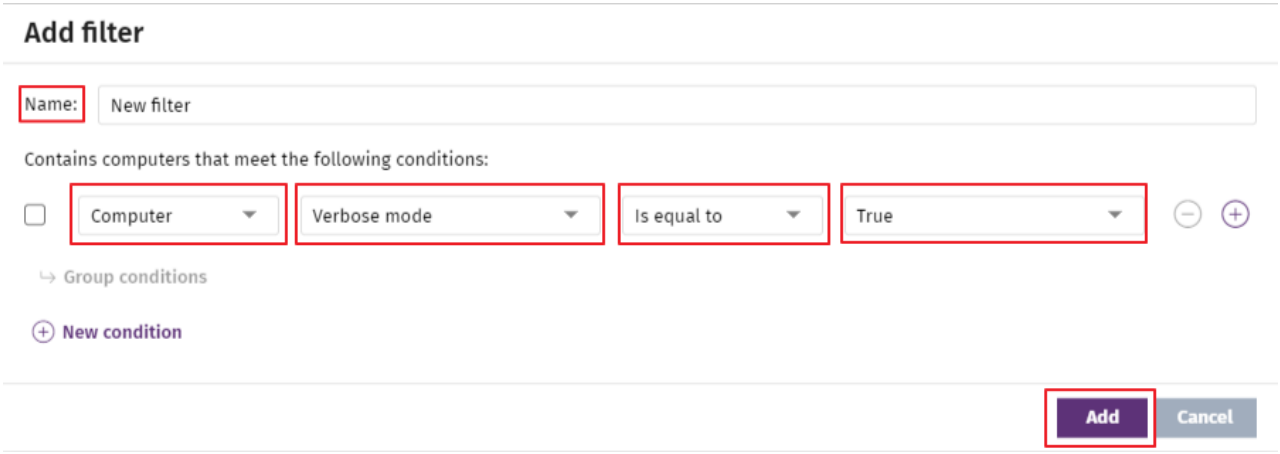


Figure 11.4: Computers filtered by Verbose mode

- From the top menu, select **Computers**. The **Computers** page opens.
- From the side panel, select the **Filters** tab  . A list opens that shows all configured filters.
- In the **Operating system** folder, click the ⋮ icon. A context menu opens.
- Select **Add filter**, The **Add filter** dialog box opens.
- In the **Name** text box, type a name for the filter.
- From the **Select a category** drop-down menu, select **Computer**.
- From the **Select a property** drop-down menu, select **Verbose mode**.
- From the **Select an operator** drop-down menu, select **is equal to**.
- From the **Select a value** drop-down menu, select **True**.
- Click **Add**. The filter is created and applied to the list of computers, showing only those with Verbose mode enabled.

Chapter 12

Security settings for mobile devices

The **Settings** menu at the top of the Advanced EPDR console provides the parameters required to configure the security of the smartphones and tablets in the organization. Select the **Mobile devices** option in the menu on the left to view a list of the security profiles already created, or to create a new one.

The following is a description of the available security and anti-theft configuration options for mobile devices, and recommendations to protect smartphones and tablets without interfering with user activity.

*For more information about the **Mobile devices** module, see:*

***Creating and managing settings profiles** on page **294**: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*

***Accessing, controlling, and monitoring the management console** on page **61**: Managing user accounts and assigning permissions.*

Chapter contents

Security settings for Android devices

Accessing the settings

- From the top menu, select **Settings**.
- From the side menu, select **Mobile devices**.
- Select the **Android devices** tab. Click **Add**. The **Add settings** page opens.

Required permissions

Permission	Access type
Configure security for mobile devices	Create, edit, delete, copy, or assign settings profiles for mobile devices.
View security settings for mobile devices	View the security settings profiles for mobile devices defined.
Use the anti-theft protection for mobile devices (locate, wipe, lock, etc.)	Send actions to target mobile devices to prevent data loss, locate them in the event of loss or theft, and lock them.

Table 12.1: Permissions required to access the Android device security settings

Updates

Define the type of connection to be used by the device to download updates from the Cytomic cloud.

For more information about how to configure updates, see ***Product updates and upgrades*** *on page* ***203****.*

Antivirus

The antivirus protection for Android mobile devices scans both devices and their SD cards permanently and on demand. It also protects against the installation of apps from unknown sources that could be infected with malware and PUPs.

To enable the antivirus protection and scan apps from unknown sources, enable the toggles.

Exclusions

This option enables you to select installed apps that you do not want to be scanned. Enter the names of the packages you want to exclude from the scans, separated by commas (“,”).

To look up an app package name, find the app in the Google Play store using a web browser. The package name appears at the end of the URL after the '`?id=`'.

Anti-theft

The anti-theft feature enables you to send actions to target Android devices to prevent data loss or locate them in the event of loss or theft.

Accessing the anti-theft feature

- From the top menu, select **Settings**. From the side menu, select **Mobile devices**.
- Select the **Android devices** tab. A list opens and shows all created settings profiles.
- To create a new setting profile, click the **Add** button. The **Add settings** page opens.
- To edit an existing setting profile, click it. The **Edit settings** page opens.
- Select the **Anti-Theft** section. Use the toggle to enable or disable the anti-theft feature.
- Click **Save**.

For more information about the anti-theft actions available in Advanced EPDR, see ***General section for mobile devices*** *on page* ***254****.*

Anti-theft protection settings

Field	Description
Report the device's location	Advanced EPDR uses the device GPS to get its GPS coordinates and send them to the Advanced EPDR server. If this feature is unavailable, it tries to get them through Wi-Fi or the carrier communication infrastructure. To enable or disable this option, use the toggle.
Take a picture after three failed unlock attempts and email it	If the user of the device has three consecutive failed attempts to unlock it, a photo is taken and sent by email to the email addresses entered in the text box. You can enter multiple addresses separated by a comma. To enable or disable this option, use the toggle.

Field	Description
Privacy	Enables users to enable private mode. Private mode disables geolocation tracking. To enable or disable this option, use the toggle.

Table 12.2: Anti-theft features for Android devices

Security settings for iOS devices

Accessing the settings

- From the top menu, select **Settings**.
- From the side menu, select **Mobile devices**.
- Select the **iOS devices** tab. Click **Add**. The **Add settings** page opens.

Required permissions

Permission	Access type
Configure security for mobile devices	Create, edit, delete, copy, or assign settings profiles for iOS devices.
View security settings for mobile devices	View the settings profiles for iOS devices defined.
Use the anti-theft protection for mobile devices	Send actions to target mobile devices to prevent data loss, locate them in the event of loss or theft, and lock them.

Table 12.3: Permissions required to access the iOS device security settings

Antivirus for web browsers

The antivirus protection for iOS devices scans the URLs that the device connects to to prevent the installation of malware apps and phishing attacks.

To enable detection of malware and phishing URLs, enable the toggles.

This feature is not available for iOS devices not enrolled into an MDM solution. See ***Installation on iOS systems*** *on page* ***154****.*

Exclusions

You can exclude certain URLs and domains from scans. In the text box, type the URLs and domains that you want to exclude.

Anti-theft

The anti-theft feature enables you to send actions to target iOS devices to prevent data loss or locate them in the event of loss or theft.

Accessing the anti-theft protection

- From the top menu, select **Settings**. From the side menu, select **Mobile devices**.
- Select the **iOS devices** tab. A list opens and shows all created settings profiles.
- To create a new setting profile, click the **Add** button. The **Add settings** page opens.
- To edit an existing setting profile, click it. The **Edit settings** page opens.
- Select the **Anti-Theft** section. To enable or disable the anti-theft feature, use the toggle.
- Click **Save**.

For more information about the anti-theft actions available in Advanced EPDR, see ***General section for mobile devices*** *on page* ***254****.*

Anti-theft protection settings

Field	Description
Behavior	Advanced EPDR uses the device GPS to get its GPS coordinates and send them to the Advanced EPDR server. If this feature is unavailable, it tries to get them through Wi-Fi or the carrier communication infrastructure. To enable or disable this option, use the toggle.
Privacy	Enables users to enable private mode. Private mode disables geolocation tracking. To enable or disable this option, use the toggle.

Table 12.4: Anti-theft features for iOS devices

Web access control

This protection enables you to limit access to specific web content categories and configure a list of URLs to allow and deny access to.

This feature is not available for iOS devices not enrolled into an MDM solution. See ***Installation on iOS systems*** *on page* ***154****.*

Namely, web access control enables you to:

- Select the days and hours when you want to enable web access control.
- Deny access to specific web pages.
- Configure lists of allowed/denied addresses and domains.
- Keep a database of the URLs accessed from each computer.

Enabling web access control

- From the top menu, select **Settings**.
- From the side menu, select **Mobile devices**.
- Select the **iOS devices** tab.
- Click **Add**.
- Select the **Web access control** section.

To enable or disable the feature, click the **Enable web access control** toggle.

Configuring time periods for web access control

This option enables you to limit access to certain website categories and denied sites during business hours and authorize it during non-business hours and weekends.

To specify when you want to enable web access control, select the **Enable only during the following times** option.

On the calendar, select the days and hours when you want to enable web access control.

- Click the day to select the whole day.
- Click and drag the squares to select multiple days and times.
- To select all times every day of the month, click the **Select all** button.
- Click **Clear** to disable web access control for all of the times selected.

Click the **Save** button.

Denying access to specific web pages

Advanced EPDR groups the web pages it classifies into 160 content categories. To prevent users from accessing a specific set of web pages:

- Select the web page categories.
- In the upper-right corner of the page, click **Save**.

To select all categories, click **Select all**. To clear all selections, click **Clear**.

If a user visits a web page that belongs to a forbidden category, a warning page appears that indicates that access is denied and the reason.

Denying access to pages categorized as unknown

To **Deny access to pages categorized as unknown**, select the toggle.

Internal and intranet sites accessible on ports 80 and 8080 could be categorized as unknown. To avoid this, add exclusions for internal pages you want to allow.

List of allowed/denied addresses and domains

You can set a list of pages that are always allowed (allowlist) or blocked (blocklist), regardless of the category that they belong to:

- In the text box, enter the URL of the relevant IP address or domain. Press **Enter**. The URL appears inside a tag.
- To add another domain or address, click **Add URL**.
- To edit the list, use the **Copy** and **Clear** buttons. These buttons appear when you point the mouse to the text box.
- To save the settings profile, click **Save** in the upper-right corner of the page.

URL matches can be full or partial. With long URLs, it is enough to enter the beginning of the URL in the text box to allow/block all URLs that start with the entered characters.

Chapter 13

Cytomic Data Watch (Personal data monitoring)

Files with Personally Identifiable Information (PII) are files that contain information that can be used to identify individuals related to the organization (for example, customers, employees, and suppliers) This information can include different types of data, such as social security numbers, phone numbers, and email addresses.

Cytomic Data Watch is the Advanced EPDR security module that enables companies to comply with data protection regulations, such as the GDPR. It also monitors and improves the visibility of personal data (PII) stored in an organization IT infrastructure.

To achieve this, Cytomic Data Watch provides three key features:

- It generates a complete, daily inventory of the PII files found on the network, along with basic information such as their name, extension, and the name of the computer where the file was detected.
- It discovers, audits, and monitors the entire life cycle of PII files in real time: from data at rest, to data in use (the operations taken on personal data), and data in motion (data exfiltration).
- It provides tools to perform flexible, content-based searches and delete duplicate personal data files to limit their presence across the network.

For more information about the Cytomic Data Watch module, see:

***Creating and managing settings profiles** on page **294**: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*

***Accessing, controlling, and monitoring the management console** on page **61**: Managing user accounts and assigning permissions.*

***Managing lists** on page **48**: Information about how to manage lists.*

*For more information about the specific management console for this service, see the **Cytomic Data Watch Administration Guide**.*

Chapter contents

Introduction to Cytomic Data Watch operation

To fully understand the processes involved in the discovery and monitoring of the personal data stored across an organization, you must be familiar with some concepts associated with the technologies used by Cytomic Data Watch.

Entity

Each word or group of words with their own meaning referring to a certain type of personal information is called 'entity'. These entities include personal ID numbers, first and last names, phone numbers, and other.

Given the highly ambiguous and variable nature of natural language, each entity can have different formats depending on the language, and so it is necessary to apply flexible, adaptable algorithms for the detection of personally identifiable information. Generally, analyzing entities consists of applying a set of predefined formats or expressions to data and uses the local context surrounding the detection, as well as the presence or absence of certain keywords, to avoid false positives. For more information, see **Supported entities and countries**.

PII file

After an entity is identified, the context in which it appears is evaluated to determine if the information it provides is enough to identify a specific person. If it is, the file can be protected with specific processing and access protocols that enable the organization to comply with the applicable legislation (GDPR, PCI, etc.). This evaluation process leverages a monitored machine learning model and a mature model based on the analysis of entities and the global context of documents to finally classify a file with detected entities as a PII file to protect.

Unstructured files and IFilter components

Cytomic Data Watch scans unstructured files (text files with different formats, spreadsheets, PowerPoint presentation files, etc.) searching for entities and classifying files as PII files or non-PII files. However, to correctly interpret the content of unstructured files, certain third-party components must be installed on user computers. These components are called IFilters and are not part of the Advanced EPDR installation package. Microsoft Search, Microsoft Exchange Server, and Microsoft SharePoint Server, along with other operating system and third-party product services, use IFilters to index user files and enable content-based searches.

Each file format supported by Cytomic Data Watch has its own associated IFilter component, and many of them come preinstalled with the Windows operating system. However, other components must be manually installed or updated.

The Microsoft Filter Pack is a free single point-of-distribution for Office IFilters. After it is installed, it enables Cytomic Data Watch to parse the content of all file formats supported by the Microsoft Office productivity suite. For more information, see **Microsoft Filter Pack Component**.

Index process

This consists of inspecting and storing the contents of all files supported by Cytomic Data Watch to generate an inventory of PII files and search the content of these files. The indexing process has little impact on computer performance, but does require a significant amount of time. You can schedule the start of the indexing task or limit its scope to expedite the process and improve the results returned by searches. For more information, see **The indexing process**.

Normalization process

When performing an indexing process, Cytomic Data Watch applies a number of rules to homogenize indexed data. The aim of this process is to store each word individually and increase its chances of being found, as well as reducing search times. The rules to apply during the

normalization process vary depending on whether the content to store is an entity or plain text. For more information, see **Search requirements and properties**.

PII file inventory

After a computer is indexed and all entities and PII files are identified, Cytomic Data Watch generates an inventory, accessible to you , with the names of the files and their characteristics. This inventory is sent to the Advanced EPDR server once a day. For more information, see **PII file inventory**.

> *Cytomic Data Watch does not send the contents of files with PII to the Advanced EPDR server. It only sends their attributes (name, extension, etc.) and the number and type of found entities.*

File searches

Cytomic Data Watch finds files by name, extension, or content on the indexed storage drives of computers on the network.

Searches run in real time. As soon as you run a search task, you start to see results from the target computers. For more information, see **File searches**.

Monitoring of the actions taken on PII files

Cytomic Data Watch monitors the events that affect PII files and sends them to the Cytomic Insights console. This tool shows the trend of PII files on the network, enabling you to view whether they have been copied, moved, emailed, etc. For more information about Cytomic Insights, see the Cytomic Data Watch Administration Guide at **https://info.cytomicmodel.com/resources/guides/DataWatch/en/DATAWATCH-guide-EN.pdf**.

Cytomic Data Watch requirements

Supported operating systems

> *From 30 September 2024, you will not be able to add devices to the management console or install the protection software on new computers that run these operating system versions: Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008 (Windows 2008 R2 will continue to be supported). Existing computers in the management console will continue to be protected. See* ***https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.***

Cytomic Data Watch supports devices that run Microsoft Windows XP SP3 and higher and Windows Server 2003 SP1 and higher. It does not support Linux and macOS.

Microsoft Filter Pack Component

Microsoft Filter Pack and Microsoft Office

Microsoft Office includes the Microsoft Filter Pack. The IFilter components that correspond to Office products installed on the user computer are installed automatically. To make sure that all IFilter components are available on the computer, see **Installing the Microsoft Filter Pack manually**.

Installing the Microsoft Filter Pack manually

To install the Microsoft Filter Pack, go to:

https://www.microsoft.com/en-us/download/details.aspx?id=17062

The Microsoft Filter Pack is compatible with Windows XP SP2, Windows Server 2003 SP2, and higher. In some cases, you must install the Microsoft Core XML Services 6.0 library or Microsoft Search Service.

The indexing process

This consists of inspecting and storing the contents of all files supported by Cytomic Data Watch. This process is indispensable to generate the PII file inventory and to search for files on computers by their contents. The indexing process is configured transparently when enabling any of the aforementioned two features. The indexed information is stored locally in the following path on each user's computer: `%ProgramData%\Panda Security\Panda Security Protection\indexstore`.

Despite indexing processes have a low impact on computer performance, they may take considerable time. For that reason, Cytomic Data Watch is configured to launch the process only once on each computer on the network at the time the module is enabled and every time the entity detection technology is updated for improvement purposes.

After the indexing process is complete, Cytomic Data Watch starts monitoring the creation of new files as well as the deletion and modification of existing ones, updating the index and sending newly detected entities to the Advanced EPDR server every 24 hours.

Configuring the scope, schedule, and type of indexing processes

You can exclude certain files and folders from indexing processes and even change the accuracy of the searches conducted by Cytomic Data Watch.

- To exclude certain files or folders from indexing processes, see **Exclusions**.
- To adjust the accuracy of searches, see **Index the following content**.
- To schedule indexing processes, see **Schedule indexing**.

PII file inventory

> *Cytomic Data Watch does not send the contents of the PII files found on the network to the Advanced EPDR server. Only their attributes (name, extension, etc.) and the number and type of found entities are sent.*

The PII file inventory shows the PII files that Cytomic Data Watch has found on the customer's network.

To enable the inventory, see **Personal data (inventory, searches, and monitoring)** for more information.

Viewing inventories

Cytomic Data Watch incorporates multiple tools to monitor the PII files found on the network and view the entities they contain.

- To view statistics of the number of PII files found on the network, see **Files with personal data** for more information.
- To view statistics of the number of computers with PII files found on the network, see **Computers with personal data**for more information.
- To view a list with details of PII files found on the network, see **Files with personal data**for more information.
- To view a list with details of computers with PII files found on the network, see **Computers with personal data** for more information.

Continuous monitoring of files

PII file monitoring

Cytomic Data Watch collects all events related to the creation, modification, and deletion of PII files, providing visibility into all actions taken and enabling detection of dangerous situations such as data theft, unauthorized access to information, etc.

To view the actions taken on PII files, go to the **Cytomic Insights** in the lower-left corner of the side panel accessible from the **Status** top menu. For more information, see the Cytomic Data Watch User Guide at **https://info.cytomicmodel.com/resources/guides/DataWatch/en/DATAWATCH- guide-EN.pdf**.

To enable monitoring of the actions taken on PII files, see **Personal data (inventory, searches, and monitoring)**.

Monitoring of files specified by the administrator

In addition to automatically monitoring the files classified as PII by Cytomic Data Watch, you can add new files to monitor by using rules. See **Rule-based monitoring of files** for more information.

File searches

Requirements for conducting searches

To search for files with specific contents on the computers on the network, the following requirements must be met:

- The user account used to launch the search from the web console must have a role with the permission **Search for data on computers**. See **Accessing, controlling, and monitoring the management console** on page 61 for more information about roles.
- The computers targeted by the search must have a Cytomic Data Watch license assigned.
- The computers targeted by the search must have a Cytomic Data Watch settings profile assigned with the option **Allow data searches on computers** enabled. See **Cytomic Data Watch settings**

Searches widget

This is the entry point for the file search feature. It enables searches to be viewed and managed.

To access the **Searches** widget, go to the **Status** top menu. From the side panel, select **Cytomic Data Watch**

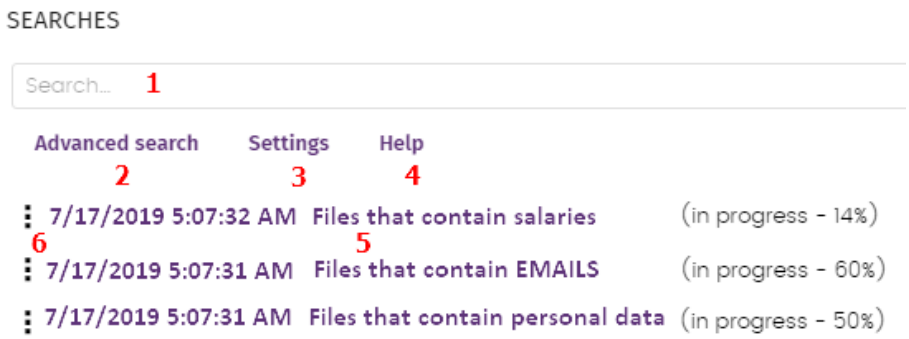


Figure 13.1: Searches widget

The widget has the following features:

- **(1)** Text box to enter search criteria. See **Search syntax** for a description of the search terms permitted by Cytomic Data Watch.
- **(2) Advanced search**: Defines the scope of the search.
- **(3) Settings**: Access to the Cytomic Data Watch settings profiles. For more information, see **Cytomic Data Watch settings**.

- **(4) Help**: Link to a Cytomic support article, showing updated information about the Cytomic Data Watch search syntax.
- **(5) Previous searches**: Searches that have been used before and that can be relaunched if required.
- **(6) Search context menu**: Enables you to edit the name of the search and its parameters, as well as relaunching and deleting it.

Search requirements and properties

To run searches successfully, the following requirements must be met:

- The user account used to launch the search from the web console must have a role with the permission **Search for data on computers**. See **Accessing, controlling, and monitoring the management console** on page **61** for more information about roles.
- The computers targeted by the search must have a Cytomic Data Watch license assigned.
- The computers targeted by the search must have a Cytomic Data Watch settings profile assigned with the option **Allow data searches on computers** enabled.

Search properties

- The maximum number of simultaneous searches in the management console per user account is 10. After this number, an error message appears.
- The maximum number of searches saved per user account is 30. After this number, an error message appears.
- The maximum number of results in total for each search is 10,000 records. Results in excess of this number are not displayed.
- The maximum number of results per computer is 10,000 / number of computers on which the search is run. So, if you search on a network of 100 computers, the maximum number of results displayed is 10,000 / 100 = 100 results per computer.
- The minimum number of results displayed per computer, regardless of the number of computers on the network, is 10.
- The maximum number of computers on which searches can be run simultaneously is 50. If the total number of computers in the search is greater, they are queued until the searches in progress are completed.

Normalization process

The normalization process does not affect the entity detection process.

Cytomic Data Watch applies a number of rules to the data obtained from the indexing process in order to homogenize it. Because the searches run by administrators are performed on the normalized data, it is necessary to know these rules as they may affect the results shown in the console.

String conversion to lowercase letters

Before a string is stored in the database, it is converted to lowercase letters.

Separating characters

Cytomic Data Watch detects the following special characters as separators between words. These characters are removed from indexes unless they are part of an entity.

- **Carriage return**: `\r`
- **Line break**: `\n`
- **Tab key**: `\t`
- **Characters**: `" : ; ! ? - + _ * = ( ) [ ] { } , . | % \ / ’`

For example, "`Cytomic.Data(Watch`" is stored as three separate words without the punctuation characters: "`cytomic`", "`data`", and "`watch`".

Entity normalization

The entity normalization process follows independent rules:

Entity	Separating characters	Indexing settings
• **Bank account numbers** • **Credit card numbers** • **Personal ID numbers** • **Phone numbers** • **Driver's license numbers** • **Passport numbers** • **Social security numbers**	They are removed. The entity is stored in the index as a single item.	They are ignored

Entity	Separating characters	Indexing settings
• **IP addresses** • **Email addresses**	They are respected. The entity is stored in the index as a single item.	They are ignored
• **First and last names** • **Postal addresses**	They are used as separators. The entity is stored in the index as multiple items.	They are observed

Table 13.1: Entity normalization rules

Entity normalization examples

- "1.42.67.116-C" is stored as IDCARD entity "14267116C".
- "192.168.1.1" is stored as IP entity "192.168.1.1".
- "Sesame Street 5 1st Floor" is stored as "sesame", "street", "floor" if the indexing method is **Text only** or as "sesame", "street", "5", "1", "floor" if the indexing method is **All**.

Creating searches

Creating a free search

- Click the **Status** menu at the top of the console. Select **Cytomic Data Watch** from the side panel.
- In the **Searches** widget text box, enter the search terms, in accordance with the search syntax described in section **Search syntax**.
- Click the icon or press Enter.

After you have entered the search, the **Search results** page opens. See **Previous searches** for more information about how to edit previous searches.

Creating a guided search

- Click the **Status** menu at the top of the console. Select **Cytomic Data Watch** from the side panel.
- Click the **Advanced search** link.

- Select **Guided search**.
- Configure the search parameters.

Advanced search parameters:

Parameter	Description
Search name	Type a name for the search.
Search for files with	Enter the content to search for. There are three text boxes: • **All of these exact words or phrases**: The search looks for files that contain all of the specified words or entries. • **Any of these exact words or phrases**: The search looks for files that contain any or all of the specified words or entries. • **None of these exact words or phrases**: The search looks for files that do not contain any of the specified words.
Personal data	Select the relevant checkboxes to specify the entities that the PII files you want to find must include. • **All**: All selected entities must appear in the PII file for it to be included in the search results (AND logic). • **Any**: All or at least one of the selected entities must appear in the PII file for it to be included in the search results (OR logic).
Narrow search to	**Computers**: • **All**: Search for the content in all computers with a Cytomic Data Watch license assigned and with the search option enabled in their settings profile. • **The following computers**: Displays a list of the computers with a Cytomic Data Watch license assigned. Use the checkboxes to select the computers to search for the specified content. • **The following computer groups**: Displays the folder structure with the computer hierarchy configured in Advanced EPDR. Use the checkboxes to select the groups to search for the specified content.
Cancel the search automatically	Select the search timeout period for computers that are turned off or offline.

Table 13.2: Advanced search parameters

Previous searches

Both free searches and guided searches are saved so they can be launched quickly in the future.

After a new search has been created, it appears in the **Searches** widget along with the date and time it was created, as well as the name and a key indicating the status (**In progress**, **Canceled**) or no status (**Finished**).

Changing the name of a previous search

Click the context menu of the search (**6** in **Figure 13.1:**) and select **Change name**.

Creating a copy of a previous search

To duplicate a previous search, click the context menu of the search (**6** in **Figure 13.1:**) and select **Make a copy**. A page is displayed with the search settings and the search name changed to 'Copy of'.

Launching a previous search

Click the context menu of the search (**6** in **Figure 13.1:**) and click **Relaunch search**. The status of the search changes, specifying the percentage of the task completed.

Canceling and deleting previous searches

Click the context menu of the search (**6** in **Figure 13.1:**). Click **Cancel** to stop the search and **Delete** to cancel the search and remove it from the **Searches** widget.

Editing a previous search

Click the context menu of the search (**6** in **Figure 13.1:**) and select **Edit search**. The **Advanced search** page opens, where you can edit the search parameters.

Viewing search results

To see the results of a search, go to the **Search results** list, either by:

- Clicking on a previous search.
- Creating a new search.

The list shows the computers that contain the search term entered, along with the name of the file detected and other information.

List header

Quick search parameters:

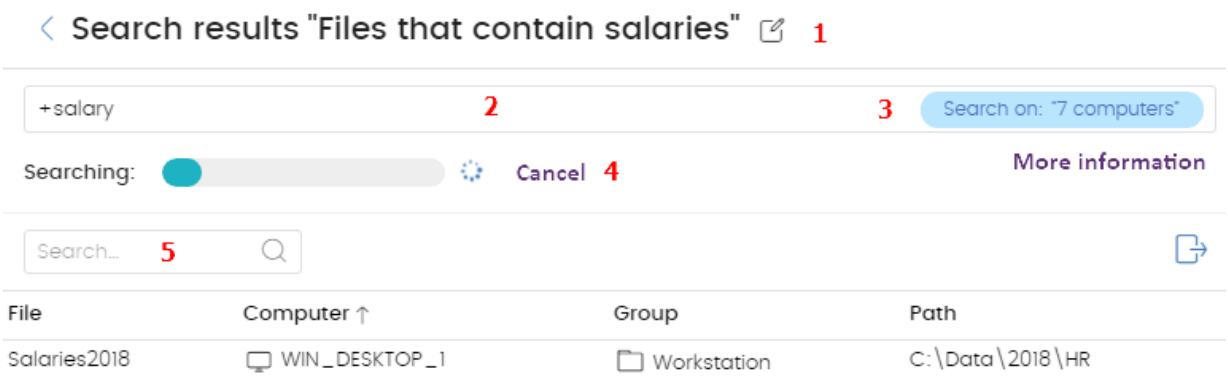


Figure 13.2: Search results page

- **(1)** icon: Change the search name.
- **(2) Text box**: Search content.
- **(3) Search on: 'x computers'**: Opens the **Advanced search** page to narrow the search.
- **(4) Searching**: Search status (**In progress**, **Canceled**).If the search has not begun or is complete, no status is indicated.
- **(5) Search text box**: Filters the results by computer name.

List fields

Field	Comment	Values
File	Name of the file found.	Character string
Computer	Name of the computer where the file was found.	Character string
Group	Advanced EPDR group to which the computer belongs.	Character string
Path	Path to the file on the storage device.	Character string

Table 13.3: Fields in the Search results list

Fields displayed in the exported file

Field	Comment	Values
File	Name of the file found.	Character string
Computer	Name of the computer where the file was found.	Character string

Field	Comment	Values
Group	Advanced EPDR group to which the computer belongs.	Character string
Path	Path to the file on the storage device.	Character string
Personal ID numbers	Indicates whether any personal ID numbers (national ID card numbers or similar) were found in the file.	Boolean
Passport numbers	Indicates whether any passport numbers were found in the file.	Boolean
Credit card numbers	Indicates whether any credit card numbers were found in the file.	Boolean
Bank account numbers	Indicates whether any bank account numbers were found in the file.	Boolean
Driver's license numbers	Indicates whether any driver's license numbers were found in the file.	Boolean
Social security numbers	Indicates whether any social security numbers were found in the file.	Boolean
Email addresses	Indicates whether any email addresses were found in the file.	Boolean
IPs	Indicates whether any IP addresses were found in the file.	Boolean
First and last names	Indicates whether any first and last names were found in the file.	Boolean
Addresses	Indicates whether any postal addresses were found in the file.	Boolean

Field	Comment	Values
Phone numbers	Indicates whether any phone numbers were found in the file.	Boolean

Table 13.4: Fields in the Search results exported file

Search syntax

Cytomic Data Watch enables you to perform flexible searches for files by content using plain text and parameters to narrow the scope of the results.

Syntax allowed in quick searches

- **Word**: Searches for 'word' in the document content and metadata.
- **WordA WordB**: Searches for '`worda`' or '`wordd`' (logical operator OR) in the document content.
- "**WordA WordB**": Searches for '`worda`' and '`wordb`' consecutively in the document content.
- **+WordA +WordB**: Searches for '`worda`' and '`wordb`' in the document content.
- +**WordA** -WordB: Searches for '`worda`' but not '`wordb`' in the document content.
- **Word***: Searches for all words that start with "`word`".. The wildcard '*' is only allowed at the end of the search term.
- **Wo?rd**: Searches for words that begin with '`wo`' and end in '`rd`' and have a single alphabet character in between. The character '`?`' can be located at any point in the search string.
- **Word~**: Searches for all words that contain the string '`word`'.

Syntax allowed in guided searches

Guided searches do not allow the '+' or '−' characters. Instead, search words are entered in different text boxes. If the characters '+' or '−' are used, they are considered part of the search term.

Available entities

To narrow the scope of results, Cytomic Data Watch supports the use of qualifiers to indicate entities or file characteristics in quick and advanced searches. Qualifiers are:

Qualifier	Description
PiiType	Specifies the type of PII data detected in the file.

Qualifier	Description
HasPii	Indicates that the file has PII data.
Filename	Indicates the name of the file.
FileExtension	Indicates the file extension.

Table 13.5: Available qualifiers

The values allowed in these qualifiers are:

Qualifier	Description
PiiType:BANKACCOUNT	Files that contain any bank account numbers.
PiiType:CREDITCARD	Files that contain any credit card numbers.
PiiType:IDCARD	Files that contain any personal ID numbers (national ID card numbers or similar).
PiiType:SSN	Files that contain any social security numbers.
PiiType:IP	Files that contain any IP addresses.
PiiType:EMAIL	Files that contain any email addresses.
PiiType:PHONE	Files that contain any phone numbers.
PiiType:ADDRESS	Files that contain any postal addresses.
PiiType:FULLNAME	Files that contain any first names and last names.
PiiType:PASSPORT	Files that contain any passport numbers.
PiiType:DRIVERLIC	Files that contain any driver's license numbers.
HasPii:True	Files that contain any PII data.
Filename:'file name'	Files with the specified file name.
Fileextension:'file	Files with the specified file extension.

Qualifier	Description
extension'	

Table 13.6: Values allowed in qualifiers

Syntax for searches with entities

Entities can be used in all search types (quick or guided) alone or combined with other character strings.

- **PiiType:IDCARD**: Searches for files with Personal ID numbers detected.
- **+PiiType:IDCARD +'Company'**: Searches for files containing a list of personal ID numbers in the company (with the character string 'Company').
- **+Filename:scan* +fileextension:docx -PiiType:fullname**: Searches for scan files (files whose name starts with 'scan') in Word (.docx extension) and that are not officially signed (no Fullname -first names and last names - were detected).

Tips for building searches that are compatible with the normalization process

- It is preferable to use lowercase letters.
- Bear in mind the settings you have previously configured regarding the type of content to index and excluded files, as those settings determine the number of results returned in searches.
- To search for **bank account numbers, credit card numbers, personal ID numbers, social security numbers, passport numbers, or driver's license numbers** do not use separating characters.
- To search for **IP addresses** and **email addresses**, enter them as they are.
- To search for **phone numbers**, remove any separating characters and enter the country code if necessary without the '+' sign.
- To search for **postal addresses**, do not use the numeric characters.

Searching for duplicate files

To help centralize sensitive information in one place and minimize the exposure of this type of data, Cytomic Data Watch provides a feature to look for and delete duplicate files.

About duplicate files

Two files are duplicated when their content is identical, regardless of the normalization process described in section **Normalization process** or the settings defined by the administrator in section **Index the following content**. This comparison does not take into account the names and extensions of the files.

Searching for duplicate files

Follow these steps to search for duplicate files:

- From the **My lists** side panel:
    - Go to the **Status** menu at the top of the console. Click **Add** from the **My lists** side panel. A window appears with all available lists.
    - Click the **Files with personal data** list. A list opens with all PII files found across the network.
- From the **Files with personal data** widget:
    - Go to top menu **Status**. Select **Cytomic Data Watch** from the side menu. Click one of the items in the **Files with personal data** widget. The **Files with personal data** list opens, filtered by the selected criteria.
- From the **Files by personal data type** widget:
    - Go to top menu **Status**. Select **Cytomic Data Watch** from the side menu. Click one of the items in the **Files by personal data type** widget. The **Files with personal data** list opens, filtered by the selected criteria.
    - From the context menu of the relevant file, click the **Search for copies of the file** option. A list opens with all files with the same content found across the network.

Deleting and restoring files

Deleting files from computers on the network

Cytomic Data Watch enables you to delete indexed files shown in computer inventories. File deletion is an asynchronous operation launched by the network administrator from their console and which takes place when the agent receives a request from the Advanced EPDR server and the following conditions are met:

- The file is not in use.
- The content of the file has not changed with respect to the file stored in the inventory.
- The file has not been deleted by the computer user in the time between when the inventory was generated and when the administrator launched the deletion action.

- The computer is online. If this condition is not met, Cytomic Data Watch marks the file as **Pending deletion** until the computer connects to the Advanced EPDR server.

Deletion action statuses

Because file deletion is an asynchronous operation, it can have the following statuses:

- **Deleted**: The file has been moved to the Advanced EPDR backup area.
- **Pending deletion**: Cytomic Data Watch is waiting for the computer to connect to the Advanced EPDR server in order to delete it.
- **Error**: It was not possible to delete the file due to an error.

Backing up the files deleted by Cytomic Data Watch

Files deleted by Cytomic Data Watch are not permanently erased from the computers' hard disks. Instead, they are moved to a backup area where they are kept for 30 days, after which they are permanently deleted.

This area is automatically excluded from inventories, searches, and the file monitoring feature, and cannot be accessed by the software installed on users' computers.

Deleting files

Follow these steps to delete one or more files:

- From the **My lists** side panel:
    - Go to the **Status** menu at the top of the console. Click **Add** from the **My lists** side panel. A window appears with all available lists.
    - Click the **Files with personal data** list. A list opens with all PII files found across the network.
- From the **Files with personal data** widget:
    - Go to top menu **Status**. Select **Cytomic Data Watch** from the side menu. Click one of the items in the **Files with personal data** widget.The **Files with personal data** list opens, filtered by the selected criteria.
- From the **Files by personal data type** widget:
    - Go to top menu **Status**. Select **Cytomic Data Watch** from the side menu. Click one of the items in the **Files by personal data type** widget.The **Files with personal data** list opens, filtered by the selected criteria.
- Follow these steps to delete multiple files:
    - Select the checkboxes next to the files you want to delete.
    - Click the icon at the top of the page. A confirmation dialog box opens.
- Follow these steps to delete a single file:

- From the context menu of the file you want to delete, click **Delete**. A confirmation dialog box opens.

- If you confirm the action, the file appears in red and with the  icon indicating that the file is pending deletion.

Viewing deleted files

Follow these steps to view the files deleted by the administrator:

- Go to the **Status** menu at the top of the console. Click **Add** from the **My lists** side panel. A window appears with all available lists.
- Click the **Files deleted by the administrator** list. A list opens with all PII files found on the network that were previously deleted or restored by the administrator.

Restoring files previously deleted by the administrator

Cytomic Data Watch enables you to restore, to their original location, all files previously deleted by the administrator through the console, provided they still remain in the backup area (up to 30 days after they were deleted). File restore is an asynchronous operation launched by the network administrator from their console and which takes place when the agent receives a request from the Advanced EPDR server and the following conditions are met:

- **The file remains in the backup area**: Deleted files are kept in the backup area for up to 30 days after being deleted. After that period, they are deleted permanently with no option for recovery.
- **There is no other file with the same name in the restore path**: If there is another file with the same name in the restore path, Cytomic Data Watch restores the file to the `Lost&Found` folder.
- **There is no other file with the same name in the restore path**: If there is another file with the same name in the restore path, Cytomic Data Watch restores the file to the Lost & Found folder.
- **The restore path exists**: If the restore path does not exist, Cytomic Data Watch restores the file to the Lost & Found folder.

Restore action statuses

Because file restore is an asynchronous operation, it can have the following statuses:

- Restored
- Pending restore
- Error

Restoring deleted files

Follow these steps to restore the files deleted by the administrator:

Accessing the restore feature:

- Go to the **Status** menu at the top of the console. Click **Add** from the **My lists** side panel. A window appears with all available lists.
- Click the **Files deleted by the administrator** list. A list opens with all PII files found on the network that were previously deleted or restored by the administrator.

Or

- Go to top menu **Status**. Select **Cytomic Data Watch** from the side menu. Click the **Files deleted by the administrator** widget. The **Files deleted by the administrator** list opens with no preconfigured filters.

Follow these steps to restore multiple files:

- Select the checkboxes next to the files you want to recover.
- Click the  icon at the top of the page. A confirmation dialog box opens.
- If you confirm the restore action, the file status changes to **Restoring**.

Follow these steps to restore a single file:

- Click the context menu of the file you want to recover.
- Click the **Restore** option. A confirmation dialog box opens.
- If you confirm the restore action, the file status changes to **Restoring**.

Cytomic Data Watch settings

Accessing the settings

- Click the **Settings** menu at the top of the console. Select **Cytomic Data Watch** from the side menu.
- Click the **Add** button. The **Add settings** page opens.

Required permissions

Permission	Access type
Configure Cytomic Data Watch	Create, edit, delete, copy, or assign Cytomic Data Watch settings profiles.

Permission	Access type
View Cytomic Data Watch settings	View Cytomic Data Watch settings profiles.

Table 13.7: Permissions required to access the Cytomic Data Watch settings

Requirements for finding and monitoring Microsoft Office documents

To find computers on the network lacking some or all of the required IFilter components, click the **Check now** link from the settings page. The **Computers** area opens with a list filtered by the following criteria: **Computers without Microsoft Filter Pack**.

Personal data (inventory, searches, and monitoring)

- **Generate and keep an up-to-date inventory of personal data**: Shows the PII files detected on the network in the dashboard widgets and in lists. See **Cytomic Data Watch panels/widgets** and **Cytomic Data Watch lists** for more information. For the PII files stored on a specific computer to appear in the console, the inventory process must have completed on that computer.
- **Monitor personal data on disk**: Monitors the actions executed on the PII files stored on computers.
- **Monitor personal data in email**: Monitors the actions executed on the personal data stored in email messages.
- **Allow data searches on computers**: Searches for files by their name or content, provided they have been previously indexed. When you select this option, Cytomic Data Watch starts indexing the files stored on users' computers. See **File searches** for more information.

Exclusions

You can exclude from searches those files stored on the computers on the network whose content you do not consider appropriate to take into account.

- **Extensions**: Type the extensions of the files you want to exclude.
- **Files**: Type the names of the files you want to exclude. You can use wildcard characters ? and *.
- **Folders**: Type the names of the folders whose files you want to exclude. You can use system variables and wildcard characters ? and *.

Rule-based monitoring of files

You can define rules for Cytomic Data Watch to monitor files not classified as PII. The system can store up to ten rules, each of which must have a unique name.

Monitor files on disk

Monitor the actions taken on the files selected in section **Monitoring rules**.

Monitor files in email

Monitor the actions taken on the email attachments that meet the rules defined in section **Monitoring rules**.

Monitoring rules

Shows the list of default file extensions to which monitoring is applied. You can add or remove extensions from the list. This list is common to all created rules.

If you assign a "file extension" property to a rule, the rule monitors only those files whose extension matches the extension you specify. It does not monitor all files whose extension matches those in the default list.

To add a monitoring rule, click the **+** icon. This opens the **Add monitoring rules** window where you can configure the rule settings.

- Fill in the name and description fields.
- Enter the condition criteria.

Property	Operator	Value
File name	Is equal to / Is not equal to	• Text field. You can use wildcard characters * and ?. • The character string cannot start with a wildcard character.
File path	Is equal to / Is not equal to	• Text field. You can use wildcard characters * and ?. • If a file system path is entered, the default separator character is \. • You must use the wildcard character * when defining a rule with the File path field. • The character string cannot start with a wildcard character.

Property	Operator	Value
File content	Is equal to / Is not equal to	• Text field. You can use wildcard characters * and ?. • The character string cannot start with a wildcard character.
File extension	Is equal to / Is not equal to	• Text field. You cannot use wildcard characters. • File extensions must be entered without the dot character.

Table 13.8: Fields for configuring conditions

New condition

Add more conditions to the rule. Logical operators AND/OR are applied.

Logical operators

To combine two or more conditions in the same rule, use the logical operators AND and OR. When you add a second or more conditions to a rule, a drop-down menu with the available logical operators is automatically displayed. These operators apply to the adjacent conditions.

Rule condition groupings

In a logical expression, parentheses are used to change the order in which the operators that relate rule conditions are evaluated.

As such, to group two or more conditions in a parenthesis, you must create a grouping by selecting the consecutive rules that will be part of the group and clicking **Group conditions**. A thin line appears connecting the monitoring rules that are part of the grouping.

The use of parentheses enables you to group operands at different levels in a logical expression.

Examples of monitoring rules

Property	Content	Search
File path	c:\path*	• Searches all files and folders located in C:\path\
File path	c:\path\ c:\path	• Wrong format. No results are returned.
File extension	txt	• Searches TXT files.
File extension	.txt	• Wrong format. No results are returned.

Property	Content	Search
File name	FileName	• Returns all files whose name is "FileName".
File name	FileName*	• Returns all files whose name starts with "FileName".
File name	?FileName *FileName	• Wrong format. No results are returned.

Table 13.9: Examples of monitoring rules

Advanced indexing options

To view the indexing status of your network, click the **View your computers' indexing status** link. The **Cytomic Data Watch status** list opens.

Index the following content

This section enables you to define the type of content to be considered when generating inventories and performing searches.

Computers whose contents have already been indexed and receive a change of settings delete the index and restart the indexing process from the beginning.

You can choose between two different types of indexing operations depending on whether you just want to generate an inventory of PII files across the network or search files by content:

- **Index text only**: Only text is indexed unless it is part of an entity recognized by Cytomic Data Watch. With this indexing option selected, searches by content are more limited. Therefore, this option is recommended if you just want to generate an inventory of PII files across the network.
- **Index all content**: This option indexes both texts and alphanumeric characters. This is the recommended option if, in addition to generating an inventory of PII files across the network, you also want to perform accurate content searches.

*Cytomic Data Watch searches for contents in files based on the option selected in the **Index the following content** section. If your computers have different indexing settings profiles assigned, search results might not be homogeneous.*

Schedule indexing

This section enables you to set the days and times when you want the indexing process to start if required:

- **Always enabled**: There is not a set schedule. The indexing process start when required.
- **Enable only during the following times**: Select, in the calendar, the days and times when you want the indexing process to start.
- Use the **Clear** and **Select all** buttons to clear or select all cells in the calendar (the latter is equivalent to selecting the **Always enabled** option).

Write to removable storage drives

This section enables you to restrict write to USB external storage media.

- **Allow write to removable drives only when the drive is encrypted**: If this option is selected, the user can write only to USB external storage media previously encrypted with Cytomic Encryption or BitLocker.

*The **Device control** settings defined in **Workstations and servers** take precedence over the settings defined in the **Cytomic Data Watch** section. So, if the **Device control** feature is enabled and does not allow USB drives to be read or written to, it is not possible to write to them, regardless of whether the drive is encrypted or not. See* ***Device control (Windows computers)** on page **353** for more information.*

Cytomic Data Watch panels/widgets

Accessing the dashboard

To access the dashboard, click the **Status** menu at the top of the console. Select **Cytomic Data Watch** from the side menu.

Required permissions

Permission	Access to widgets
No permissions	• Deployment status • Offline computers • Update status • Indexing status • Features enabled on computers

Permission	Access to widgets
	• Files deleted by the administrator
View personal data inventory	• Files with personal data • Files by personal data type • Computers with personal data
Search for data on computers	• Searches

Table 13.10: Permissions required to access the Cytomic Data Watch widgets

Deployment status

Shows computers where Cytomic Data Watch is working correctly and computers where an error has occurred. The status of computers is depicted by a circle with various colors and associated counters. The panel provides a graphical representation and percentage of computers with the same status.

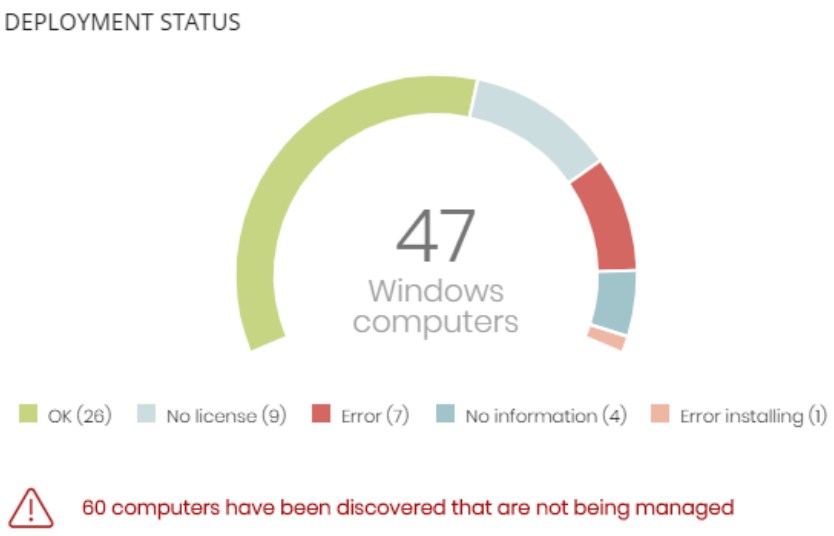


Figure 13.3: Deployment status panel

Meaning of the data displayed

Data	Description
OK	Computers where Cytomic Data Watch is installed, licensed, and is working correctly.
Error	Computers with Cytomic Data Watch installed, but for one reason or another the module does not respond to the requests sent from the Cytomic

Data	Description
	servers.
No license	Computers that are compatible with Cytomic Data Watch, but do not have a Advanced EPDR license assigned.
Error installing	Computers on which the installation process could not be completed.
No information	Computers that have just received a license and have not reported their status to the server yet and computers with an outdated agent.
Central area	Sum of all computers compatible with Cytomic Data Watch.

Table 13.11: Description of the data displayed in the Deployment status panel

Lists accessible from the panel

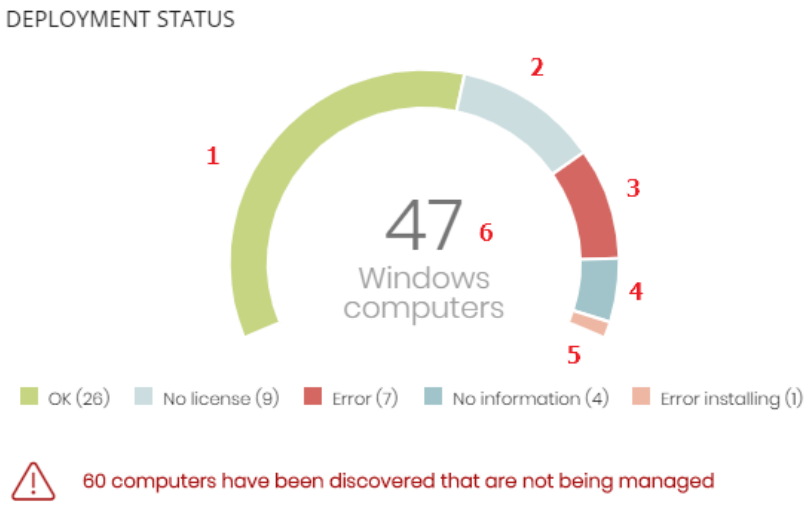


Figure 13.4: Hotspots in the Deployment status panel

Click the hotspots shown in **Figure 13.4:** to open the **Cytomic Data Watch status** list with the following predefined filters:

Hotspot	Filter
(1)	Cytomic Data Watch status = OK.
(2)	Cytomic Data Watch status = No license. The computer does not have a Advanced EPDR license assigned.
(3)	Cytomic Data Watch status = Error.

Hotspot	Filter
(4)	Cytomic Data Watch status = No information.
(5)	Cytomic Data Watch status = Error installing.
(6)	No filter.

Table 13.12: Filters available in the Cytomic Data Watch status list

Offline computers

Shows computers that have not connected to the Cytomic cloud for a certain amount of time. These computers are susceptible to security problems and require special attention from the administrator.

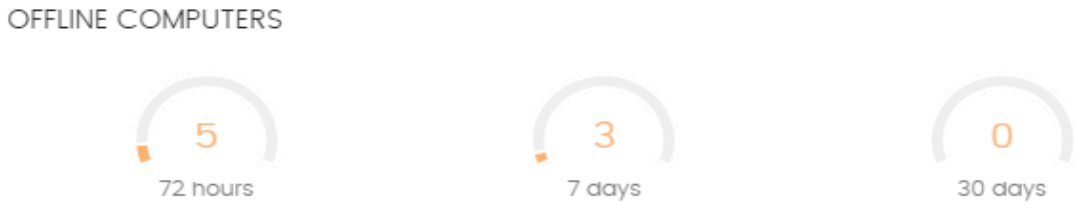


Figure 13.5: Offline computers panel

Meaning of the data displayed

Data	Description
72 hours	Number of computers that have not reported their status in the last 72 hours.
7 days	Number of computers that have not reported their status in the last 7 days.
30 days	Number of computers that have not reported their status in the last 30 days.

Table 13.13: Description of the data displayed in the Offline computers panel

Lists accessible from the panel

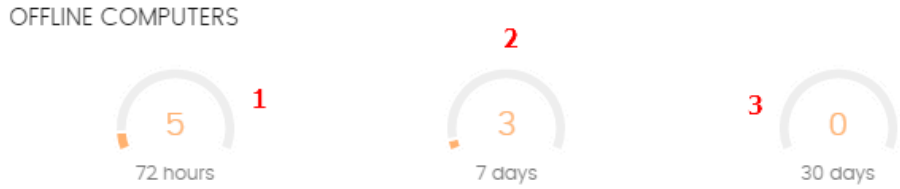


Figure 13.6: Hotspots in the Offline computers panel

Click the hotspots shown in **Figure 13.6:** to open the **Cytomic Data Watch status** list with the following predefined filters:

Hotspot	Filter
(1)	Last connection = More than 72 hours ago.
(2)	Last connection = More than 7 days ago.
(3)	Last connection = More than 30 days ago.

Table 13.14: Filters available in the Cytomic Data Watch status list

Update status

Shows the status of computers with respect to updates of the Cytomic Data Watchengine.

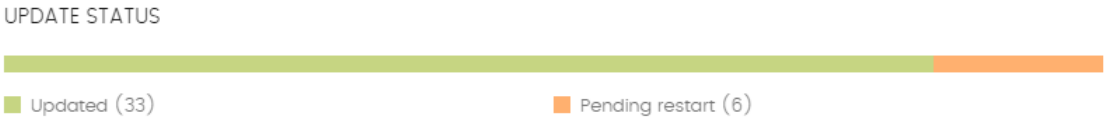


Figure 13.7: Update status panel

Meaning of the data displayed

Data	Description
Updated	Number of computers with the Cytomic Data Watch engine updated.
Outdated	Number of computers with the Cytomic Data Watch engine not updated.
Pending restart	Number of computers with Cytomic Data Watch installed but that have not yet restarted and so it is not updated.

Table 13.15: Description of the data displayed in the Update status panel

Lists accessible from the panel

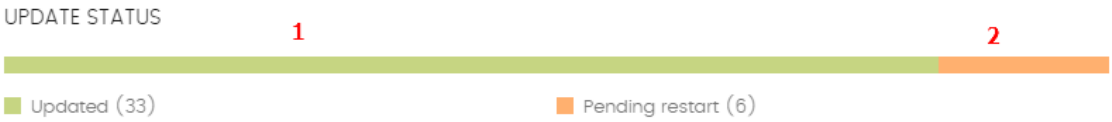


Figure 13.8: Hotspots in the Update status panel

Click the hotspots shown in **Figure 13.8:** to open the **Cytomic Data Watch status** list with the following predefined filters:

Hotspot	Filter
(1)	Updated protection = Yes.
(2)	Updated protection = Pending restart.
(3)	Updated protection = No.

Table 13.16: Filters available in the Cytomic Data Watch status list

Indexing status

Shows the status of computers with respect to the indexing status of the storage drives connected.

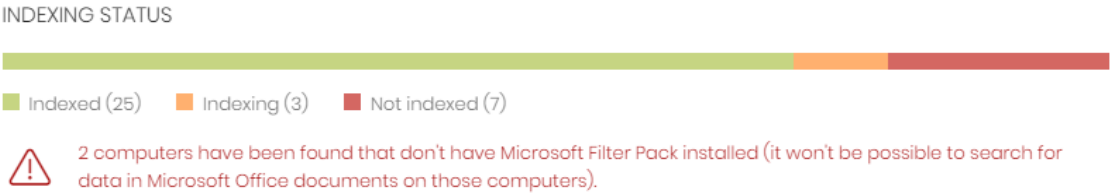


Figure 13.9: Indexing status panel

Meaning of the data displayed

Data	Description
Indexed	Number of computers where the contents of the storage drives are fully indexed. Requires that the searches and/or inventory be enabled. See **Cytomic Data Watch settings**.
Not indexed	Number of computers where the contents of the storage drives are not indexed. Requires that the searches and/or inventory be enabled. See **Cytomic Data Watch settings**.
Indexing	Number of computers where the contents of the storage drives are in the

Data	Description
	process of being indexed. Requires that the searches and/or inventory be enabled. See **Cytomic Data Watch settings**.

Table 13.17: Description of the data displayed in the Indexing status panel

Lists accessible from the panel

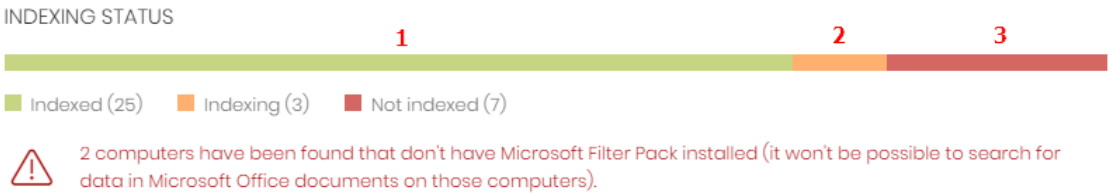


Figure 13.10: Hotspots in the Indexing status panel

Click the hotspots shown in **Figure 13.10:** to open the **Cytomic Data Watch status** list with the following predefined filters:

Hotspot	Filter
(1)	Indexing status = Indexed.
(2)	Indexing status = Indexing.
(3)	Indexing status = Not indexed.

Table 13.18: Filters available in the Cytomic Data Watch status list

Features enabled on computers

Shows the total number of computers on the network where Cytomic Data Watch is correctly installed and licensed, and which have reported the status of the three features that make up the module as **Enabled**.

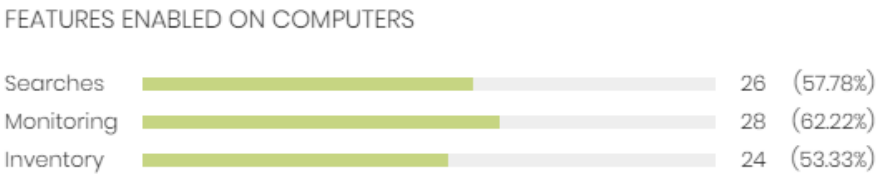


Figure 13.11: Features enabled on computers panel

Meaning of the data displayed

Data	Description
Searches	Shows the total number of computers which have reported the status of the feature for performing content-based searches in PII files as Enabled.
Monitoring	Shows the total number of computers which have reported the status of the PII file monitoring feature as Enabled.
Inventory	Shows the total number of computers which have reported the status of the PII inventory feature as Enabled.

Table 13.19: Description of the data displayed in the Features enabled on computers panel

Lists accessible from the panel

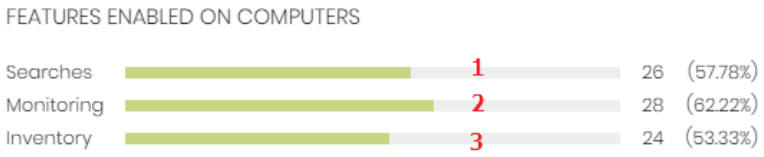


Figure 13.12: Hotspots in the Features enabled on computers panel

Click the hotspots shown in **Figure 13.12:** to open the **Cytomic Data Watch status** list with the following predefined filters:

Hotspot	Filter
(1)	Data searches on computers enabled = Yes.
(2)	Personal data monitoring enabled = Yes.
(3)	Personal data inventory enabled = Yes.

Table 13.20: Filters available in the Cytomic Data Watch status list

Files deleted by the administrator

Shows the different statuses of the files deleted by the administrator.

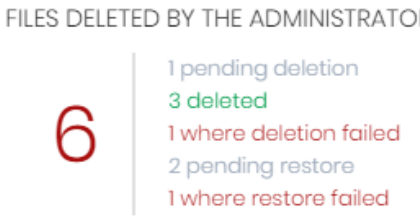


Figure 13.13: Files deleted by the administrator panel

Meaning of the data displayed

Data	Description
Pending deletion	Files marked for deletion which have not been deleted yet.
Deleted	Deleted files that remain in the Advanced EPDR backup area.
Where deletion failed	Files which could not be deleted.
Pending restore	Files marked for restore which have not been restored yet.
Restored	Files which have been moved from the backup area to their original location.

Table 13.21: Description of the data displayed in the Files deleted by the administrator panel

Lists accessible from the panel

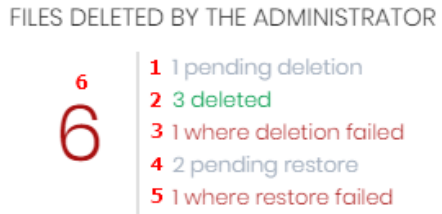


Figure 13.14: Hotspots in the Files deleted by the administrator panel

Click the hotspots shown in **Figure 13.14:** to open these lists with the following predefined filters:

Hotspot	List	Filter
(1)	Files with personal data.	Pending deletion.
(2)	Files deleted by the administrator.	Status = Deleted.

Hotspot	List	Filter
(3)	Files with personal data.	Error deleting.
(4)	Files deleted by the administrator.	Status = Pending restore.
(5)	Files deleted by the administrator.	Status = Error restoring.
(6)	Files deleted by the administrator.	Status = All.

Table 13.22: Lists accessible from the Files deleted by the administrator panel

Files with personal data

Shows the number of files with personal data found on the network and the total number of files with personal data found in the last daily inventory generated.

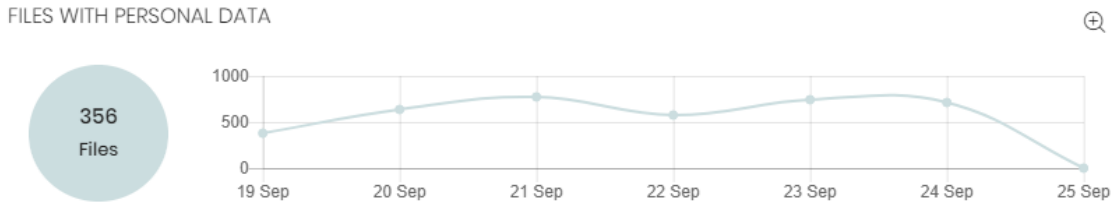


Figure 13.15: Files with personal data panel

Meaning of the data displayed

Data	Description
Bubble	Total number of PII files found according to the last inventory sent by each computer.
Line	Number of PII files found in the daily inventories generated on the dates indicated in the X-axis, on all computers on the network.

Table 13.23: Description of the data displayed in the Files with personal data panel

Lists accessible from the panel

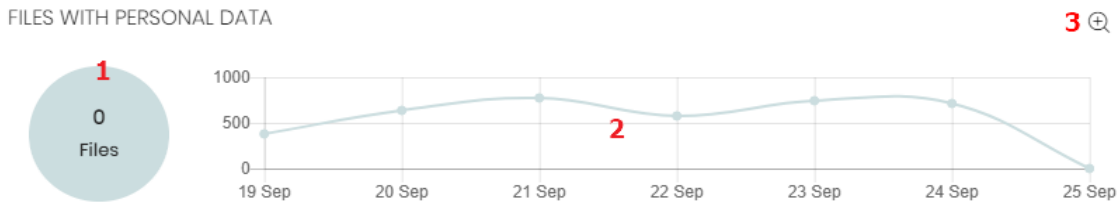


Figure 13.16: Hotspots in the Files with personal data panel

Click the hotspots shown in Figure 13.16: to open the **Files with personal data** list with the following predefined filters:

Hotspot	Filter
(1)	No filter.
(2)	Date 1 = Selected date and Date 2 = Current date.
(3)	Opens a window with more detailed information.

Table 13.24: Lists accessible from the Files with personal data panel

Files with personal data extended graph

Click the ⊕ icon to open a window with an extended version of the **Files with personal data** graph. This graph displays a different line for the number of PII files containing each of the supported entities.

- Follow these steps to configure the information displayed in the graph:
- Click the legend keys to enable/disable the relevant data series.
- Click the **Hide all data** link to display the number of PII files containing any type of entity.
- Click **Show all data** to display the number of PII files containing each type of supported entity.

Computers with personal data

Shows the number of workstations and servers with files containing personal data found in the last daily inventory generated.

Figure 13.17: Files with personal data panel

Meaning of the data displayed

Data	Description
Bubble	Number of computers containing PII files according to the last data sent by each computer.

Data	Description
Line	Total number of computers containing PII files found in the daily inventories generated on the dates indicated in the X-axis.

Table 13.25: Description of the data displayed in the Computers with personal data panel

Lists accessible from the panel

Figure 13.18: Hotspots in the Computers with personal data panel

Click the hotspots shown in **Figure 13.18:** to open the **Files with personal data** list with the following predefined filters:

Hotspot	Filter
(1)	No filter.
(2)	Date 1 = Selected date and Date 2 = Current date.

Table 13.26: Lists accessible from the Files with personal data panel

Files by personal data type

Shows the number of PII files found in the last daily inventory generated, by entity type.

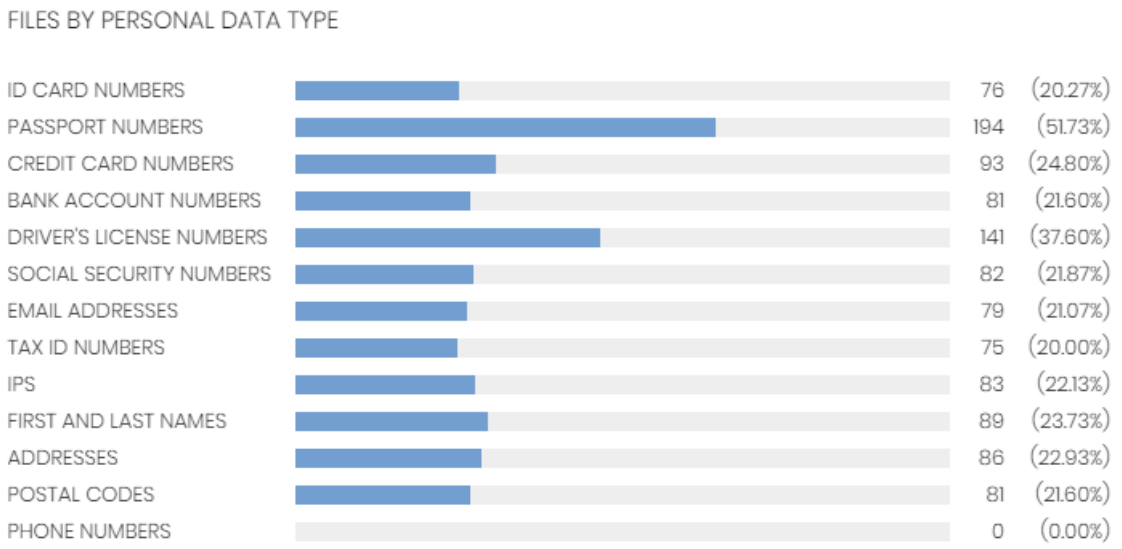


Figure 13.19: Files by personal data type panel

Meaning of the data displayed

Data	Description
Data	Total number of PII files found in the last daily inventory generated, by entity type, and percentage over the total number of PII files detected.

Table 13.27: Description of the data displayed in the Files by type personal data panel

Lists accessible from the panel

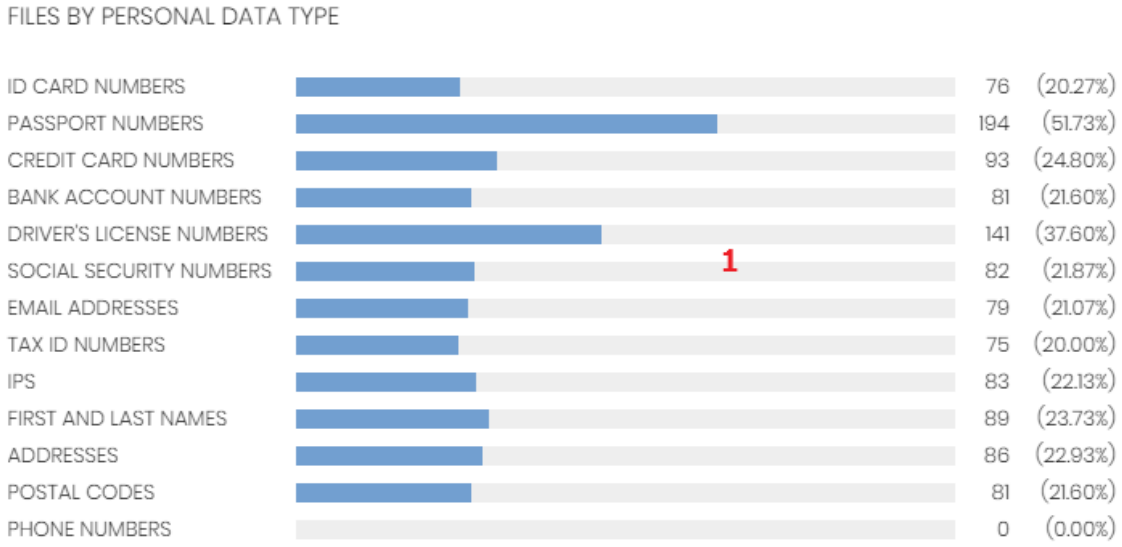


Figure 13.20: Hotspots in the Files by personal data type panel

Click the hotspot shown in the figure above to open the **Files with personal data** list with the following predefined filters:

Hotspot	Filter
(1)	Personal data = Selected entity.

Table 13.28: Lists accessible from the Files with personal data panel

Cytomic Data Watch lists

Accessing the lists

You can access the lists in two ways:

- Click the **Status** menu at the top of the console. Select **Cytomic Data Watch** from the side menu and click the relevant widget.

Or,

- Click the **Status** menu at the top of the console. Click the **Add** link from the side menu. A window opens with the available lists.
- Select a list from the **Data protection** section to view the associated template. Edit it and click **Save**. The list is added to the side menu.

Required permissions

Permission	Access to lists
No permissions	• Cytomic Data Watch status
View personal data inventory	• Files with personal data • Computers with personal data • Files deleted by the administrator

Table 13.29: Permissions required to access the Cytomic Data Watch lists

Cytomic Data Watch status

Shows all network computers and includes filters regarding the status of the Cytomic Data Watch module to find the computers or mobile devices that meet the criteria established in the panel.

Field	Comment	Values
Computer	Computer name.	Character string
Group	Folder within the Advanced EPDR folder tree the	Character string

Field	Comment	Values
	computer belongs to.	
Computer status	Agent reinstallation: •  Reinstalling the agent. •  Agent reinstallation error Protection reinstallation: •  Reinstalling the protection. •  Protection reinstallation error. •  Pending restart. Computer isolation status: •  Computer in the process of being isolated. •  Isolated computer. •  Computer in the process of stopping being isolated. "RDP attack containment" mode: •  Computer in "RDP attack containment" mode. •  Ending "RDP attack containment" mode.	Icon
Personal data monitoring	Indicates whether Cytomic Data Watch can monitor the personal data files found on the computer's storage devices. If it cannot, it indicates the reason.	•  Error installing and Error •  Disabled •  Enabled •  No license • No information
Inventory	Indicates whether Cytomic Data Watch can	•  Error

Field	Comment	Values
	generate an inventory of the personal data files found on the computer's storage devices. If it cannot, it indicates the reason.	installing and Error • Disabled • Enabled • No license • No information
Searches	Indicates whether Cytomic Data Watch can search for files on the computer's storage devices. If it cannot, it specifies the reason.	• Error installing and Error • Disabled • Installing • Enabled • No license • No information
Updated	Indicates whether the Cytomic Data Watch module installed on the computer is the latest release or not. Point the mouse to the field to see the version of the installed protection.	• Updated • Pending restart • Not updated
Microsoft Filter Pack	Indicates whether all required Microsoft Filter Pack components are installed on the computer or not.	• Installed • Not installed

Field	Comment	Values
		• — Information not available
Indexing status	Indicates the status of the file indexing process.	• Indexing • Indexed (Text only or All content) • Not indexed • — Not available
Last connection	Date when the Advanced EPDR status was last sent to the Cytomic cloud.	Date

Table 13.30: Fields in the Cytomic Data Watch status list

*To view a graphical representation of the list data, go to the following widgets as appropriate: **Deployment status**, **Offline computers**, **Update status**, **Features enabled on computers**, or **Indexing status**.*

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string

Field	Comment	Values
IP address	The computer's primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description		Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
Agent version		Character string
Installation date	Date when the Advanced EPDR software was successfully installed on the computer.	Date
Last connection date	Date when the computer status was last sent to the Cytomic cloud.	Date
Last update on	Date the agent was last updated.	Date
Platform	Operating system installed on the computer.	• Windows • Linux • macOS • Android
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Updated protection	Indicates whether the protection module is updated to the latest version or not.	Binary value
Protection version	Internal version of the protection module.	Character string
Updated knowledge	Indicates whether the signature file on the computer is the latest version or not.	Binary value
Last update on	Date the signature file was last updated.	Date

Field	Comment	Values
Personal data monitoring	Indicates whether Cytomic Data Watch can monitor the personal data files found on the computer's storage devices. If it cannot, it indicates the reason.	• Error installing • Error • Disabled • OK • No license • No information
Personal data inventory	Indicates whether Cytomic Data Watch can generate an inventory of the personal data files found on the computer's storage devices. If it cannot, it indicates the reason.	• Error installing • Error • Disabled • OK • No license • No information
Searches	Indicates whether Cytomic Data Watch can search for files on the computer's storage devices. If it cannot, it specifies the reason.	• Error installing • Error • Disabled • OK • No license • No information
Microsoft Filter Pack	Indicates whether all required Microsoft Filter Pack components are installed on the computer or not.	• Installed • Not installed • Not available
Indexing status	Indicates the status of the file indexing process.	• Indexing • Indexed • Not indexed • Not available
Indexing type	Shows the indexing type applied to the computer.	• Text only • All content

Field	Comment	Values
Isolation status	Indicates if the computer has been isolated or can communicate normally with all other computers on the network.	• Isolated • Not isolated
Installation error date	Date of the unsuccessful attempt to install Cytomic Data Watch.	Date
Installation error	Reason for the installation error.	Character string

Table 13.31: Fields in the Cytomic Data Watch status exported file

Filter tool

Field	Comment	Values
Computer type	Filters computers according to type.	• Workstation • Laptop • Mobile device • Server
Search computer	Filters computers by name.	Character string
Last connection	Date when the Cytomic Data Watch status was last sent to the Cytomic cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago

Field	Comment	Values
		• More than 30 days ago
Updated protection	Filters according to the protection version installed on computers.	• All • Yes • No • Pending restart
Indexing status	Filters computers according to the file indexing status.	• All • Indexing • Indexed • Not indexed • Not available
Indexing type	Shows computers that have a specific type of indexing assigned.	• All • Text only • All content
Microsoft Filter Pack	Filters computers according to whether they have all required Microsoft Filter Pack components.	• All • False • True
Cytomic Data Watch status	Filters computers according to the status of the Cytomic Data Watch module.	• Installing... • No information • OK • Personal data monitoring disabled • Data searches on computers disabled • Error • Error installing

Field	Comment	Values
		• No license • Personal data monitoring enabled • Data searches on computers enabled • Personal data inventory enabled • Personal data inventory disabled

Table 13.32: Filters available in the Cytomic Data Watch status list

Files with personal data

Shows all PII files found on your network, along with their type, location, and other relevant information.

Because Cytomic Data Watch keeps only the last complete inventory generated for each machine, those computers that were turned off at the time when the inventory was generated only display information in the **Files with personal data** list if the date displayed in the **Last seen** column falls within the range selected for the feature.

Field	Comment	Values
Computer	Computer name.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
File	Name of the file.	Character string
Path	Full path to the folder that contains the file on the computer.	Character string
Personal data	Personal data type found in the file.	• Personal ID

Field	Comment	Values
		number entity •  Passport number entity •  Credit card number entity •  Bank account number entity •  Social Security Number entity •  Driver's license number entity. •  Email address entity. •  IP address entity. •  First name and last name entity •  Physical address entity •  Phone number entity
Last seen	Date when the last snapshot of the computer's file system was taken.	Date

Table 13.33: Fields in the Files with personal data list

*To view a graphical representation of the list data, see the **Files by personal data type** widget.*

Fields displayed in the exported file

Field	Comment	Values
Computer	Computer name.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
File	Name of the file.	Character string
Path	Full path to the folder that contains the file on the computer.	Character string
Personal ID numbers	ID card number entity.	Boolean
Passport numbers	Passport number entity.	Boolean
Credit card numbers	Credit card number entity.	Boolean
Bank account numbers	Bank account number entity.	Boolean
Driver's license numbers	Driver's license number entity.	Boolean
Social security numbers	Social Security Number entity.	Boolean
Email addresses	Email address entity.	Boolean
IPs	IP address entity.	Boolean
First and last	First name and last name entity.	Boolean

Field	Comment	Values
names		
Addresses	Physical address entity.	Boolean
Phone numbers	Phone number entity.	Boolean
Last seen	Date when the file was last included in the daily inventory.	Date
Status	File status.	• Deleted • Pending deletion • Restored • Pending restore • Error restoring
Error	• The file is in use. • The content of the file has changed with respect to the file in the inventory. • The file has been deleted by the computer user in the time between when the inventory was generated and when the administrator launched the deletion action. • An error occurred trying to delete the file.	Character string

Table 13.34: Fields in the Files with personal data exported file

Filter tool

Field	Comment	Values
Computer type	Filters computers according to type.	• Workstation • Laptop • Server
Last seen	Shows the inventory of the computers that were last	• All

Field	Comment	Values
	seen within the selected date range.	• Last 24 hours • Last 7 hours • Last month • Last year
Personal data	Indicates the entity type found in the PII file.	• Personal ID numbers • Credit card numbers • Driver's license numbers • Email addresses • IPs • Addresses • Phone numbers • Passport numbers • Bank account numbers • Social security numbers • Tax ID numbers • First and last names

Table 13.35: Filters available in the Files with personal data list

Computers with personal data

Shows the number of PII files found on each computer on your network. The list displays different types of information depending on the way the **Date 1** and **Date 2** filters are configured:

- If fields **Date 1** and **Date 2** are set, the list displays the variation in the number of PII files found on each computer between those two dates. That is, it displays the evolution of the number of PII files found on each computer on the network.

- If fields **Date 1** and **Date 2** are empty, the list displays the number of PII files found on each computer on the network, according to the result of the last complete inventory generated.
- If field **Date 1** is set, the list displays the number of PII files found on each computer on the network, according to the result of the complete inventory generated on the selected date.

To view a list of the PII files found on a computer, click its name. The **Files with personal data** list opens filtered by the name of the selected computer.

Field	Comment	Values
Computer	Computer name.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
Files (date)	Name of the file.	Character string
Variation	Difference between the number of PII files found on Date 1 and Date 2. If the number is positive, the ↑ icon is displayed. If the number is negative, the ↓ icon is displayed.	Numeric value

Table 13.36: Fields in the Computers with personal data list

*To view a graphical representation of the list data, see the **Computers with personal data** widget.*

Fields displayed in the exported file

Field	Comment	Values
Computer	Computer name.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
Date 1	Start date to see the evolution of PII files.	Date

Field	Comment	Values
Inventory date	Date when the computer's complete inventory was generated.	Date
Files with personal data	Number of PII files found on the date specified on Date 1.	Numeric value
Passport numbers	Number of PII files containing the Passport number entity found on the date specified on Date 1.	Numeric value
Credit card numbers	Number of PII files containing the Credit card number entity found on the date specified on Date 1.	Numeric value
Bank account numbers	Number of PII files containing the Bank account number entity found on the date specified on Date 1.	Numeric value
Driver's license numbers	Number of PII files containing the Driver's license number entity found on the date specified on Date 1.	Boolean
Social security numbers	Number of PII files containing the Social Security Number entity found on the date specified on Date 1.	Numeric value
Email addresses	Number of PII files containing the Email address entity found on the date specified on Date 1.	Numeric value
Tax ID numbers	Number of PII files containing the Tax ID number entity found on the date specified on Date 1.	Numeric value
IPs	Number of PII files containing the IP address entity found on the date specified on Date 1.	Numeric value
First and last names	Number of PII files containing the First and last names entity found on the date specified on Date 1.	Numeric value
Addresses	Number of PII files containing the Physical address entity found on the date specified on Date 1.	Numeric value
Phone	Number of PII files containing the Phone number entity	Numeric

Field	Comment	Values
numbers	found on the date specified on Date 1.	value
Date 2	Start date to see the evolution of PII files.	Date
Inventory date	Date when the computer's complete inventory was generated.	Date
Files with personal data	Number of PII files found on the date specified on Date 2.	Numeric value
Passport numbers	Number of PII files containing the Passport number entity found on the date specified on Date 2.	Numeric value
Credit card numbers	Number of PII files containing the Credit card number entity found on the date specified on Date 2.	Numeric value
Bank account numbers	Number of PII files containing the Bank account number entity found on the date specified on Date 2.	Numeric value
Driver's license numbers	Number of PII files containing the Driver's license number entity found on the date specified on Date 2.	Boolean
Social security numbers	Number of PII files containing the Social Security Number entity found on the date specified on Date 2.	Numeric value
Email addresses	Number of PII files containing the Email address entity found on the date specified on Date 2.	Numeric value
Tax ID numbers	Number of PII files containing the Tax ID number entity found on the date specified on Date 2.	Numeric value
IPs	Number of PII files containing the IP address entity found on the date specified on Date 2.	Numeric value
First and last names	Number of PII files containing the First and last names entity found on the date specified on Date 2.	Numeric value

Field	Comment	Values
Addresses	Number of PII files containing the Physical address entity found on the date specified on Date 2.	Numeric value
Phone numbers	Number of PII files containing the Phone number entity found on the date specified on Date 2.	Numeric value

Table 13.37: Fields in the Computers with personal data exported file

Filter tool

Field	Comment	Values
Search	Filters the list by computer name.	Character string
Date 1	First date to compare.	Date
Date 2	Second date to compare.	Date
Computer type	Filters computers according to type.	• Workstation • Laptop • Server
Personal data	Indicates the entity type found in the PII file.	• Personal ID numbers • Credit card numbers • Driver's license numbers • Email addresses • IPs • Addresses • Phone numbers • Passport numbers • Bank account numbers • Social security numbers • Tax ID numbers • First and last names
Variation	Shows computers with a	• **Positive**: The number of files found on

Field	Comment	Values
	positive/negative variation in the number of PII files found.	date 2 is higher than the number of files found on date 1. • **Negative**: The number of files found on date 2 is lower than the number of files found on date 1. • **All**

Table 13.38: Filters available in the Computers with personal data list

Computer details page

Click any of the rows in the list to open the computer details page. See **Computer details** on page **252** for more information.

Files deleted by the administrator

Shows the status of those files that have received a deletion or restore task and are still accessible on the computers on the network or in the backup area.

Field	Comment	Values
Date	Date when the file status changed.	Date
Computer	Computer name.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
File	Name of the file.	Files with personal data
Path	Location of the file on the computer's file system.	Character string
Performed by	Management console account responsible for the file status change.	Character string
Status	File status.	• All • Deleted • Pending deletion

Field	Comment	Values
		• Restored • Pending restore • Error restoring

Table 13.39: Fields in the Files deleted by the administrator list

*To view a graphical representation of the list data, see the **Files deleted by the administrator** widget .*

Fields displayed in the exported file (history)

This file displays the deletion and restore actions performed by the administrator on the files on the network.

Field	Comment	Values
Date	Date when the file status changed.	Date
Computer	Computer name.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
File	Name of the file.	Files with personal data
Path	Location of the file on the computer's file system.	Character string
Performed by	Management console account responsible for the file status change.	Character string
Status	File status.	• All • Deleted • Pending deletion • Restored

Field	Comment	Values
		• Pending restore • Error restoring

Table 13.40: Fields in the Files deleted by the administrator list

Fields displayed in the exported file (detailed history)

This file displays all deletion and restore actions performed by the administrator over time on the files on the network.

Field	Comment	Values
Date	Date when the file status changed.	Date
Computer	Computer name.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
File	Name of the file.	Files with personal data
Path	Location of the file on the computer's file system.	Character string
Performed by	Management console account responsible for the file status change.	Character string
Status	File status.	• All • Deleted • Pending deletion • Restored • Pending restore • Error restoring

Table 13.41: Fields in the Files deleted by the administrator list

Filter tool

Field	Comment	Values
Status	File status.	• All • Deleted • Pending deletion • Restored • Pending restore • Error restoring

Table 13.42: Filters available in the Files deleted by the administrator list

Supported program extensions

Suite name	Product	Extensions
Office	Word	• DOC • DOT • DOCX • DOCM • RTF
	Excel	• XLS • XLSM • XLSX • XLSB • CSV
	PowerPoint	• PPT • PPS • PPSX • PPSM • SLDX • SLDM

Suite name	Product	Extensions
		• POTX • PPTM • PPTX • POTM
OpenOffice	Writer	• ODM • ODT • OTT • OXT • STW • SXG • SXW
	Draw	• ODG • OTG • STD
	Math	• ODF • SXM
	Base	• ODB
	Impress	• OTP • ODP • STI • SXI
	Calc	• OTS • ODS • SXC
Plain text		• TXT
Web browsers	Internet Explorer	• HTM

Suite name	Product	Extensions
	Chrome Opera Other	• HTML • MHT • OTH
Mail clients	Outlook Outlook Express	• EML
Other	Adobe Acrobat Reader	• PDF
	Extensible Markup Language	• XML
	Contribute	• STC
	ArcGIS Desktop	• SXD

Table 13.43: List of supported program extensions

Supported packers and compressors

File compressor/packer/algorithm name	Extensions
7-ZIP	7Z
Bzip2	BZ2
Gzip	GZ
Binhex	HQX
LHARC	• LHA • LZH
Lempel-Ziv & Haruyasu	LZH
Lempel–Ziv–Oberhumer / lzop	LZO
Multi-Purpose Internet Mail	MME

File compressor/packer/algorithm name	Extensions
Lotus Notes Traveler	NTS
WinRAR	RAR
Tar	TAR
Tar & Gzip	TGZ
Uuencode	• UU • UUE
XXEncoding	• XX • XXE
PKZIP/PKWARE	ZIP

Table 13.44: List of supported compressor/packer extensions

Supported entities and countries

Cytomic Data Watch supports the following data types or entities:

- Bank account numbers.
- Credit card numbers.
- Personal ID numbers.
- IP addresses.
- Email addresses.
- Phone numbers.
- Driver's license numbers.
- Passport numbers.
- Social security numbers.
- First names and last names.
- Postal addresses and ZIP/postal codes.

Supported countries

The format of recognized data varies from country to country. Cytomic Data Watch recognizes data from the countries listed below:

- Germany
- Austria
- Belgium
- Denmark
- Spain
- Finland
- France
- Hungary
- Ireland
- Italy
- Norway
- Netherlands
- Portugal
- United Kingdom
- Sweden
- Switzerland

Chapter 14

Cytomic Patch (Updating vulnerable programs)

Cytomic Patch is a built-in module on Cytomic platform that finds computers on the network with known software vulnerabilities and updates them centrally and automatically. It minimizes the attack surface and prevents malware attacks on vulnerable workstations and servers.

Cytomic Patch supports Windows, macOS, and Linux operating systems. It detects both third-party applications with missing patches or in EOL (end of life), as well as all patches and updates published by Microsoft for all of its products (operating systems, databases, Office applications, etc.).

For more information about the vendors and applications supported by Cytomic Patch, see ***https://info.pandasecurity.com/patchmanagementapp/?type=windows****.*

Cytomic Patch does not support Extended Security Updates (ESU licenses). These licenses enable you to run Microsoft products past the end of support. For more information about ESU licenses, their availability, and end dates, see ***https://learn.microsoft.com/en-us/lifecycle/faq/extended-security-updates****.*

For more information about the Cytomic Patch module, see:

Creating and managing settings profiles *on page* ***294****: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*

Accessing, controlling, and monitoring the management console *on page* ***61****: Managing user accounts and assigning permissions.*

Managing lists *on page* ***48****: Information about how to manage lists.*

Chapter contents

Cytomic Patch features

You can access the features provided by Cytomic Patch from these sections in the management console:

- **To configure the discovery of missing patches**: Go to the **Patch management** settings section (top menu **Settings**, side panel **Patch management**). For more information, see **Configuring the discovery of missing patches**.
- **To configure patch exclusions**: Go to the **Available patches** list. For more information, see **Exclude patches for all or certain computers**.
- **To have visibility into the update status of the entire IT network**: Go to the **Cytomic Patch** dashboard (top menu **Status**, side panel). For more information, see **Patch management status**.
- **To view lists of missing patches**: Check the **Patch management status**, **Available patches**, and **End-of-Life programs** lists (top menu **Status**, side panel **My lists - Add**). For more information, see **Cytomic Patch module lists**.
- **To view a history of all installed patches**: Check the **Installation history** list (top menu **Status**, side panel **My lists - Add**). For more information, see **Installation history**.

- **To patch computers**: From the **Tasks** top menu, create an **Install patches** scheduled task. You can also patch computers from the context menus in the group tree available from the **Computers** top menu, from lists, and from **Computer details**. For more information, see **Download and install patches**.
- **To exclude computers from patch installation tasks**: You can exclude computers and computer groups from patch installation tasks. The ability to exclude computers from patch installation tasks is a feature aimed at service providers that use CYTOMIC Nexus to manage multiple customers.

  For more information, ssee **Security product settings** in the **CYTOMIC Nexus Administration Guide**.
- **To patch test computers**: When you configure Cytomic Patch, you can designate test computers to install patches on and verify the installation results before you install the patches on the other computers on the network. To designate test computers:
  - Create a Cytomic Patch settings profile. From the **Patch installation** drop-down menu, select **Designate as test computers and install patches**. Assign the settings profile to the computers you want to designate as test computers. For more information, see **Patch installation**.
  - Create a Cytomic Patch task. Enable the **Run the task only on test computers** toggle. For more information, see **Configuring a patch installation task**.
- **To uninstall patches**: Choose one of these options:
  - From the **Last patch installation tasks** widget, click the **View installation history** link. For more information, see **Last patch installation tasks**.
  - From the top menu, select **Status**. Click **My lists - Add**. Select the **Installation history** list. For more information, see **Installation history**.
  - From the top menu, select **Tasks**. Select the task that installed the patch you want to uninstall. Click **View installed patches**.
- Click the patch you want to uninstall. A page opens and shows the patch details and the **Uninstall** button if the patch supports this option. For more information, see **Uninstalling a patch**.

Cytomic Patch requirements

From 30 September 2024, you will not be able to add devices to the management console or install the protection software on new computers that run these operating system versions: Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008 (Windows 2008 R2 will continue to be supported). Existing computers in the management console will continue to be protected. See ***https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.***

Supported Windows operating systems

Workstations

- Windows 7 (32-bit and 64-bit)
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)
- Windows 11 (64-bit)

Servers

- Windows 2008 (32-bit and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2, and 2016
- Windows Server 2022

Support for Windows ARM-based computers

Cytomic Patch is partially compatible with Windows ARM systems:

- Detects 32-bit and 64-bit patches.
- Installs only 32-bit patches.
- Does not detect operating system patches.

These limitations do not apply to Linux or Mac computers.

Supported macOS operating systems

- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura
- macOS Sonoma

Installing operating system patches on Apple Silicon macOS computers

To install operating system patches on these computers, the computer user must enter their user name and password. The user has three attempts to enter valid credentials. After the patch is installed, the computer restarts automatically.

If the installation task includes other patches that do not require credentials, they install normally. See **Installing operating system patches on macOS computers**.

Supported Linux operating systems

Supported 64-bit distributions:

- **Red Hat**: 7.0 and higher; 8.0 and higher.
- **CentOS**: 7.0 and higher.
- **SUSE Linux Enterprise**: 12.0 and higher; 15.0 and higher.

To install patches correctly, make sure the computer repository settings have not been modified and point to the distribution vendor servers.

Unsupported computers

On computers not compatible with Cytomic Patch:

- Cytomic Patch does not install.
- Computers keep the Cytomic Patch settings profiles and tasks assigned to them, but they are not applied.
- The **Available patches** list does not show information about these computers or about the status of the patches installed.
- These computers do not count toward the number of Cytomic Patch licenses used.
- The installation history reports previous installations of Cytomic Patch as **Not available**.

Required URLs

- https://content.ivanti.com
- https://application.ivanti.com
- https://stlicense.ivanti.com
- https://help.ivanti.com
- https://license.shavlik.com

General workflow

Cytomic Patch is a comprehensive tool for patching and updating the operating systems and all programs installed on the computers on your network. To effectively reduce the attack surface of your computers, follow these steps:

- Make sure Cytomic Patch works correctly on the protected computers on your network.
- Make sure that all published patches are installed.
- Isolate computers with unpatched known vulnerabilities.
- Install the selected patches.
- Uninstall any patches that are causing malfunction problems (rollback).
- Exclude patches for all or certain computers.
- Make sure the programs installed on your computers are not in EOL (End-Of-Life) stage.
- Regularly check the history of patch and update installations.
- Regularly check the patch status of those computers where incidents have been recorded.

Make sure that Cytomic Patch works correctly

Follow these steps:

- Make sure that all computers on your network have a Cytomic Patch license assigned and the module is installed and running. Use the **Patch management status** widget.
- Make sure that all computers with a Cytomic Patch license assigned can communicate with the Cytomic cloud. Use the **Time since last check** widget.
- Make sure the computers that are to receive the patches have the Windows Update service running with automatic updates disabled.

*Enable the **Disable Windows Update on computers** toggle in the patch management settings profile for Advanced EPDR to manage the service correctly. For more information, see **General options**.*
*On devices running Windows 10 and higher, the operating system enables you to defer quality updates but not disable them. Therefore, these updates will be applied after 30 days despite you select **Disable Windows Update on computers**.*

Make sure that all published patches are installed

As software vendors discover flaws in their products, they publish updates and patches that must be installed on the affected systems in order to fix them. These patches have a criticality level and type associated to them:

- To view missing patches by type and criticality level, use the **Patch criticality** widget.
- To view details of the patches that are missing on a computer or computer group:
    - Go to the computer tree (top menu **Computers**, **My organization** tab in the side panel). Click the context menu of the computer group. Select **View available patches**. The **Available patches** list opens, filtered by the relevant group.

  Or,

    - Go to the computer list (top menu **Computers**). Click a computer's context menu. Select **View available patches**. The **Available patches** list opens, filtered by the relevant computer.
- To get an overview of all missing patches:
    - Go to **Status** in the top menu. Click **Add** in the **My lists** section of the side panel. Select the **Available patches** list.
    - Use the filter tool to narrow your search.
- To find computers that do not have a specific patch installed:
    - Go to **Status** in the top menu. Click **Add** in the **My lists** section of the side panel. Select the **Available patches** list.
    - Use the filter tool to narrow your search.
    - Click the context menu of the specific computer-patch you want to look for and select the option **View which computers have the patch available**.

Isolate computers with unpatched known vulnerabilities

To find and isolate computers that have not yet received published patches that fix known vulnerabilities, follow these steps:

- Go to **Status** in the top menu. Click **Add** in the **My lists** section of the side panel. Select the **Available patches** list.
- Click the context menu of a patch in the list and select **Isolate computer**.

Download and install patches

To install patches and updates, Cytomic Patch uses the task infrastructure implemented in Advanced EPDR.

Requirements

Patches released by Microsoft are installed using the Windows Update service on the target workstation or server. However, to prevent Cytomic Patch from overlapping with the Windows Update service, the latter should be configured to be inactive on the computer. See **General options**

Required permissions

The user account used to access the web console must have the **Install, uninstall, and exclude patches** permission assigned to its role. For more information about the permissions system, see **Managing roles and permissions** on page **69**.

Patch download and bandwidth savings

Before the solution installs a patch, the computer downloads it from the software vendor. The download occurs in the background on each computer when a patch installation task starts. To minimize bandwidth usage, the solution uses cache computers on the network to download and disseminate patches and updates.

Limits to downloading patches from proxy and cache computers

Patches can be downloaded directly from the Internet and also through a Advanced EPDR proxy or cache computer. See **Configuring downloads from cache computers** on page **315** and **Configuring proxies lists for Internet access** on page **313**.

There are limitations to using one method or another, depending on the computer operating system:

- **Computers with a Windows or macOS operating system**: They can download patches from cache computers and the Internet. They cannot download patches from the Advanced EPDR proxy.
- **Computers with a Linux operating system**: Linux computers use the distribution package manager to download patches from the Internet. They cannot download patches from the Advanced EPDR proxy or cache computers.

Cache computers store patches for up to 30 days, after which patches are deleted. If a computer requests a patch from a cache computer, but the cache computer does not have the patch in its repository, the computer waits for the cache computer to download it. The wait time depends on

the size of the patch to download. If the cache computer cannot download the patch, the target computer tries to download the patch instead.

After patches are applied to a target computer, they are deleted from the storage media.

Types of patch installation tasks

- **Quick (Install option)**: Downloads and installs the patch in real time but does not restart the computer, even if the installation requires a restart. Quick tasks start to download patches as soon as you create the task. This can result in high bandwidth usage if the task applies to many computers or the patches are large.
- **Scheduled (Schedule installation option):** Enables you to configure all settings related to the patch installation and start the task when you want. If the start time of multiple tasks coincides, the solution delays tasks up to 2 minutes to prevent simultaneous downloads and minimize bandwidth usage.

Interrupting patch installation tasks

You can cancel patch installation tasks if the installation process has not started yet on the target computers. If the installation process has already begun, however, you cannot cancel the task as doing so could cause errors on computers.

Patches corresponding to the operating system

Even if you set a computer with an incompatible operating system as the target for a specific patch, computers receive only patches that correspond to their operating systems.

Installing operating system patches on macOS computers

Some operating system patches for macOS computers require that the computer restart to complete patch installation, regardless of the restart options you select when configuring the patch installation task.

These patches contain new features, bug fixes, and enhancements for the operating system installed, but do not upgrade the operating system to a higher version. You can identify these patches because they include the text *SoftwareUpdate* in their name. This name appears on the **Detected patch** page and in the **Available patches** list.

Warning messages

Because installing these patches restarts the computer automatically, a warning message is shown to you and the computer user in these circumstances:

- When you select any of these patches from the list of available patches to create a quick or scheduled task. If you accept the message, the task runs (quick task), or you are taken to the task settings (scheduled task). See **From the Available patches list**.

- When you select **macOS** from **Install patches for the following products** upon configuring a patch installation task. A warning message appears for you to confirm whether you want to include those patches in the task. This option is disabled by default. See **Configuring a patch installation task**.
- The target computer for the task shows a message to the computer user informing that a patch installation task is in progress and the computer will restart.

Installation on Apple macOS computers

With Apple macOS computers, you must enter the volume owner user name and password to install operating system patches.

- **If the credentials are correct**: The **Installation** column in the **Available patches** list shows the **Pending restart** text. When patch installation is complete, the computer restarts automatically and the patch disappears from the list.
- **If the computer user cancels the installation**: The computer shows an error code on the task results page. See **Task results** on page **920**.

If the patch installation task for a macOS computer includes patches that do not require credentials, the patches proceed to install.

Installation on Intel macOS computers

In this case, you do not need to enter any credentials. The target computer for the task shows a message to the computer user informing that a patch installation task is in progress.

Because you cannot postpone the automatic restart, we recommend that you close and save any open files.

Patch installation in the console

From the Available patches list

- From the top menu, select **Status**.
- In the **My lists** section of the side panel, click **Add**. Select **Available patches**
- Use the filter tool to narrow your search.
- Select the checkboxes for the computers/patches you want to install.
- To create a quick task, select **Install** in the toolbar. To create a scheduled task, select **Schedule installation**. For more information about how to configure a scheduled task, see **Configuring a patch installation task**.

If the patches you select to install include operating system patches for macOS that require the computer to automatically restart, a warning message appears. See ***Installing operating system patches on macOS computers***

From the Available patches by computers list

- From the top menu, select **Status**.
- In the **My lists** section of the side panel, click **Add**. Select **Available patches by computers**.
- Use the filter tool to narrow your search.
- Click the context menu associated with the patch. A list appears and shows the **Available patches**. See **From the Available patches list**.

From the computer tree

- From the top menu, select **Computers**. From the left panel, select the **My organization** tab in the computer tree.
- To install patches on a group of computers, click the group context menu. Select **View available patches**. A list appears and shows the **Available patches**. See **From the Available patches list**.
- To schedule the installation of patches on a group of computers, click the group context menu. Select **Schedule patch installation**. A new patch installation task is created. For more information about how to configure it, see **Configuring a patch installation task**.

From the computer tree list

- From the top menu, select **Computers**. From the left panel, select the **My organization** tab in the computer tree.
- Select the group of computers. Select the checkboxes for the computers you want to patch.
- If you selected a single computer, click the computer context menu. Select **View available patches**. If you selected more than one, select **View available patches** in the toolbar above. A list appears and shows the **Available patches**. See **From the Available patches list**.
- To schedule installation of groups of patches, if you selected a single computer, click the computer context menu. Select **Schedule patch installation**. If you selected more than one, select **Schedule patch installation** in the toolbar above. A new patch installation task is created. For more information about how to configure it, see **Configuring a patch installation task**.

From the Tasks menu

From the top menu, select **Tasks**. Click **Add task**. Select **Install patches**.

Configuring a patch installation task

- Enter general details of the task in the **Name** and **Description** fields.
- If no recipients are defined, click the **No recipients selected** link in the **Recipients** section. A page opens where you can select the computers that will receive the configured task.

> *To access the computer selection page, you must first save the task. If you did not save the task, a warning message appears.*

- If you want to send the patch installation task only to computers you designated as test computers on your network, enable the **Run the task only on test computers** toggle. You designate a computer as a test computer in the Cytomic Patch settings profile you assign to it. See **Cytomic Patch features**.
- Select the types of computers you want to receive the task: **Workstation**, **Laptop**, or **Server**.
- Click ⊕ to add individual computers or computer groups. Click 🗑 to remove them.
- On the **Edit task** page, click the **View computers** button to view the computers that will receive the task.
- Schedule the task. You can configure these parameters:

- **Starts:** Indicates the task start date/time.

Value	Description
As soon as possible (selected)	The task runs immediately provided the computer is available (turned on and accessible from the cloud), or as soon as it becomes available within the time interval specified in the **If the computer is turned off** section
As soon as possible (cleared)	The task runs on the date selected in the calendar. Specify whether the time is based on the computer local time or the Advanced EPDR server time.
If the computer is turned off	If the computer is turned off or cannot be accessed, the task does not run. The task scheduler enables you to establish the task expiration time, from 0 (the task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available). • **Do not run:** The task is immediately canceled if the computer is not available at the scheduled time. • **Run the task as soon as possible, within:** Define a time interval during which the task will run if the computer becomes available. • **Run when the computer is turned on:** There is no time limit. The solution waits indefinitely for the computer to be available to run the task.

Table 14.1: Task execution parameters

- **Frequency**: Set a repeat interval (every day, week, month, or year) from the date specified in the **Starts:** field.

Value	Description
One time	The task runs only once at the time specified in the **Starts:** field.
Daily	The task runs every day at the time specified in the **Starts:** field.
Weekly	Use the checkboxes to select the days of the week on which the task must run, at the time specified in the **Starts:** field.

Value	Description
Monthly	Choose an option: • Run the task on a specific day of every month. If you select the 29th, 30th, or 31st of the month, and the month does not have that day, the task runs on the last day of the month. • Run the task on the first, second, third, fourth, or last Monday to Sunday of every month.

Table 14.2: Task frequency parameters

- In **Security patches**, select the criticality or importance of the patches to install.
- In **Install patches for the following products**, specify which products to install patches for. The product tree appears ordered by operating systems. Each operating system contains the patches that are available for it. Specify which products are to receive patches by selecting the relevant checkboxes in the product tree.

> *If the patches you select to install include operating system patches for macOS that require the computer to automatically restart, a message appears for you to confirm whether you want to include those patches in the task. See* ***Installing operating system patches on macOS computers***

Because the product tree is a dynamic resource that changes over time, keep these rules in mind when you select items from the tree:

- When you select a node, you also select all of its child nodes and all items dependent on them. For example, when you select Adobe you also select all nodes below that node.
- If you select a node, and Cytomic Patch automatically adds a child node to that branch, that node is selected as well. For example, as previously explained, selecting Adobe also selects all of its child nodes. Additionally, if, later, Cytomic Patch adds a new program or family to the Adobe group, that program or family is selected as well. Conversely, if you manually select a number of child nodes from the Adobe group, and later Cytomic Patch adds a new child node to the group, this is not automatically selected.
- The programs to patch are evaluated at the time when tasks run, not at the time when they are created or configured. For example, if Cytomic Patch adds an entry to the tree after you have created a patch task, and that entry is selected automatically

in accordance with the aforementioned mechanism, the task installs the patches associated with that new program when it runs.

- In the **Restart options** section, select an option to specify whether computers must restart automatically after patches install.
    - **Do not restart automatically**: If you select this option, users see a message indicating that their computer must restart and can select whether to restart **immediately** or **later**. If the latter is selected, a reminder appears 24 hours later.

      Computers with a Linux operating system without a GUI are sent a message reminding of the need to restart to complete the patch installation.

    - **Automatically restart workstations only**: Select the time interval to restart workstations. At the end of the set time, the agent shows the computer user a reminder message with the **Restart now** button and a countdown timer indicating how much time they have left before the computer restarts.

      Computers with a Linux operating system without a GUI are sent a message informing of the time remaining until the restart.

      As the restart approaches, you are no longer able to close the notification message. Every 30 minutes, the message appears on screen to remind the user of the need to restart. When the countdown finishes, the computer restarts automatically.

    - **Automatically restart servers only**: This option behaves in the same way as **Automatically restart workstations only**, but applies to servers only.
    - **Automatically restart both workstations and servers**: This option behaves in the same way as **Automatically restart workstations only**, but applies to both workstations and servers.
- Click **Save**. The task is added to the list of configured tasks. However, it shows the **Unpublished** label, meaning that it is not yet active.
- To publish a task, click the **Publish** button. The task is added to the Advanced EPDR task scheduler, which runs it in accordance with its settings.

When two or more patch installation tasks that require a restart overlap in time, Advanced EPDR restarts the computer when indicated by the task whose restart interval is closer in time. This avoids postponing the computer restart indefinitely if multiple successive patch installation tasks are chained together.

Lower versions of the security software

Lower versions of Advanced EPDR that do not support the feature of setting the restart interval set it to 4 hours automatically.

If the recipient computers have a lower version of the security software installed, they might not correctly interpret frequency settings. These computers interpret the task frequency settings as follows:

- **Daily tasks**: Unchanged.
- **Weekly tasks**: Recipient computers ignore the days selected in the task by the administrator in the latest software. The first run occurs on the specified start date and then runs again every 7 days.
- **Monthly tasks**: Recipient computers ignore the days selected in the task by the administrator in the latest software. The first run occurs on the specified start date and then runs again every 30 days.

Download patches manually

In some cases, Advanced EPDR cannot get a download URL to install a patch automatically. This can occur for several reasons:

- The patch requires payment, is not a publicly available patch, or requires user registration to download.
- Patches protected by an EULA cannot be downloaded and distributed by Cytomic.

In such cases, Cytomic Patch provides a link to manually download the patch. If the link is not helpful, contact the vendor of the software to patch.

For these patches, you can download the patch manually and add it to the patch repository so other computers can install it.

You cannot download patches manually on Linux or macOS computers or devices.

To manually add a patch to the repository, you must have the download URL of the patch. To install patches that require manual download, follow these steps:

- Identify patches that you must manually download.
- Get the patch download URL from the vendor and download the patch.
- Add the downloaded patch to the patch repository.
- Mark the patch as manually downloaded and available to install.
- Optional: Disable a manually downloaded patch for installation.

Identify patches that require manual download

- From the top menu, select **Status**. In the **My lists** side panel, click **Add**. A dialog box opens that shows all available lists.
- Select the **Available patches** list. Configure these filters:
  - **Installation**: Requires manual download.
  - **Show non-downloadable patches**: Yes.
- Click the **Launch query** button. The list shows all patches that computers on the network require which Cytomic Patch cannot download automatically.

Get the download URL and download the patch

- After following the steps in the previous section, in the **Identify patches that require manual download** list, click a patch that requires manual download. The **Patch detected** page opens and shows details of the patch.
- Note the file name shown in the **Patch details** section. To download the patch, click the **Download URL** link.

Add the downloaded patch to the patch repository

- Identify a computer on the network that has Advanced EPDR installed and has the cache role. Copy the downloaded file to this path on the cache computer:

```
C:\ProgramData\Panda Security\Panda Aether
Agent\Repository\ManuallyDeploy.
```

If you installed Advanced EPDR on a computer drive that differs from the default installation drive, copy the file to:
`X:\Panda Security\Panda Aether Agent\Repository\ManuallyDeploy`
Where X is the drive where the repository is located. For more information, see ***Specifying the storage drive*** *on page* ***311****.*

- If the **ManuallyDeploy** folder does not exist, create it with read and write administrator permissions.
- If needed, rename the downloaded file to match the File Name you noted in the **Get the download URL and download the patch** section.

Mark the patch as Manually downloaded

- After you copy the patch to the repository, go to the **Available patches** list. Click the context menu associated with the patch.
- From the drop-down menu, select **Mark as manually downloaded**. After you mark a patch as manually downloaded, its status changes from **Requires manual download** to **Pending (manually downloaded)** for all computers that need to install it and the patch can be installed like an automatically downloaded patch. For more information, see **Download and install patches**.

Cytomic Patch does not check whether there are patches with the ***Pending (manually downloaded)*** *status on cache computers, or whether computers on the network that require a patch have a cache computer assigned that has the patch in its repository. You must make sure that cache computers used for patch downloads have all necessary manually downloaded files in the* ***ManuallyDeploy*** *folder.*

Disable a manually downloaded patch for installation

If you no longer want a manually downloaded patch to be available to install, you can disable the patch for installation. To disable a manually downloaded patch for installation:

- Go to the **Available patches** list and configure a filter with these characteristics:
  - **Installation**: Pending (manually downloaded).
  - **Show non-downloadable patches**: Yes.

- Click the **Filter** button. The list shows all patches manually downloaded and enabled for installation.
- Click the context menu of any patches you want to disable installation for. Select **Mark as 'Requires manual download'**  . The patch disappears from the repository of installable patches, and you cannot install it.

Uninstall problematic patches

Sometimes, the patches published by software vendors do not work correctly, which can lead to serious problems. This can be avoided by selecting a small number of test computers prior to deploying a patch across the entire network. In addition to this, Cytomic Patch also enables you to remove (roll back) installed patches.

Linux and macOS do not support patch uninstallation.

Requirements for uninstalling an installed patch

- You must have the **Install/Uninstall patches** permission enabled. See **Install, uninstall, and exclude patches** on page **77** for more information.
- The patch must have been successfully installed.
- The patch must support the rollback feature. Not all patches support this feature.

Uninstalling a patch

- Go to the patch uninstallation page. There are three ways to do this:
  - Go to the **Status** menu at the top of the console. Click **My lists - Add** in the side panel. Select **Installation history**
  - Go to the **Tasks** menu at the top of the console. Select the task that installed the patch you want to uninstall. Click the **View installed patches** link in the upper-right corner of the page.
  - Access the **Last patch installation tasks** widget. To do this, go to the **Status** menu at the top of the console and select **Cytomic Patch** from the side menu. Click **Installation history**.
- From the list displayed, select the patch you want to uninstall.
- If the patch can be removed, the **Uninstall the patch** button is displayed. Click the button. The computer selection window appears.

- Select **Uninstall from all computers** to remove the patch from all computers on the network.
- Select **Uninstall from "{{hostName}}" only** to remove the patch from the selected computer only.

- Cytomic Patch creates an immediate execution task to uninstall the patch.
- If a restart is required to finish uninstalling the patch, the solution waits for the user to restart it manually.

> *An uninstalled patch is displayed again in the list of available patches unless it is excluded. If a scheduled patch installation task has been configured and the patch has not been excluded, it will be reinstalled on the next execution. However, if a patch is withdrawn by the corresponding vendor, it will no longer be shown or installed. See* ***Exclude patches for all or certain computers*** *for more information.*

Check the result of patch installation/uninstallation tasks

Go to the **Tasks** menu at the top of the console to view those tasks in which patches have been installed or uninstalled from computers. Both provide a **View results** option that enables you view on which computers the action was taken and which patches were installed/uninstalled. See **Patch installation/uninstallation task results** and **View installed/uninstalled patches** for more information.

Exclude patches for all or certain computers

You have the option to prevent the installation of malfunctioning patches or patches that significantly change the characteristics of the target program. This is called excluding the patch. To do this, follow these steps:

- Go to the **Status** menu at the top of the console. Click **Add** from the **My lists** menu on the left. Click the **Available patches** list. This list displays a line for each computer-available patch pair. An available patch is a patch that has not been installed yet on a specific computer or has been uninstalled from it.
- To exclude a single patch, click the context menu ⋮ associated with the patch. Select the **Exclude** option. A window opens for you to select the exclusion type.
  - **Exclude for X only**: Excludes the patch for the selected computer only.
  - **Exclude for all computers**: Excludes the patch for all computers on the network.
- To exclude several patches and/or a single patch for multiple computers, select them using the relevant checkboxes. From the action bar, choose **Exclude**. A window opens for you to select the exclusion type.

- **Exclude for the selected computers only**: Excludes the patches for the selected computers only.
- **Exclude for all computers**: Excludes the patches for all computers on the network.

When you exclude a patch, you exclude a specific version of the patch. That is, if you exclude a patch, and later the software vendor releases a later version of that patch, this is not automatically excluded.

Make sure the programs installed are not in EOL (End-Of-Life) stage

Programs in EOL (End-Of-Life) stage do not receive any type of update from the relevant software vendor, therefore it is advisable to replace them with an equivalent program or a more advanced version.

Follow these steps to find those programs on the network that have reached their EOL or will reach it shortly:

- Go to the **Status** menu at the top of the console. Select **Cytomic Patch** from the side panel.
- Find the **End-of-Life programs** widget, which is divided into the following sections:
  - **Currently in EOL**: Programs on the network that do not receive updates from the relevant vendor.
  - **In EOL (currently or in 1 year)**: Programs on the network that have reached their EOL, or will reach their EOL in a year.
  - **With known EOL date**: Programs on the network with a known EOL date.

Follow these steps to find all programs on your network with a known EOL date:

- Go to top menu **Status**. Click **Add** in the **My lists** section in the side panel.
- Select **End-of-Life programs**.

The list displays a line for each computer-EOL program combination found.

Check the history of patch and update installations

To find out if a specific patch is installed on the computers on your network:

- Go to top menu **Status**. Click **Add** in the **My lists** section in the side panel.
- Select **Installation history**.

The list displays a line for each computer/installed patch combination found, with information about the affected program's or operating system's name and version, and the patch criticality/type.

Click a computer's context menu to display a number of options that enable you to:

- View the patch installation or uninstallation task.
- View all patches installed on the computer.
- View all computers that have the selected patch installed.

Check the patch status of computers with incidents

Cytomic Patch correlates those computers where incidents have been recorded with their patch status so that you can determine whether an infected computer or a computer where threats have been detected has missing patches.

To check whether a computer where an incident has been detected has missing patches:

- Go to top menu **Status**. In the widgets **Threats detected by the antivirus**, **Malware activity**, **PUP activity**, **Exploit activity**, or **Currently blocked programs being classified**, click a computer or incident. Information about the threat detected on the computer is displayed.
- In the **Affected computer** section, click the **View available patches** button. The **Available patches** list opens, filtered by the relevant computer.
- Select all of the available patches for the computer and click **Install** from the action bar in order to create a quick patch installation task.

Because the patching process may require downloading patches from the software vendor's servers and therefore delay their application, it is advisable to isolate any infected computer that needs patching and shows network traffic in the threat's life cycle. This minimizes the risk of spreading the infection to other computers on the corporate network while the patch operation is taking place. See ***Forensic analysis*** *on page* ***819*** *for more details of the malware life cycle and* ***Isolating one or more computers from the organization network*** *on page* ***890*** *for more information.*

Configuring the discovery of missing patches

Accessing the settings

- From the top menu, select **Settings**. From the side menu, select **Patch management**.
- Click the **Add** button. The settings page opens.

Required permissions

Permission	Access type
Patch management	Create, edit, delete, copy, or assign patch management settings profiles.
View patch management settings	View patch management settings profiles.

Table 14.3: Permissions required to access the patch management settings

General options

- Enter a name and description for the settings profile.
- To make sure that Cytomic Patch manages Windows updates on your computers, enable the **Disable Windows Update on computers** toggle.

> *On devices running Windows 10 and higher, the operating system enables you to defer quality updates, but not disable them. Therefore, these updates are applied after 30 days despite you select* ***Disable Windows Update on computers****.*

- Click **Save**.
- From the list of profiles, select the profile you created. The **Edit settings** page opens. To select the computers you want to assign the settings profile to, click the **Recipients (No recipients selected)** link.
- To add computers individually, click . To remove them, click .
- On the **Edit settings** page, enable the **Automatically search for patches** toggle to enable patch search functionality.If the toggle is not enabled, patch management lists do not show missing patches, although you can use patch installation tasks to install missing patches on computers.

Patch installation

When you configure Cytomic Patch, you can select different patch installation options to apply to recipient computers and computer groups:

- **Install patches:** Installs patches on recipient computers and computer groups.
- **Designate as test computers and install patches**: Identifies recipient computers and computer groups as test computers for patch installation. For more information, see **Cytomic Patch features**.
- **Do not install patches**: Does not install patches on recipient computers or computer groups. This option is applicable to service providers who purchased CYTOMIC Nexus. For more information, see **Security produc settings** chapter in Administration Guide of CYTOMIC Nexus.

Search frequency

Search for patches with the following frequency specifies how often Cytomic Patch searches the cloud-based patch database to check for missing patches for your computers.

Patch criticality

Specifies the importance (or criticality) of the patches that Cytomic Patch searches for in the databases of available patches.

Windows Service Packs are not applied to macOS or Linux computers or devices.

Software vendors define the importance of the security patches they make available to address vulnerabilities. Patch classifications are not universal and vary by vendor. To determine whether you want to install a patch, we recommend that you review its description, especially for patches that a vendor does not classify as Critical.

*The **Other patches** category includes patches with bug fixes and feature enhancements for macOS and Linux.*

Cytomic Patch widgets/panels

Accessing the dashboard

To access the dashboard, select the **Status** menu at the top of the console. Select Cytomic Patch from the side menu.

Required permissions

Permissions	Access to widgets
No permissions	• Patch management status • Time since last check

Permissions	Access to widgets
Install, uninstall, and exclude patches	• End-of-Life programs • Available patches • Last patch installation tasks
View available patches	• End-of-Life programs • Available patches • Last patch installation tasks

Table 14.4: Permissions required to access the Patch management widgets

Patch management status

Shows computers where Cytomic Patch is working correctly and computers where there have been errors or problems installing or running the module. The status of the module is represented with a circle with different colors and associated counters. The panel provides a graphical representation and percentage of computers with the same status.

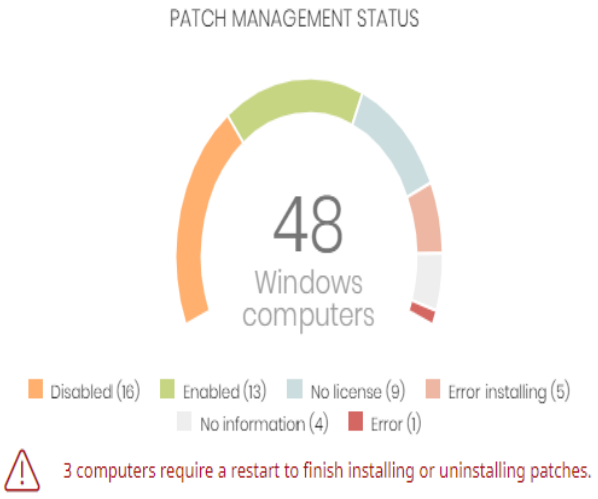


Figure 14.1: Patch management status panel

Meaning of the data displayed

Data	Description
Enabled	Cytomic Patch installed successfully, runs with no issues, and the assigned settings enable the module to search for patches automatically.
Disabled	Cytomic Patch installed successfully, runs with no issues, but the assigned

Data	Description
	settings do not enable the module to search for patches automatically.
No license	Computers that are compatible with Cytomic Patch, but do not have a Advanced EPDR license assigned.
Error installing	The module could not install.
No information	The computer has a license, but has not yet reported status to the server, or has an outdated agent installed.
Error	Cytomic Patch does not respond to requests sent from the server, or has settings that are different from those configured in the web console.
Central area	Shows the total number of computers compatible with the Cytomic Patch module.
Pending restart	Shows the number of computers that require a restart to finish installing or uninstalling patches.

Table 14.5: Description of the data displayed in the Patch management status panel

Lists accessible from the panel

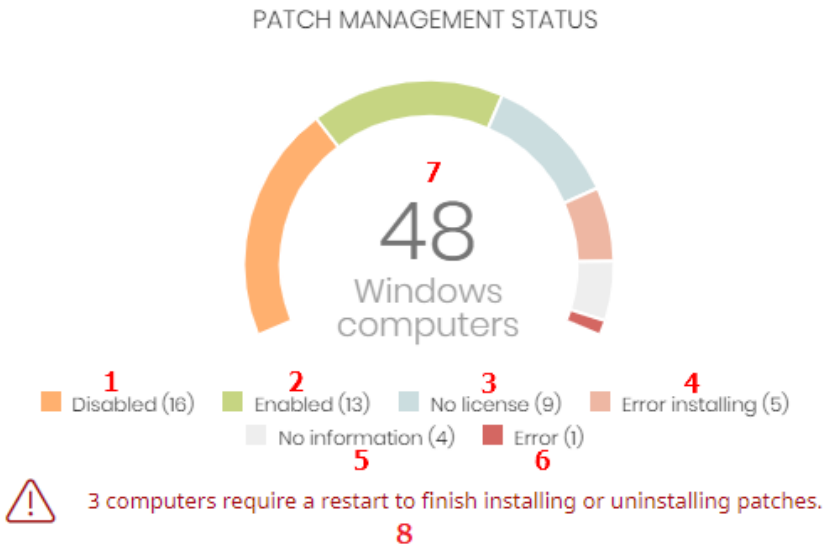


Figure 14.2: Hotspots in the Patch management status panel

Click the hotspots shown in **Figure 14.2:** to access the **Patch management status** list with the following predefined filters:

Hotspot	Filter
(1)	Patch management status = Disabled.
(2)	Patch management status = Enabled.
(3)	Patch management status = No license. The computer does not have a Advanced EPDR license assigned.
(4)	Patch management status = Error installing.
(5)	Patch management status = No information.
(6)	Patch management status = Error.
(7)	No filter.
(8)	Patch management status = Pending restart.

Table 14.6: Filters available in the Patch management status list

Time since last check

Shows the number of computers that have not connected to the Cytomic cloud and reported patch status for more than 3, 7, and 30 days. Use this panel to identify computers that might be at risk and require your attention.

Figure 14.3: Time since last check panel

Meaning of the data displayed

Data	Description
72 hours	Number of computers that have not reported patch status in the last 72 hours.
7 days	Number of computers that have not reported patch status in the last 7 days.

Data	Description
30 days	Number of computers that have not reported patch status in the last 30 days.

Table 14.7: Description of the data displayed in the Time since last check panel

Lists accessible from the panel

Figure 14.4: Hotspots in the Time since last check panel

Click the hotspots shown in **Figure 14.4:** to open the **Patch management status** list with the following predefined filters:

Hotspot	Filter
(1)	Last connection = More than 3 days ago and Patch management status = Enabled or Disabled or No information or Error.
(2)	Last connection = More than 7 days ago and Patch management status = Enabled or Disabled or No information or Error.
(3)	Last connection = More than 30 days ago and Patch management status = Enabled or Disabled or No information or Error.

Table 14.8: Filters available in the Patch management status list

End-of-Life programs

Shows information about programs that have reached or are close to end-of-life, grouped by end-of-life date.

Figure 14.5: End-of-Life programs panel

Meaning of the data displayed

Data	Description
Currently in EOL	Programs that have reached end-of-life.
In EOL (currently or in 1 year)	Programs that have reached end-of-life or will in the next year.
With known EOL date	Programs that have a known end-of-life date more than one year in the future.

Table 14.9: Description of the data displayed in the End-of-Life programs panel

Lists accessible from the panel

Figure 14.6: Hotspots in the End-of-Life programs panel

Click the hotspots shown in **Figure 14.6:** to open the **End-of-Life programs** list with the following predefined filters:

Hotspot	Filter
(1)	End-of-Life date = Currently in EOL.
(2)	End-of-Life date = In EOL (currently or in 1 year).
(3)	End-of-Life date = All.

Table 14.10: Filters available in the End-of-Life programs list

Last patch installation tasks

*See **Task management** on page **916** for more information about how to modify an existing task.*

Lists recently created patch installation tasks and shows their status. Use the options in this widget to manage patch installation tasks:

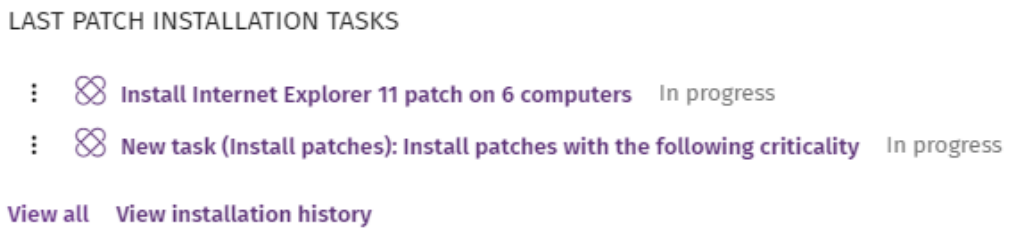


Figure 14.7: Last patch installation tasks panel

- To edit a task, click its name.
- To view all tasks in the **Tasks** page, click **View all**.
- To view details of all patch installation tasks, click **View installation history**.
- Click the context menu next to a task to display a drop-down menu with the following options:
    - **Cancel**: Cancels the task before it starts to install patches on the target computer.
    - **View results**: Shows the results of a task.

Available patches trend

Shows the evolution of the number of patches that are pending installation on the computers on the network, grouped by severity.

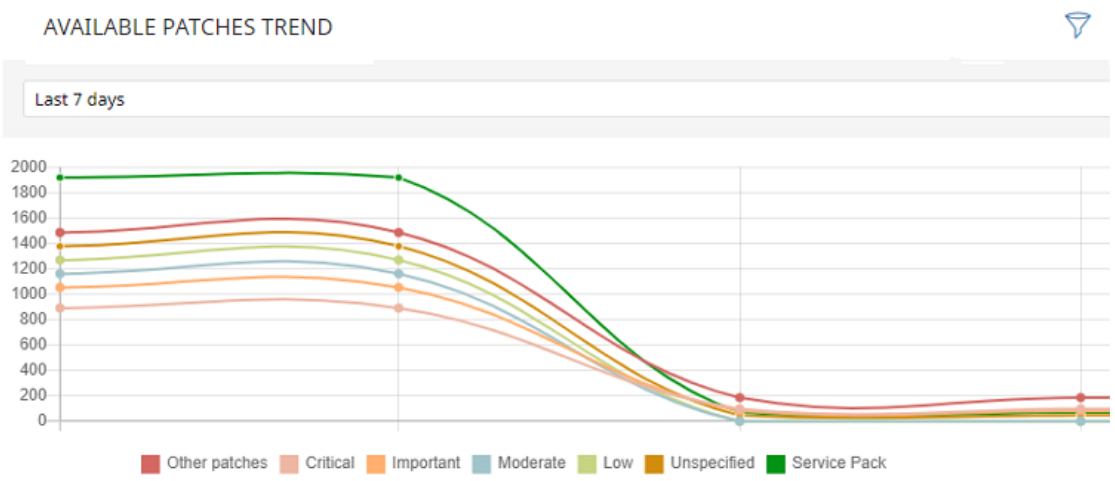


Figure 14.8: Available patches trend graph

Meaning of the data displayed

Data	Description
Security patches - Critical	Number of security patches classified as 'Critical' and pending application.
Security patches - Important	Number of security patches classified as 'Important' and pending application.
Security patches - Low	Number of security patches classified as 'Low' and pending application.
Security patches – Unspecified	Number of security patches that do not have a severity classification and are pending application.
Other patches (non-security related)	Number of patches not related to security that are pending application.
Service Packs	Number of patch and hotfix bundles that are missing from computers. Not applicable for Linux or macOS computers.

Table 14.11: Description of the data displayed in the Availabre patches trend panel

Point to a node on the graph to display a tooltip with the following information:

- Date
- Type
- Number of patches

Lists accessible from the panel

Click the legend items under the graph to open the **Available patches** list filtered by the selected item. Click the graph to open the full **Available patches** list with no filters applied.

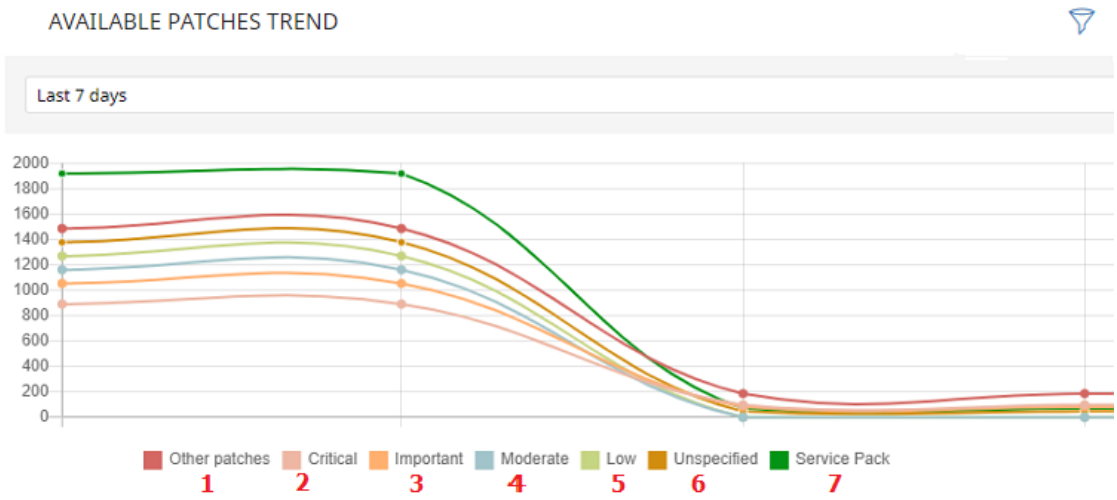


Figure 14.9: Hotspots in the Available patches trend panel

Hotspot	Filter
(1)	Criticality = Other patches (non-security-related).
(2)	Criticality = Critical (security-related).
(3)	Criticality = Important (security-related).
(4)	Criticality = Moderate (security-related).
(5)	Criticality = Low (security-related).
(6)	Criticality = Unspecified (security-related).
(9)	Criticality = Service Pack.

Table 14.12: Filters available in the Available patches trend list

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Definition
Computer type	• Workstation

Filter	Definition
	• Laptop • Server
Platform	Operating system installed on the computer.
Operating system patches	Patches available for Windows operating systems.
App patches	Patches available for apps. For a full list of the apps supported by Cytomic Patch, see **https://info.pandasecurity.com/patchmanagementapp/**. For more information about how to select the apps you want to patch, see **Configuring a patch installation task**.

Table 14.13: Filters available in the Available patches trend widget

Available patches

Shows the number of patches of different types that are available for computers on the network. Numbers in this widget count the same patch multiple times if multiple computers do not have the patch installed.

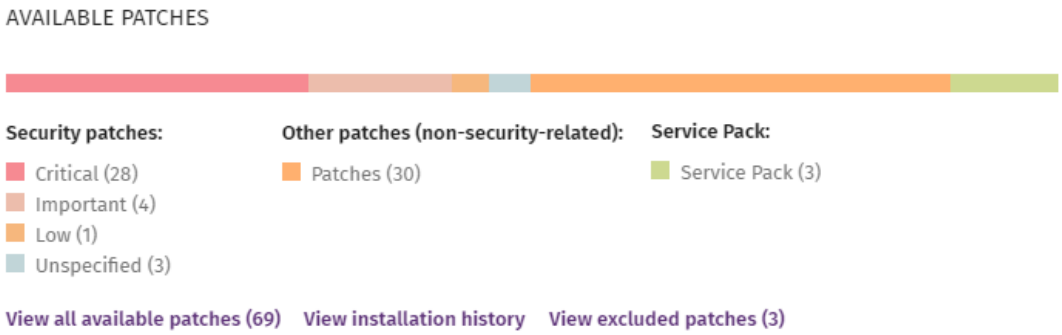


Figure 14.10: Available patches panel

Meaning of the data displayed

Data	Description
Security patches - Critical	Number of security patches classified as 'Critical' and pending application.
Security patches -	Number of security patches classified as 'Important' and pending

Data	Description
Important	application.
Security patches - Low	Number of security patches classified as 'Low' and pending application.
Security patches – Unspecified	Number of security patches that do not have a severity classification and are pending application.
Other patches (non-security related)	Number of patches not related to security that are pending application.
Service Packs	Number of patch and hotfix bundles that are pending application.
View all available patches	Number of patches of all types that are pending application.
View excluded patches	Number of patches excluded from installation.

Table 14.14: Description of the data displayed in the Availabre patches trend panel

Lists accessible from the panel

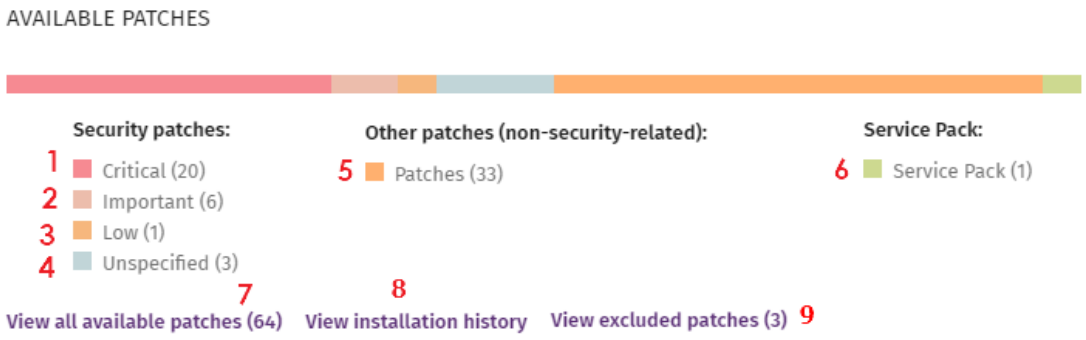


Figure 14.11: Hotspots in the Available patches panel

Click the hotspots shown in **Description of the data displayed in the Availabre patches trend panel** to open the **Available patches** list with the following predefined filters:

Hotspot	List	Filter
(1)	Available patches	Criticality = Critical (security-related).
(2)	Available patches	Criticality = Important (security-related).

Hotspot	List	Filter
(3)	Available patches	Criticality = Low (security-related).
(4)	Available patches	Criticality = Unspecified (security-related).
(5)	Available patches	Criticality = Other patches (non-security-related).
(6)	Available patches	Criticality = Service Pack.
(7)	Available patches	No filter.
(8)	Installation history	No filter.
(9)	Excluded patches	No filter.

Table 14.15: Filters available in the Available patches trend list

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Definition
Computer type	• Workstation • Laptop • Server
Platform	Operating system installed on the computer.
Operating system patches	Patches available for Windows operating systems.
App patches	Patches available for apps. For a full list of the apps supported by Cytomic Patch, see **https://info.pandasecurity.com/patchmanagementapp/**. For more information about how to select the apps you want to patch, see **Configuring a patch installation task**.

Table 14.16: Filters available in the Available patches trend widget

Most available patches for computers

Lists available patches and the number of devices the patch is available for (is in **Pending** or **Pending restart** status).

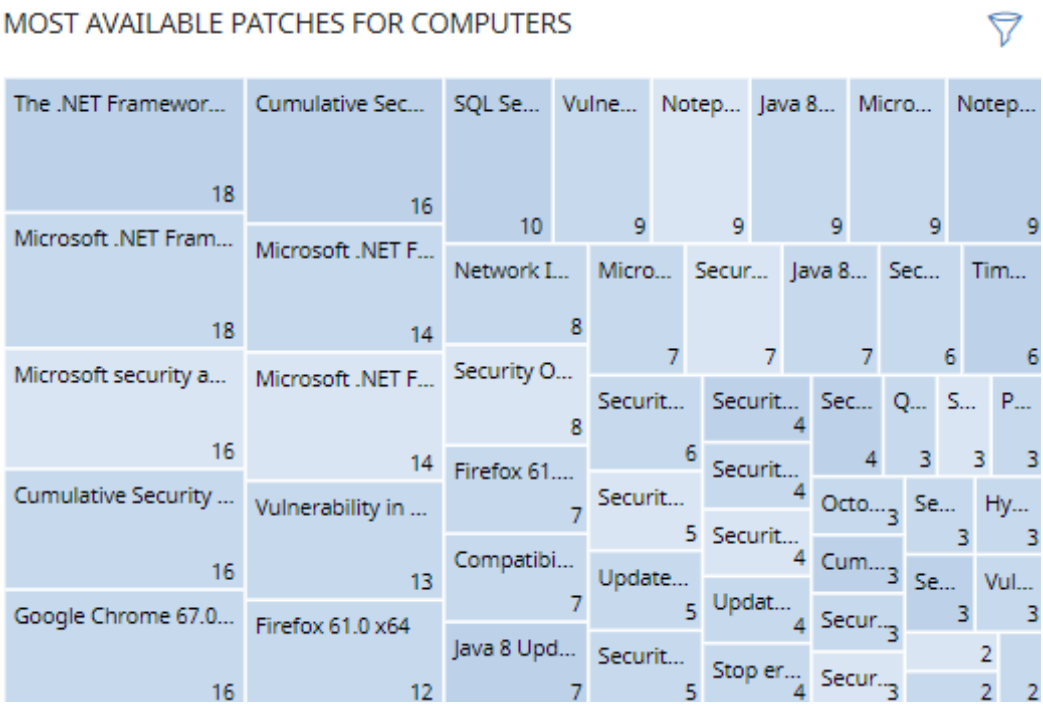


Figure 14.12: Most available patches for computers panel

Meaning of the data displayed

Data	Description
Patch name	Name of the available patch.
Number of computers	Number of computers the patch is available for (is in **Pending** or **Pending restart** status).
View all available patches link	Access to the Available patches by computers full list.

Table 14.17: Description of the data displayed in the Most available patches for computers panel

Point to a box in the widget to see a summary of the patch, including:

- Patch name.
- Number of affected computers.
- Program (or operating system family).
- Criticality.

- Release date.
- CVE (Common Vulnerabilities and Exposures) ID.

Lists accessible from the panel

Click a box in the panel to open the **Available patches** list filtered to the selected patch.

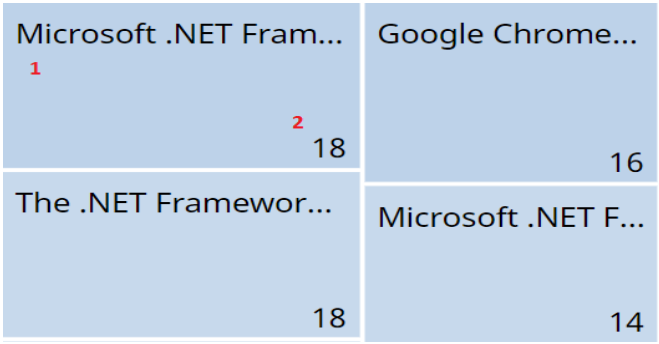


Figure 14.13: Hotspots in the Most available patches for computers panel

Hotspot	Filter
(1)	Patch = Name of the selected patch

Table 14.18: Lists available from the Most available patches for computers panel

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Description	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computer type	Type of device affected by the patch.	• Workstation • Laptop • Server

Filter	Description	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Patch type	Type of software affected by the patch.	• App patches • Operating system patches

Table 14.19: Filters available in the Most available patches for computers panel

Computers with most available patches

Lists the devices that are missing patches, as well as the number of patches the device is missing.

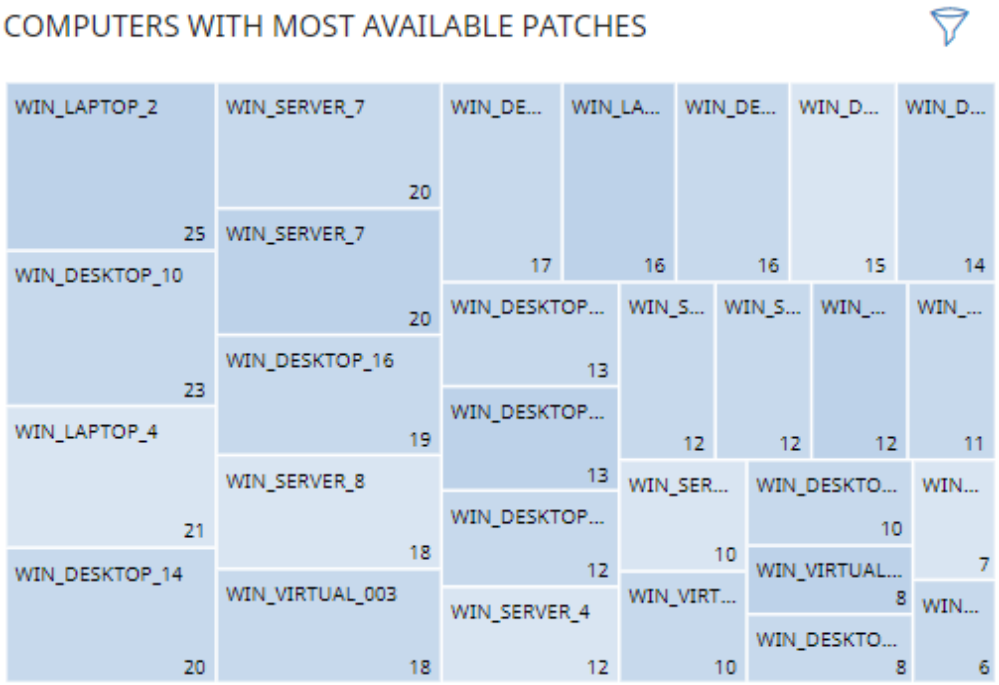


Figure 14.14: Computers with most available patches panel

Meaning of the data displayed

Data	Description
Name	Name of the computer that has patches available.

Data	Description
Number of computers	Number of patches available for the computer.

Table 14.20: Description of the data displayed in the Computers with most available patches panel

Point to a box in the widget to see the following information:

- Computer name.
- Number of patches the computer is missing.

Lists accessible from the panel

Click a box in the panel to open the **Available patches** list filtered to the selected computer.

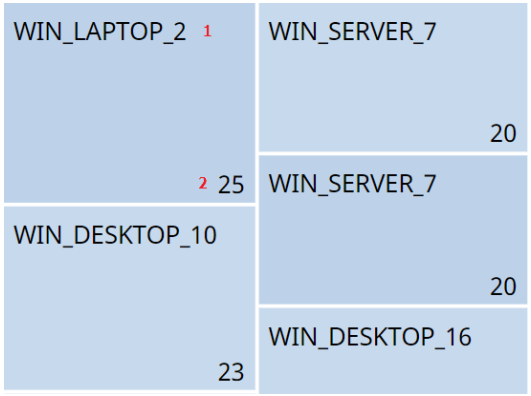


Figure 14.15: Hotspots in the Computers with most available patches panel

Hotspot	Filter
(1)	Computer = Name of the selected computer

Table 14.21: Filters available in the Available patches trend list

Filters available in the widget

Click the icon to see the available filters:

Filter	Description	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related)

Filter	Description	Values
		• Low (security-related) • Unspecified (security-related) • Service Pack
Computer type	Type of device affected by the patch.	• Workstation • Laptop • Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Patch type	Type of software affected by the patch.	• App patches • Windows operating system patches

Table 14.22: Filters available in the Computers with most available patches panel

Programs with most available patches

Lists the programs that are missing most patches, as well as the number of patches the program is missing

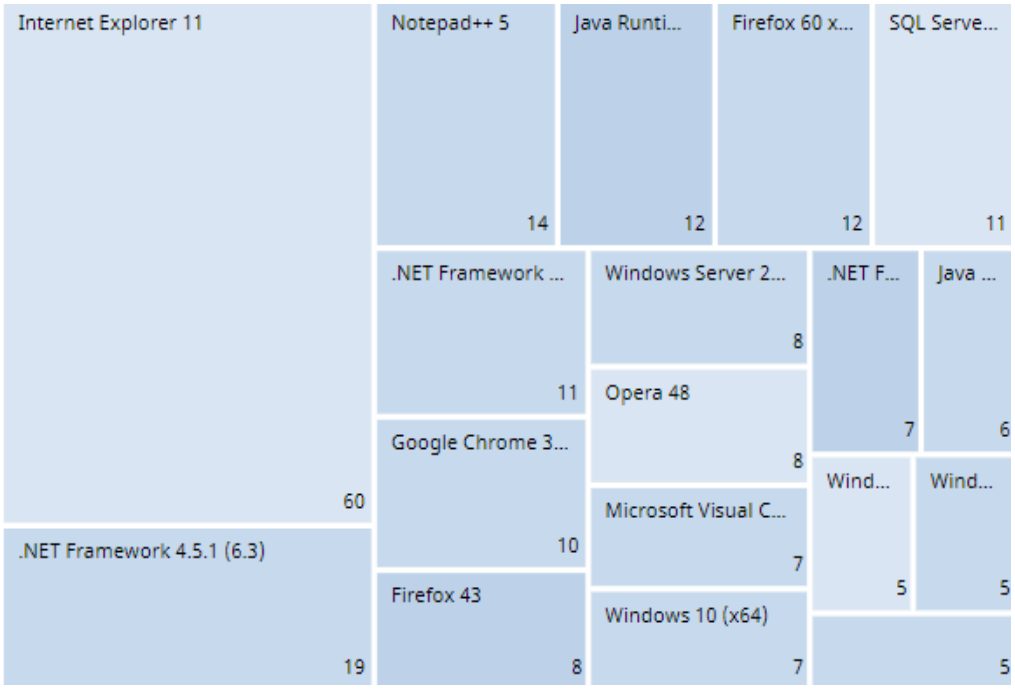


Figure 14.16: Programs with most available patches panel

Meaning of the data displayed

Data	Description
Patch name	Program name.
Number of computers	Number of patches the program is missing.

Table 14.23: Description of the data displayed in the Programs with most available patches panel

Point to a box in the widget to see the following information:

- Program name.
- Number of patches the program is missing.

Lists accessible from the panel

Click a box in the panel to open the **Available patches** list filtered to the selected computer.

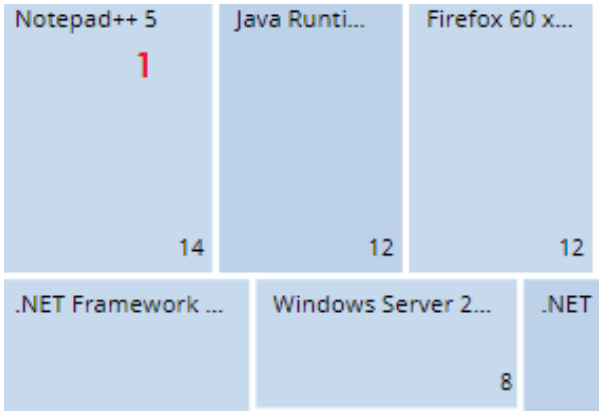


Figure 14.17: Hotspots in the Programs with most available patches panel

Hotspot	Filter
(1)	Program = Name of the selected program

Table 14.24: Filters available in the Available patches trend list

Filters available in the widget

Click the icon to see the available filters:

Filter	Description	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computer type	Type of device affected by the patch.	• Workstation • Laptop • Server
Platform	Operating system installed on the	• All

Filter	Description	Values
	computer.	• Windows • Linux • macOS
Patch type	Type of software affected by the patch.	• App patches • Windows operating system patches

Table 14.25: Filters available in the Programs with most available patches panel

Cytomic Patch module lists

Accessing the lists

There are two ways to access the lists:

- From the top menu, select **Status**. From the side menu, select **Cytomic Patch**. Click the relevant widget.

  Or,

- From the top menu, select **Status**. From the side menu, click the **Add** link. A window opens that shows the available lists.
- From the **Patch management** section, select a list to view the associated template. Edit it and click **Save**. The list is added to the side menu.

You can access the patch installation and uninstallation lists from the **Last patch installation tasks** widget by clicking **View installation history**.

You can access the **Patch installation/uninstallation task results** and **View installed/uninstalled patches** lists from the top menu **Tasks** by clicking **View results** in a patch installation or uninstallation task.

Required permissions

Permissions	Access to lists
No permissions	• Patch management status.
Install, uninstall, and exclude patches	Access to lists and context menus to install and uninstall patches:

Permissions	Access to lists
	• Available patches. • Installation history. • End-of-Life programs. • Excluded patches. • Patch installation/uninstallation task results. • View installed/uninstalled patches.
View available patches	Read-only access to lists: • Available patches. • Installation history. • End-of-Life programs. • Excluded patches. • Patch installation/uninstallation task results. • View installed/uninstalled patches. • Available patches trend. • Most available patches for computers. • Computers with most available patches. • Programs with most available patches.

Table 14.26: Permissions required to access the Patch Management lists

Patch management status

This list shows all computers on the network that are compatible with Cytomic Patch (with filters that enable you to identify workstations and servers that are not using the service due to the reasons shown in the associated panel).

Field	Comment	Values
Computer	Computer name.	Character string
Computer status	Agent reinstallation: •  Reinstalling the agent. •  Agent reinstallation error.	Icon

Field	Comment	Values
	Protection reinstallation: •  Reinstalling the protection. •  Protection reinstallation error. •  Pending restart. Computer isolation status: •  Computer in the process of being isolated. •  Isolated computer. •  Computer in the process of stopping being isolated. "RDP attack containment" mode: •  Computer in "RDP attack containment" mode. •  Ending "RDP attack containment" mode. Patch installation •  Do not install patches •  Designate as test computers and install patches	
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Patch management	Module status.	•  Enabled •  Disabled •  Installation error (failure reason) •  No license • — No

Field	Comment	Values
		information • Error
Last checked	Date when Cytomic Patch last queried the cloud to check whether new patches had been published.	Date
Last connection	Date when the Advanced EPDR status was last sent to the Cytomic cloud.	Date

Table 14.27: Fields in the Patch Management Status list

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Patch installation	Patch installation option applied to the computer: • Patch installation enabled: The computer has Cytomic Patch enabled. Cytomic Patch installs patches on the computer. • Test computer for patch installation: The computer has Cytomic Patch enabled and is	Enumeration

Field	Comment	Values
	designated as a test computer for patch installation. • Patch installation disabled: The computer has Cytomic Patch disabled. Cytomic Patch does not install patches on the computer.	
Agent version		Character string
Installation date	Date when the Cytomic Patch module was successfully installed on the computer.	Date
Last connection date	Date when the agent last connected to the Cytomic cloud.	Date
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Updated protection	Indicates whether the protection module installed on the computer is updated to the latest version or not.	Boolean
Protection version	Internal version of the protection module.	Character string
Last update on	Date the signature file was last updated.	Date
Patch management status.	Module status.	• Enabled • Disabled • Error installing • No license • No information • Error

Field	Comment	Values
Requires restart	The computer requires a reboot to finish installing or uninstalling one or more downloaded patches.	Boolean
Last checked	Date when Cytomic Patch last queried the cloud to check whether new patches had been published.	Date
Isolation status	Indicates whether the computer is isolated or can communicate normally with other computers on the network.	• Isolated • Not isolated
Installation error date	Date of the unsuccessful attempt to install Cytomic Patch.	Date
Installation error	Reason for the installation error.	• Download error • Execution error

Table 14.28: Fields in the Patch Management Status exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Computer type	Type of device.	• Workstation • Laptop • Server
Last checked	Date when Cytomic Patch last queried the cloud to check whether new patches had been published.	• All • More than 3 days ago • More than 7 days ago • More than 30 days

Field	Comment	Values
		ago
Last connection	Date when the agent last connected to the Cytomic cloud.	Date
Pending restart to complete patch installation or uninstallation	The computer requires a reboot to finish installing or uninstalling one or more patches.	Boolean
Patch installation	Patch installation option.	• Patch installation enabled • Test computer for patch installation • Patch installation disabled
Patch management status.	Module status.	• Enabled • Disabled • Error • Error installing • No license • No information

Table 14.29: Filters available in the Patch Management Status list

Computer details page

Click a row in the list to open the computer details page. For more information, see **Computer details** on page **252**.

Available patches

This list shows all missing patches on the network computers and information about patches in the process of installation. Each line in the list corresponds to a patch/computer pair.

Field	Comment	Values
Computer	Name of the computer with outdated software and patch installation option assigned to the computer in the Cytomic Patch settings: • Do not install patches • Designate as test computers and install patches	Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Version	Version number of the outdated program.	Numeric value
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Release date	Date when the patch was released for download and application.	Date
Criticality	Update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified

Field	Comment	Values
		(security-related) • Service Pack
Installation	Indicates the patch installation status: • **Pending**: The patch is available for the computer but has not been installed yet. • **Requires manual download**: The patch must be manually downloaded and copied to a cache computer by the administrator. For more information, see **Download patches manually**. • **Pending (manually downloaded)**: The patch was downloaded manually and is already included in the patch repository. For more information, see **Download patches manually**. • **Pending restart**: The patch was installed but the computer was not restarted. Some patches might not be applied until the computer is restarted.	Enumeration
Context menu	Shows an action menu: • **Install**: Create a quick task to immediately install the patch on the computer. • **Schedule installation**: Create a scheduled task to install the patch on the computer. • **Exclude**: Select the computers for which you want to exclude the patch. • **Isolate computer**: Isolate the computer from the network. Not available for Linux computers. • **View all available patches for the computer**: Shows all available patches for the computer that have not been installed yet. • **View which computers have the patch available**: Shows all computers that have the patch available for installation.	Enumeration

Table 14.30: Fields in the Available Patches list

Fields displayed in the exported file

Use the context menu to export the data. The export file can include all data in the list of available patches or a smaller version that shows the trend of the number of available patches in the last 7 days, the last month, or the last year.

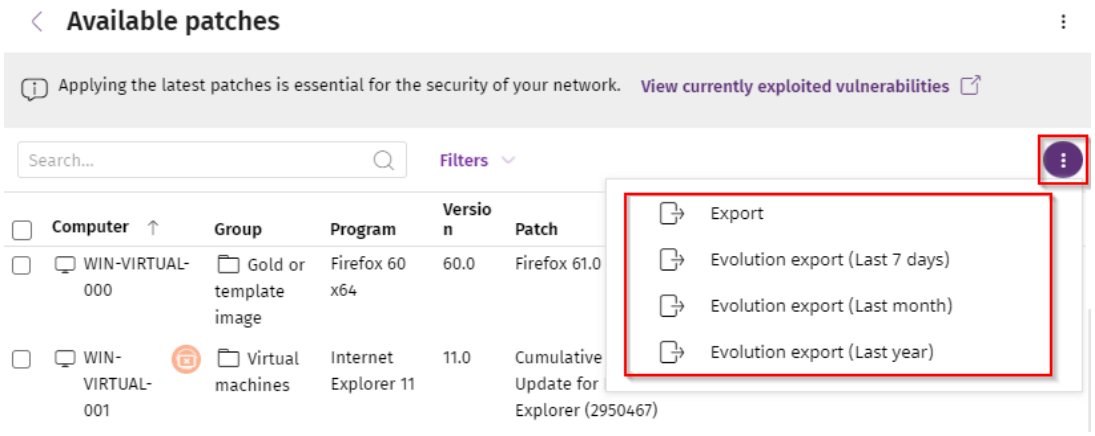


Figure 14.18: Context menu for data export

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer with outdated software.	Character string
IP address	The computer primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description		Character string
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
Group	Folder in the Advanced EPDR folder tree that the	Character string

Field	Comment	Values
	computer belongs to.	
Patch installation	Patch installation option applied to the computer.	• Patch installation enabled • Test computer for patch installation • Patch installation disabled
Vendor	The company that created the outdated program.	Character string
Product family	Name of the product with patches pending installation or a reboot.	Character string
Program version	Version number of the outdated program.	Numeric value
Program	Name of the outdated program or operating system version with missing patches.	Character string
Version	Version number of the outdated program.	Numeric value
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Criticality	Update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related)

Field	Comment	Values
		• Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Last seen	Date when the computer was last discovered.	Date
Is downloadable	Indicates whether the patch is available for download or requires an additional support contract with the software vendor to access it.	Boolean
Download size (KB)	Patch size in compressed format. Applying the patch or update might require more space on the target computer storage media than indicated in this field.	Numeric value
Status	Indicates the patch installation status: • **Pending**: The patch is available for the computer but has not been installed yet. • **Pending (manually downloaded)**: The patch was downloaded manually and is already	Enumeration

Field	Comment	Values
	included in the patch repository. For more information, see **Download patches manually** . • **Requires manual download**: The patch must be manually downloaded and copied to a cache computer by the administrator. For more information, see **Download patches manually**.	
File name	Name of the file that contains the patch.	Character string
Download URL	HTTP resource in the software vendor infrastructure to download the patch.	Character string

Table 14.31: Fields in the Available Patches exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Patch release	Date when the patch was released and made available for download.	• All • Less than 7 days ago • Less than 14 days ago • Less than 1 month ago • Less than 2 months ago • More than 7 days ago • More than 14

Field	Comment	Values
		days ago • More than 1 month ago • More than 2 months ago
Computer type	Type of device.	• Workstation • Laptop • Server
Patch type	Type of patch.	• App patches • Operating system patches
Search computer	Computer name.	Character string
Computer	Name of the computer with outdated software.	Character string
Program	Name of the outdated program or operating system version with missing patches.	Character string
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
CVE	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
Program, family, or vendor	The search applies to the selected program, product family, or company.	Character string
Patch installation	Patch installation option.	• Patch installation enabled • Test computer for patch installation • Patch installation

Field	Comment	Values
		disabled
Criticality	Indicates the update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Installation	Shows patches that are in the process of installation, filtering them by the installation stage they are in.	• Pending • Requires manual download • Pending (manually downloaded) • Pending restart
Show non-downloadable patches	Shows patches that cannot be directly downloaded by Cytomic Patch because there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.).	Boolean

Table 14.32: Filters available in the Available Patches list

Detected patch page

Click a row in the list. The **Detected patch** page opens and shows details of the patch. This data might vary depending on the operating system installed on the computer.

This page can provide this content:

- Information about the available patch and the **Install patch** button.
- Information about the patch in the process of installation. The text **Pending restart** appears next to the **Install patch** button.

Click the **Install patch** button. A dialog box opens for you to select the recipients of the patch installation task:

- **Install on the current computer only**: The task is performed on the computer selected in the list.
- **Install on all computers in the selected filter**: Select a filter from the filter tree shown. The patch is installed on all computers in the selected filter.
- **Install on all computers**: The patch is installed on all computers on the network.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the outdated program or operating system version with missing patches.	Character string
Program version	Version number of the outdated program.	Character string
Family	Name of the product with patches pending installation or a reboot.	Character string
Vendor	The company that created the outdated program.	Character string
Criticality	Indicates the update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-

Field	Comment	Values
		related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
Computer	Name of the computer with outdated software.	Character string
Installation status	Indicates whether the patch is already included in the repository that contains the patches to be applied to computers or must be manually downloaded and added to the patch repository by the administrator.	• Pending • Requires manual download • Pending (manually downloaded) • Pending restart
Release date	Date when the patch was released for download and application.	Date
Download size	Patch size in compressed format. Applying the patch or update might require more space on the target computer storage media than indicated in this field.	Numeric value
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Download URL	URL for downloading the patch individually.	Character string
File name	Name of the file that contains the patch.	Character string

Field	Comment	Values
Description	Information about the impact the vulnerability could have on computers.	Character string

Table 14.33: Fields on the Detected Patch page

Available patches by computers

This list shows available patches and the number of computers each patch is available for.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the outdated program or operating system version with missing patches.	Character string
Version	Version number of the outdated program.	Numeric value
Release date	Date when the patch was released for download and application.	Date
Criticality	Update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-

Field	Comment	Values
		related) • Service Pack
Computers	Number of computers the patch is available for.	Numeric value
Context menu	**View which computers have the patch available**: Shows all computers that have the patch available for installation.	

Table 14.34: Fields in the Available Patches by Computers list

Fields displayed in the exported file

Use the context menu to export the data. The export file can include all data in the list of available patches or a smaller version that shows the trend of the number of available patches in the last 7 days, the last month, or the last year.

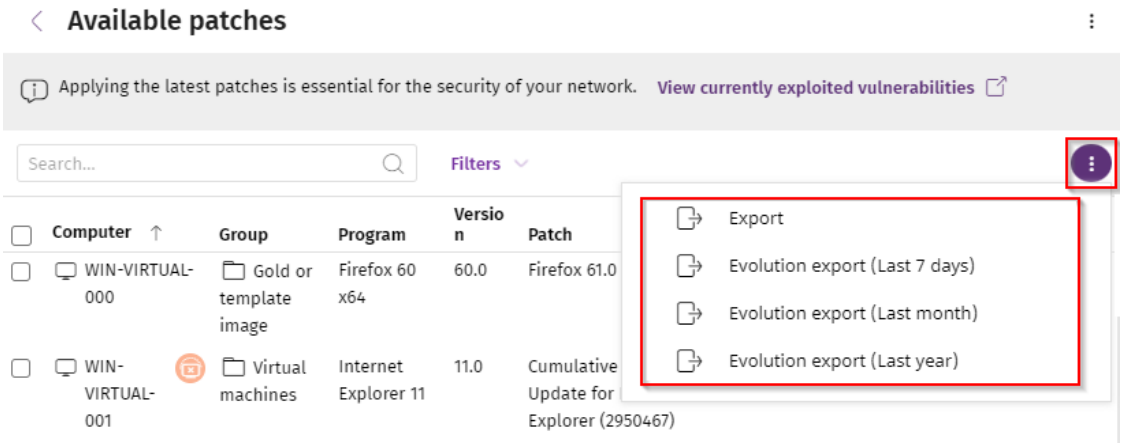


Figure 14.19: Context menu for data export

Field	Comment	Values
Vendor	The company that created the outdated program.	Character string
Product family	Name of the product with patches pending installation or a reboot.	Character string
Program version	Version number of the outdated program.	Numeric value
Program	Name of the out-of-date program or operating system version with missing	Character string

Field	Comment	Values
	patches.	
Version	Version number of the outdated program.	Numeric value
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Criticality	Update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Computers	Number of computers the patch is available for.	Numeric value

Field	Comment	Values
Platform	Operating system installed on the computer.	• Windows • macOS • Linux

Table 14.35: Fields in the Available Patches by Computers exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Computer type	Type of device.	• Workstation • Laptop • Server
Patch type	Type of patch.	• App patches • Operating system patches
Search computer	Computer name.	Character string
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
CVE	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
Select a program	The search applies to the selected program, product family, or company.	Character string

Field	Comment	Values
version, family, or vendor		
Criticality	Indicates the update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Show non-downloadable patches	Shows patches that cannot be directly downloaded by Cytomic Patch because there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.).	Boolean

Table 14.36: Filters available in the Available Patches by Computers list

Detected patch page

Click a row in the list. The **Detected patch** page opens and shows details of the patch. This data might vary depending on the operating system installed on the computer. See **Detected patch page**.

Installation history

This list shows the operations performed by Cytomic Patch on the computers on the network in the specified time period.

Field	Comment	Values
Date	Date the operation was	Date

Field	Comment	Values
	logged.	
Computer	Computer name.	Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Program	Program name or operating system version.	Character string
Version	Program or operating system version.	Character string
Patch	Patch name.	Character string
Criticality	Severity rating of the patch.	• Other patches • Critical • Important • Moderate • Low • Unspecified • Service Pack
Installation	Status of the logged operation.	• Installed • Requires restart • The patch is no longer required • Uninstalled (requires restart) • Error
Context menu ⋮	Shows a drop-down menu with options.	• **View task**: Shows the settings of the task associated with the logged operation. • **View patches installed on the computer**: Shows all patches installed on the selected computer.

Field	Comment	Values
		• **View computers with the patch installed**: Shows all computers that have the selected patch installed.

Table 14.37: Fields in the Installation History list

Fields displayed in the exported file

Use the context menu to export the data. You can download a detailed file that includes all data in the list or a reduced version. In either case, the file contains information about the patches installed in the selected time period.

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
IP address	The computer primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description		Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Date	Date of the logged operation.	Date
Program	Program name or operating system version.	Character string

Field	Comment	Values
Version	Program or operating system version.	Character string
Patch	Name of the installed patch.	Character string
Criticality	Severity rating of the patch.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Installation	Indicates whether the patch is already included in the repository that contains the patches to be applied to computers or must be manually downloaded and added to the patch repository by the administrator.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled

Field	Comment	Values
Installation error	The Cytomic Patch module did not install correctly.	• **Unable to download**: Installer not available • **Unable to download**: The file is corrupted • **Not enough disk space** • Installation error • Download error
Download URL	URL for downloading the patch individually.	Character string
Result code	Operation result code. See the vendor documentation for information about result codes.	Numeric value
Task name	Name of the patch installation task. This column appears only in the extended export.	Character string
Task launch date	Date when the Cytomic Patch task associated with the computer was scheduled to run. This column appears only in the extended export.	Date
Task start date	Date when the Cytomic Patch task associated with the computer started to run. This column appears only in the extended export.	Date
Task end date	Date when the Cytomic Patch task associated with the computer finished to run. This column appears only in the extended export.	Date

Table 14.38: Fields in the Installation History exported file

Filter tool

Field	Comment	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Search computer	Computer name.	Character string
Date	Time period in which the patches were installed.	• Last 24 hours • Last 7 days • Last month • Custom range
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Criticality	Severity rating of the patch.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related)

Field	Comment	Values
		• Service Pack
Installation	Status of the logged operation.	• Installed • Requires restart • The patch is no longer required • Uninstalled (requires restart) • Error • Download error • Installation error
Program	Program name or operating system version.	Character string
Patch	Name of the installed patch.	Character string
Installation Attempts	Shows all failed patch installation attempts or only the latest attempt.	• Show only the latest attempt • Show all attempts
CVE	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string

Table 14.39: Filters available in the Installation History list

Installed patch page

Click a row in the list. The **Installed patch** page opens and shows details of the logged operation. This data might vary depending on the operating system installed on the computer.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string

Field	Comment	Values
Program	Name of the out-of-date program or operating system version.	Character string
Criticality	Indicates the update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
Computer	Computer name.	Character string
Installation date	Date the operation was logged.	Date
Result	Status of the logged operation.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled

Field	Comment	Values
		• Installation error • Download error
Release date	Date when the patch was released for download and application.	Date
Download size	Patch size in compressed format. Applying the patch or update might require more space on the target computer storage media than indicated in this field.	Numeric value
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Description	Notes provided by the software vendor about the effects of applying the patch, special conditions, and resolved vulnerabilities.	Character string

Table 14.40: Fields on the Installed Patch page

End-of-Life programs

This list shows programs that are no longer supported by the relevant vendor. These programs are particularly vulnerable to malware and other security threats.

Field	Comment	Values
Computer	Name of the computer with EOL software.	Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Program	EOL program name.	Character string
Version	EOL program version.	Character string
EOL	Date when the program reached its end of life.	Date (in red if the program reached its end of life)

Table 14.41: Fields in the End-of-Life Programs list

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
IP address	The computer primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Program	EOL program name.	Character string
Version	EOL program version.	Character string
EOL	Date when the program reached its end of life.	Date
Last seen	Date when the computer was last discovered.	Date

Table 14.42: Fields in the End-of-Life Programs exported file

Filter tool

Field	Comment	Values
Search computer	Computer name.	Character string

Field	Comment	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
End-of-Life date	Date when the program will reach its EOL.	• All • Currently in End of Life • In End of Life (currently or in 1 year)

Table 14.43: Filters available in the End-of-Life Programs list

Program details page

Click a row in the list. The **Program details** page opens.

Field	Comment	Values
Program	Name of the program or operating system version that received the patch.	Character string
Family	Bundle, suite, or program group the software belongs to.	Character string
Publisher/Company	Company that designed or published the program.	Character string
Version	Program version.	Character string
EOL	Date when the program reached its end of life.	Date

Table 14.44: Fields on the Program Details page

Excluded patches

This list shows patches that you marked as excluded, preventing them from being installed on the computers on the organization network. The list shows a line for each computer-excluded patch pair, except for patches excluded for all computers on the network, for which a single line appears.

Field	Comment	Values
Computer	The content of this field varies depending on the target of the exclusion: If the patch was excluded for a single computer, the field shows the computer name. If the patch was excluded for all computers in the account, the text "(All)" is shown.	Character string
Group	Folder in the Advanced EPDR group tree that the computer belongs to.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Version	Version of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Criticality	Severity rating of the patch.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack

Field	Comment	Values
Excluded by	Management console user account who excluded the patch.	Character string
Excluded since	Date the patch was excluded.	Character string

Table 14.45: Fields in the Excluded Patches list

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	The content of this field varies depending on the target of the exclusion: If the patch was excluded for a single computer, the field shows the computer name. If the patch was excluded for all computers in the account, the text "(All)" is shown.	Character string
IP address	The computer primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description	The computer description assigned by the network administrator.	Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string

Field	Comment	Values
Program	Name of the program the excluded patch belongs to.	Character string
Version	Version of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Criticality	Severity rating of the patch.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date

Field	Comment	Values
Download size (KB)	Patch size in compressed format. Applying the patch or update might require more space on the target computer storage media than indicated in this field.	Numeric value
Excluded by	Management console user account who excluded the patch.	Character string
Excluded since	Date the patch was excluded.	Character string

Table 14.46: Fields in the Excluded Patches exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer for which patches were excluded.	Character string
Program	Name of the program the excluded patch belongs to.	Character string
Patch	Name of the excluded patch.	Character string
Show non-downloadable patches	Shows patches that cannot be directly downloaded by Cytomic Patch because there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.).	Boolean

Field	Comment	Values
CVEs	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
Criticality	Severity rating of the patch.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack

Table 14.47: Filters available in the Excluded Patches list

Excluded patch page

Click a row in the list. The **Excluded patch** page opens and shows details of the patch excluded from installation tasks. This data might vary depending on the operating system installed on the computer.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the outdated program or operating system version with missing patches.	Character string

Field	Comment	Values
Criticality	Indicates the update severity rating and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) Service Pack
CVEs	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
Computer	Name of the computer with outdated software.	Character string
Excluded by	Management console user account who excluded the patch.	Character string
Excluded since	Date and time the patch was excluded.	Numeric value
Release date	Date when the patch was released for download and application.	Date
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Description	Notes provided by the software vendor about the effects of applying the patch, special conditions, and resolved vulnerabilities.	Character string

Table 14.48: Fields on the Excluded Patch page

Patch installation/uninstallation task results

This list shows the results of the patch installation or uninstallation tasks performed on the computers on your network.

Field	Description	Values
Computer	Name of the computer the patch was installed/uninstalled from.	Character string
Group	Advanced EPDR group the computer belongs to.	Character string
Status	Task status.	• Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Patches installed/uninstalled	Number of patches installed/uninstalled.	Character string.
Start date	Date the installation task started.	Date
End date	Date the installation task ended.	Date

Table 14.49: Fields in the Installation/Uninstallation Task Results list

Filter tool

Field	Description	Values
Status	Installation/uninstallation task status.	• Pending • In progress

Field	Description	Values
		• Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Applied/Uninstalled patches	Computers on which patches were installed/uninstalled.	• All • No patches installed/uninstalled • With patches installed/uninstalled

Table 14.50: Filters available in the Patch Installation/Uninstallation Task Results list

View installed/uninstalled patches

This list shows the patches installed/uninstalled from computers and other additional information.

Field	Description	Values
Computer	Name of the computer the patch was installed/uninstalled from.	Character string
Group	Advanced EPDR group the computer belongs to.	Character string
Program	Patched program.	Character string
Version	Program version.	Character string
Patch	Installed/uninstalled patch.	Character string
Criticality	Severity rating of the installed/uninstalled patch.	• Other patches (non-security related) • Critical (security-

Field	Description	Values
		related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Result	Indicates whether the task was completed successfully or failed.	• Installed • Requires restart • Error • The patch is no longer required • Uninstalled
Date	Date the task ran.	Date

Table 14.51: Fields in the View Installed/Uninstalled Patches list

Endpoint Access Enforcement settings

Endpoint Access Enforcement (EAE) monitors inbound connections to computers on the corporate network, allowing or blocking them based on the security status of the connecting computer.

When you configure an Endpoint Access Enforcement policy, you must specify which characteristics of the connecting computer pose a risk to the target computer. These characteristics have to do with the connecting computer management model, the status of the security software installed on this computer, and its overall risk level.

Additionally, you must specify the protocols you want to monitor in inbound connections, and configure the action you want the security software to take on these connections (allow or block).

For more information about the Endpoint Access Enforcement module, see:

***Creating and managing settings profiles** on page **294**: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*

***Accessing, controlling, and monitoring the management console** on page **61**: Managing user accounts and assigning permissions.*

***Managing lists** on page **48**: Information about how to manage lists.*

Chapter contents

Endpoint Access Enforcement settings

Minimum requirements

- **Advanced EPDR security software**: The computer must have Advanced EPDR v4.40 or higher installed.
- **Operating system installed on the computer**: Endpoint Access Enforcement is compatible with Windows computers.

> *Computers with a macOS or Linux operating system and Advanced EPDR v4.40 or higher installed report the status of the security software to Windows computers that evaluate their risk level. See* ***Endpoint Access Enforcement operating mode****.*

- **Open ports on the computer**: The Advanced EPDR agent requires that port 33000 be open to communicate with other computers.

Accessing the settings

- From the top menu, select **Settings**. From the side menu, select **Endpoint Access Enforcement**.
- Click **Add**. The **Add settings** page opens.

Required permissions

Permission	Access type
Configure Endpoint Access Enforcement	Create, edit, delete, copy, or assign Endpoint Access Enforcement settings profiles.
View Endpoint Access Enforcement settings	View Endpoint Access Enforcement settings profiles.

Table 14.52: Permissions required to access the Endpoint Access Enforcement settings

Endpoint Access Enforcement settings options

To configure an Endpoint Access Enforcement policy:

- Enter a name and description for the settings profile.
- Click **Save**.
- From the list of profiles, select the profile you created. The **Edit settings** page opens.
- To select the computers you want to assign the settings to, click the **Recipients (No recipients selected)** link. To add computers individually, click  . To remove them, click  .
- On the **Edit settings** page, enable the **Endpoint Access Enforcement** toggle.
- To specify the characteristics that define the security status of the connecting computer, see **Security characteristics of connecting computers**.
- To configure the action Endpoint Access Enforcement must take when it detects a connection from a computer at risk, see **Endpoint Access Enforcement operating mode**.
- To configure the inbound connection protocols you want to monitor, see **Monitoring inbound connection protocols**.

Security characteristics of connecting computers

Select which conditions of connecting computers can pose a risk to the target computer:

- **Unmanaged/Unavailable**: The connecting computer:
  - Does not have a supported security software installed. See **Minimum requirements**.
  - Does not have the minimum required version of Advanced EPDR installed. See **Minimum requirements**. To update the agent, the security software, and the security software signature file, see **Product updates and upgrades** on page **203**.
  - Is not available or a firewall prevents connecting to it.
- **Managed by another account**: The connecting computer is managed by an account other than the account that manages the target computer.
- **Protection not enabled**: The connecting computer security software is up to date but not enabled. It poses a risk to the target computer. See **Minimum requirements**.
- **Risk level greater than or equal to Medium, High, or Critical**: The overall risk level for the connecting computer is greater than or equal to Medium, High, or Critical. See **Risk assessment** on page **725**.**Risk assessment** on page **725**

Endpoint Access Enforcement operating mode

From the **Action to be taken on inbound connections from computers at risk** drop-down menu, select the action Endpoint Access Enforcement must take on inbound connections detected on target computers:

- **Audit**: Endpoint Access Enforcement reports inbound connections from computers at risk. See **Endpoint Access Enforcement module lists**.

These connections are allowed by the security software and appear in red in the **Connection Map**.

- **Block**: Endpoint Access Enforcement detects and blocks connections from computers at risk.

  These connections appear in gray in the **Connection Map**.

  For a pop-up notification to appear on the user computer when a connection is blocked, enable the **Show an alert when Endpoint Access Enforcement blocks a connection** toggle. You can type the message you want to appear in the pop-up notification. Click **Save**.

Monitoring inbound connection protocols

By default, Endpoint Access Enforcement monitors inbound connections for SMB (a protocol that enables users to communicate with remote computers and servers to share, open, or edit files) and RDP (a protocol that enables users to remotely share a computer desktop) traffic.

To configure monitoring of the SMB and RDP protocols:

- Select the checkbox for the protocol you want to configure. Click  . The **Configure Protocol** dialog box opens.
- To add ports to the settings, type them in the text box. Press **Enter**.

By default, Endpoint Access Enforcement applies protocol monitoring to workstations. If you want to apply it to servers as well, disable the toggle.

- To allow connections from specific IP addresses, type them in the text box. Press **Enter**.
- Click **Save**.

To add protocols other than SMB and RDP:

- On the **Add settings** page, click  . The **Configure Protocol** dialog box opens.
- From the **Protocol** drop-down menu, select the protocol you want to monitor. If the protocol is not in the list, select **Custom**.
- Follow the steps in the previous section.
- Click **Save**.

The settings profile you create appears at the top of the list of Endpoint Access Enforcement settings profiles.

Connection Map

The Connection Map is a visual representation of connections between computers on the network that meet the conditions you configure in the Endpoint Access Enforcement settings.

> *For more information about Endpoint Access Enforcement, see* ***Endpoint Access Enforcement settings****.*

Connection Map structure

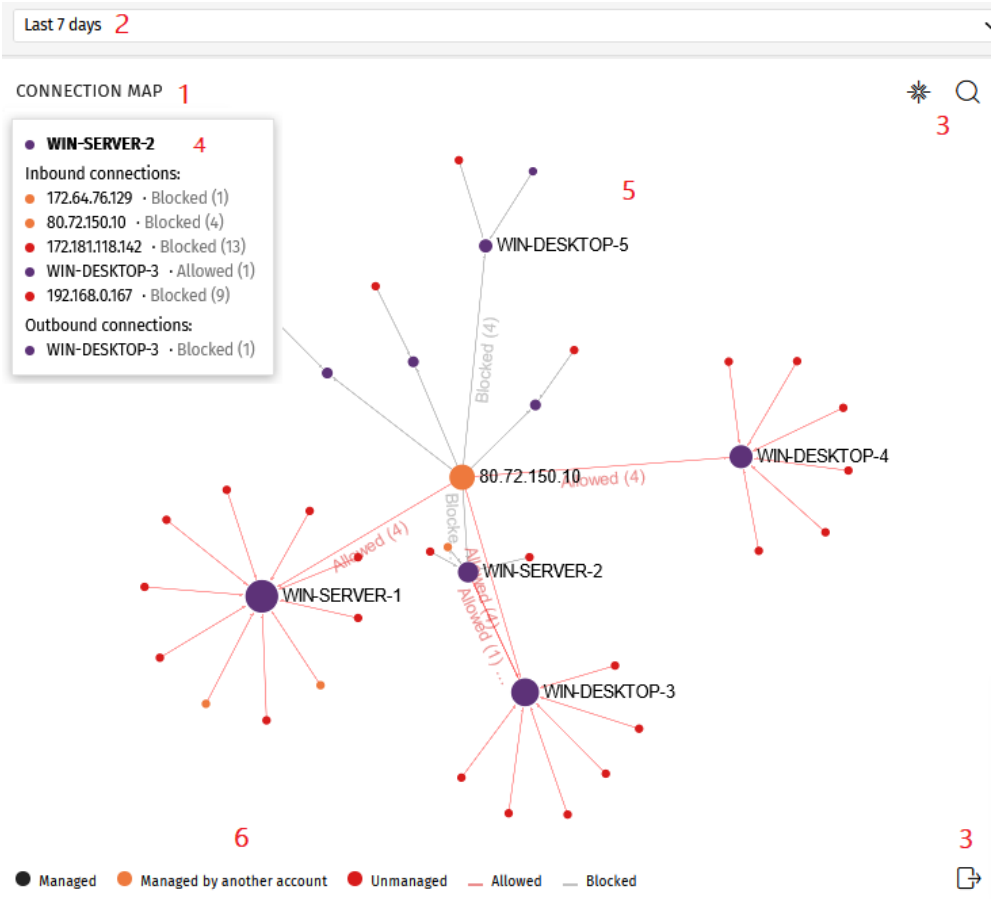


Figure 14.20: Connection Map

- **Widget name (1).**
- **Time selector (2)**: From the drop-down menu, select the time period for the data you want to see. See **Connection Map settings**.
- **Tools (3)**:

- To find a computer or an IP address, click  . See **Connection Map settings**.
- To save the Connection Map, click  . See **Connection Map settings**.

- **Information panel (4)**: Point to a node. An information panel appears and shows information about connections for the node.
- **Graph (5)**: A graphical representation that uses nodes and arrows to show connections between computers and connection direction. It also shows the actions that Endpoint Access Enforcement took on connections, and the number of connections affected by the action. See **Node and connection features**.
- **Legend (6)**: A color system that shows managed and unmanaged computers, and lines for allowed and blocked connections.

Connection Map controls

- **Zoom**: By default, the widget has a sufficient level of zoom to make sure you can see all nodes without having to move the graph. You can use your mouse wheel to zoom in and out on the Connection Map. Click  to reset the zoom level.
- **Filter by group**: Depending on the number of computers or computer groups involved in connections, a large amount of data can be shown in the graph. To limit the amount of generated data, click the **Filter by group** icon  next to the web notification icon  . For more information, see **Filtering results by groups** on page **227**.
- **Move the graph**: To move the graph, click and drag it in the appropriate direction. Click  to move the graph back to its initial position.
- **Access the Connections identified by Endpoint Access Enforcement list**: Click a computer node. The **Connections identified by Endpoint Access Enforcement** list opens filtered by the computer name or IP address.

> *See **Endpoint Access Enforcement module lists** and **Node and connection features**.*

Connection Map settings

- **Time range**. Select the time period for the data you want to see:
  - **Last 24 hours**
  - **Last 7 days**

- **Last month**
- **Last year**

- **Search tool**. Click  . From the drop-down menu, select the name or IP address of the computer you want to find in the graph.
- **Save graph.** You can show or hide information layers in the graph, and save the graph. Click  . A drop-down menu opens and shows these options:
  - **Computers**: Hides or shows graph nodes.
  - **Connections**: Hides or shows connection lines.
  - **Computers labels**: Hides or shows node labels.
  - **Connections labels**: Hides or shows connection line labels and the number of connections for each line.
  - Click **Export**.

Node and connection features

The Connection Map represents computers and connections through nodes, lines, and associated labels. See **Connection Map**.

Node colors

Nodes show information through their associated icons:

- **Purple**: A managed computer.
- **Orange**: A computer managed by another account.
- **Red**: An unmanaged computer.

Node labels

Based on the type of computer, the node label shows the computer name or IP address.

- **Computer managed by the same account as the other end of the connection**: The label shows the name of the selected computer.
- **Computer managed by a different account than the account that manages the other end of the connection**: The label shows the IP address of the selected computer.
- **Unmanaged computer**: The label shows the IP address of the selected computer.

*See **Endpoint Access Enforcement settings options**.*

Node size

- **Managed computer (purple node)**: The size of the node depends on the number of inbound and outbound connections.
- **Computer managed by another account (orange node)**: The size of the node depends on the number of inbound and outbound connections.
- **Unmanaged computer (red node)**: The size of the node depends on the number of outbound connections.

Connection lines

Connections between nodes are represented through lines and numbers.

Line direction

- **Unidirectional line**: The number on the line indicates all allowed or blocked connections between two nodes for the selected period.

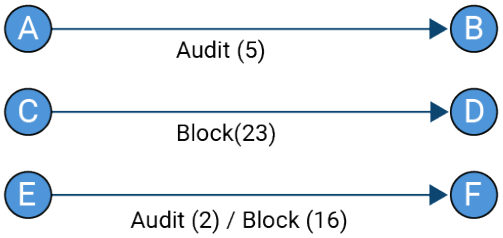


Figure 14.21: Unidirectional connection line

- **Bidirectional line**: The number on the line indicates the total sum of allowed and blocked connections between two nodes, in both directions, for the selected period.

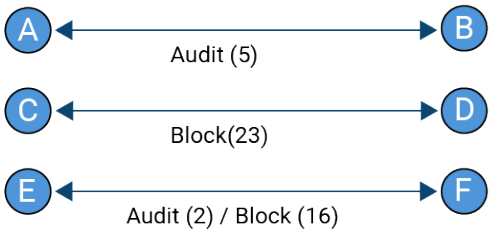


Figure 14.22: Bidirectional connection line

Line color

The color of the line indicates the action Endpoint Access Enforcement took on the connection. Red lines represent allowed connections in Audit mode. Gray lines represent blocked connections. See **Endpoint Access Enforcement operating mode**.

Endpoint Access Enforcement panels/widgets

Accessing the dashboard

To access the dashboard, select **Status** from the top menu. From the side menu, select **Endpoint Access Enforcement**.

Required permissions

Permission	Access to widgets
View detections and threats	Connection map Top 5 computers reporting high-risk outbound connections Top 5 computers reporting high-risk inbound connections Connections by condition Connections by monitored protocol

Table 14.53: Permissions required to access the Endpoint Access Enforcement widgets

Connection map

This widget provides a visual representation of connections between computers on the network, which meet the conditions configured in the Endpoint Access Enforcement settings. For more information about this widget, see **Connection Map**.

Top 5 computers reporting high-risk outbound connections

This widget shows the IP addresses or names of the five computers responsible for the highest number of high-risk connections to computers on the network.

The computer name appears if:

- The computer is managed by the same account that manages the target computer and has version 4.40 or higher of the security software installed.
- The logged-in user has visibility of the computer.

In other cases, the IP address appears.

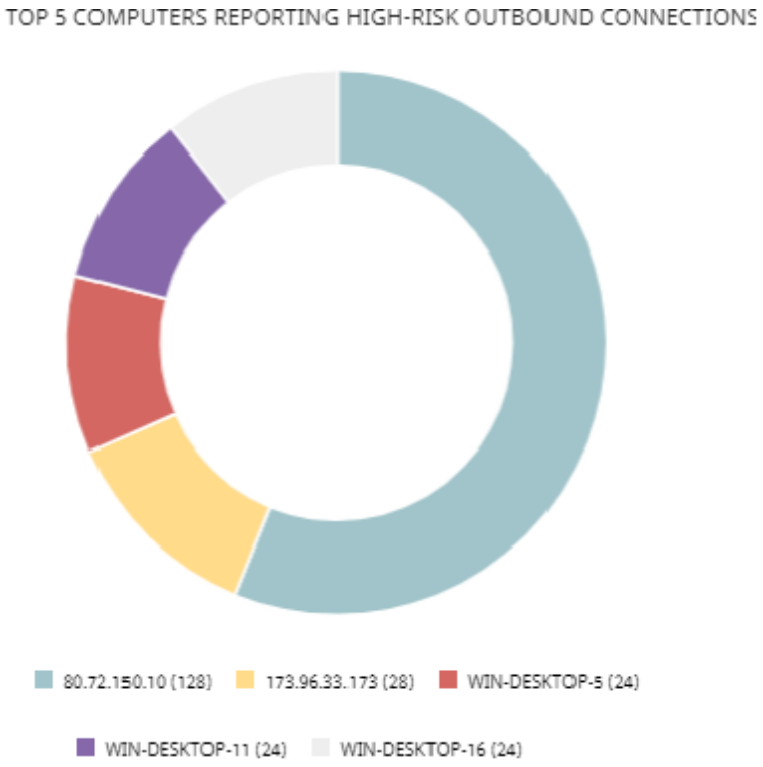


Figure 14.23: Top 5 Computers Reporting High-Risk Outbound Connections panel

Meaning of the data displayed

Each color represents one of the five IP addresses or computers responsible for the highest number of high-risk connections to the computers on the network, and the percentage corresponding to each one with respect to the total number of connections.

Lists accessible from the panel

Click one of the sections to open the **Connections identified by Endpoint Access Enforcement** list, filtered by that computer.

Top 5 computers reporting high-risk inbound connections

This widget shows the names of the five network computers that receive the highest number of high-risk inbound connections from managed computers.

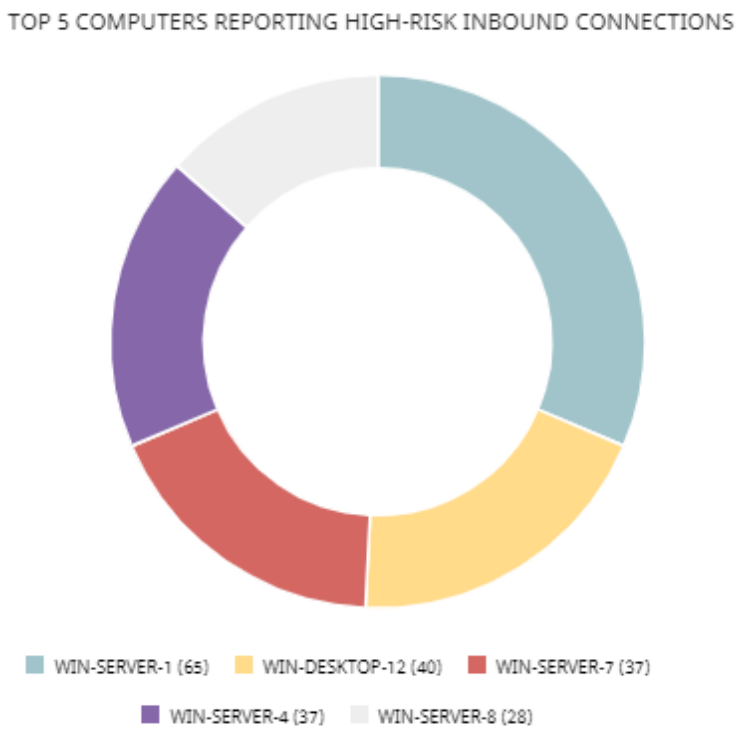


Figure 14.24: Top 5 Computers Reporting High-Risk Inbound Connections panel

Meaning of the data displayed

Each color represents one of the five network computers that receive the highest number of high-risk inbound connections, and the percentage corresponding to each one with respect to the total number of connections.

Lists accessible from the panel

Click one of the sections to open the **Connections identified by Endpoint Access Enforcement** list, filtered by that computer.

Connections by condition

This widget shows the trend of connections by the reason why they were categorized as dangerous. For more information, see **Security characteristics of connecting computers**

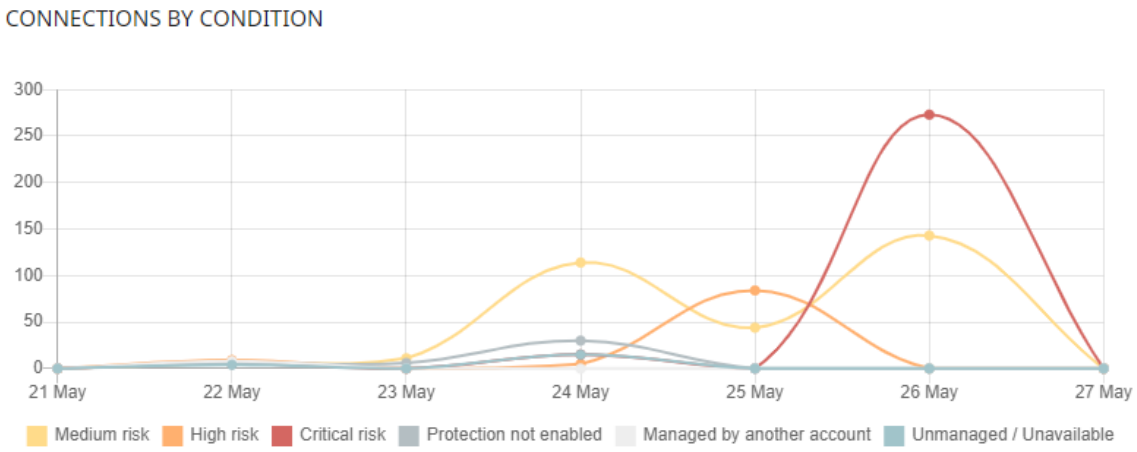


Figure 14.25: Connections by Condition panel

Meaning of the data displayed

Data	Description
Unmanaged/Unavailable	Number of connections from computers that do not meet the requirements described in **Minimum requirements**.
Protection not enabled	Number of connections from computers whose protection is not enabled.
Managed by another account	Number of connections from computers whose security software is installed but managed by another account.
Critical risk	Number of connections where the risk level for the connecting computer is critical risk.
High risk	Number of connections where the risk level for the connecting computer is high risk.
Medium risk	Number of connections where the risk level for the connecting computer is medium risk.

Description of the data displayed in the Connections by Condition panel

Lists accessible from the panel

Figure 14.26: Hotspots in the Connections by Condition panel

Click the hotspots shown to open the **Connections identified by Endpoint Access Enforcement** list with these predefined filters:

Hotspot	Filter
(1)	Connections where the risk detected = Unmanaged/Unavailable
(2)	Connections where the risk detected = Protection not enabled.
(3)	Connections where the risk detected = Managed by another account.
(4)	Connections where the risk detected = Critical risk.
(5)	Connections where the risk detected = High risk.
(6)	Connections where the risk detected = Medium risk.

Table 14.54: Connections by Condition widget filters

Connections by monitored protocol

This widget shows the connections made over monitored protocols. See **Monitoring inbound connection protocols**.

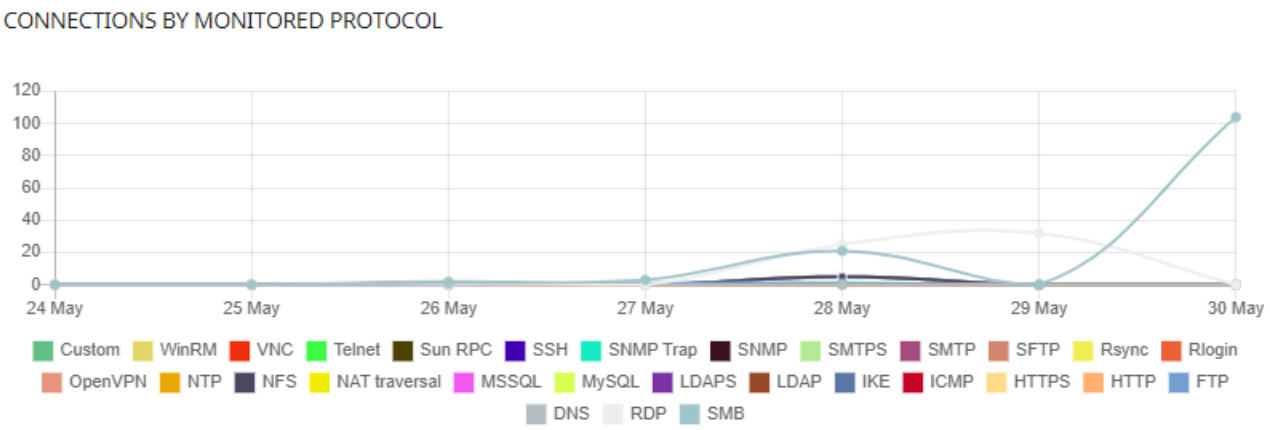


Figure 14.27: Connections by Monitored Protocol panel

Meaning of the data displayed

This widget shows the number of detected connections for each protocol.

Lists accessible from the panel

Click a protocol to open the **Connections identified by Endpoint Access Enforcement** list filtered to show the connections that used the selected protocol.

Endpoint Access Enforcement module lists

Accessing the lists

Access the Endpoint Access Enforcement lists as follows:

- From the top menu, select **Status**. From the side menu, select **Endpoint Access Enforcement**. Click any of the widgets.
- From the top menu, select **Status**. From the side menu, click **Add**. A dialog box opens with the available lists. Select the **Connections identified by Endpoint Access Enforcement** list.

Required permissions

Permission	Access to lists
View detections and threats	Connections identified by Endpoint Access Enforcement

Table 14.55: Permissions required to access the Endpoint Access Enforcement lists

Connections identified by Endpoint Access Enforcement

This list shows the inbound connections received by computers on the network that meet the conditions configured in the Endpoint Access Enforcement settings. See **Endpoint Access Enforcement settings options**.

Field	Description	Values
Computer	Name of the target computer.	Character string
Group	Group to which the target computer belongs.	Character string
Remote computer	IP address or name of the connecting computer.	Character string
Risk detected	Status of the connecting computer.	• Unmanaged/Unavailable • Managed by another account • Protection not enabled • Medium risk • High risk • Critical risk
Action	The action that Advanced EPDR took on the connection.	• Allowed • Blocked
Protocol/Port	Protocol/port of the connection.	Numeric value
Occurrences	Number of times the connection was detected in one hour.	Numeric value
Date	Date on which Endpoint Access Enforcement detected the connection.	Date
Context menu	Shows an action menu: • **View connections for the computer**: Shows connections received by the computer in the selected period. • **View connections for the**	Enumeration

Field	Description	Values
	remote computer: Shows connections established by the selected computer.	

Table 14.56: Fields in the Connections Identified by Endpoint Access Enforcement list

*To view a graphical representation of the list data, see the **Programs blocked by the administrator** widget.*

Fields displayed in the exported file

Field	Description	Values
Client	Customer ID or name.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the target computer.	Character string
Group	Group to which the target computer belongs.	Character string
IP address	Primary IP address of the target computer.	Numeric value
Risk detected	Status of the connecting computer	• Unmanaged/Unavailable • Managed by another account • Protection not enabled • Medium risk • High risk • Critical risk
Protocol	Protocol/port of the connection.	Numeric value

Field	Description	Values
Action	Action taken by Endpoint Access Enforcement on the connection.	• Allowed • Blocked
Local IP address	IP address of the target computer.	Numeric value
Remote host name	Name of the connecting computer.	Character string
Remote IP address	IP address of the connecting computer.	Numeric value
Local port	Connection port on the target computer.	Numeric value
Remote port	Connection port on the connecting computer.	Numeric value
Date	Date on which Endpoint Access Enforcement detected the connection.	Date
Occurrences	Number of times the connection was detected in one hour.	Numeric value

Table 14.57: Fields in the Connections Identified by Endpoint Access Enforcement exported file

Filter tool

Field	Description	Values
Search computer	Search by computer name.	Character string
Computer type	Filters by type of device.	• Workstation • Laptop • Server
Dates	Set a time period, from the current moment back.	• Last 24 hours • Last 7 days

Field	Description	Values
		• Last month • Last year
Action	Filter by the action taken by Endpoint Access Enforcement on the connection.	• Allowed • Blocked
Risk detected	Filter by the status of the connecting computer.	• Unmanaged/Unavailable • Managed by another account • Protection not enabled • Medium risk • High risk • Critical risk
Protocol	Filter by the connection protocol.	Character string

Table 14.58: Filters available in the Connections Identified by Endpoint Access Enforcement list

Connection Details page

In the Connections Identified by Endpoint Access Enforcement list, click a line to open the Connection Details page. The page has three sections:

- **Computer alerts (1)**: Shows details of the alert generated by the target computer.
- **Affected computer (2)**: Name, IP address, and type of the target computer.
- **Connection details (3)**: Summary of the local and remote IP addresses and ports used in the connection, and the number of times the connection was detected.

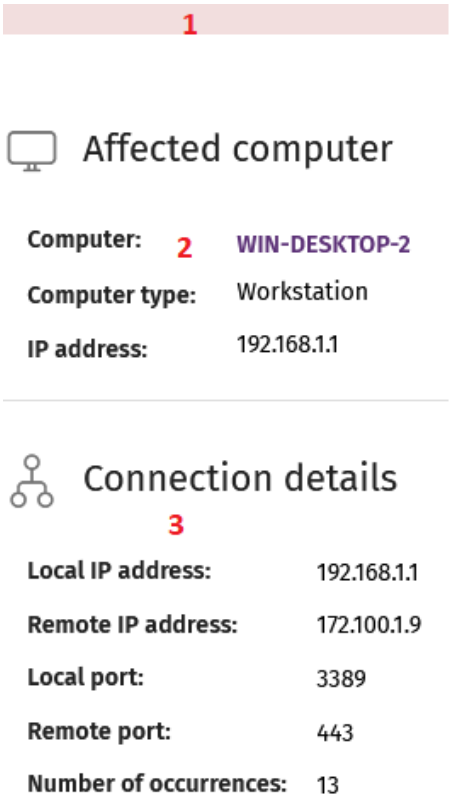


Figure 14.28: Breakdown of connection details information

Computer alerts (1)

Field	Description	Values
Detection date	Date the connection was detected.	Date

Risk detected	Status of the connecting computer	• Unmanaged/Unavailable
		• Managed by another account
		• Protection not enabled
		• Risk level equal to or greater than:
		  • Medium
		  • High
		  • Critical

Protocol	Protocol/port of the	Numeric value

Field	Description	Values
	connection.	
Action	Action taken by Endpoint Access Enforcement on the connection.	• Allowed • Blocked
Recommendations	Recommendations for the security administrator of the target computer.	Character string

Table 14.59: Computer alert details

Affected computer (2)

Field	Description	Values
Computer	Name of the target computer. If you have permission to view the computer, click it to access the Computer Details page. See **Computer details** on page **252**.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
IP address	Primary IP address of the target computer.	Numeric value

Table 14.60: Target computer details

Connection details (3)

Field	Description	Values
Local IP address	IP address of the target computer.	Numeric value
Remote IP address	IP address of the connecting computer.	Numeric value

Field	Description	Values
Local port	Connection port on the target computer.	Numeric value
Remote port	Connection port on the connecting computer.	Numeric value
Occurrences	Number of times the connection was detected in one hour.	Numeric value

Table 14.61: Connection details

Chapter 15

Cytomic Encryption (Device encryption)

Cytomic Encryption is a built-in module on Cytomic platform that encrypts the content of the data storage media connected to the computers managed by Advanced EPDR. By doing this, it minimizes the exposure of corporate data in the event of data loss or theft as well as when storage devices are removed without having deleted the data.

Cytomic Encryption is compatible with certain versions of Windows 7 and higher and certain versions of macOS (see **Supported Windows operating systems**). It enables you to monitor the encryption status of network computers and centrally manage their recovery keys. It also takes advantage of hardware resources such as TPM chips, delivering great flexibility when it comes to choosing the optimum authentication system for each computer.

For more information about the Cytomic Encryption module, see:

***Creating and managing settings profiles** on page **294**: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*

***Accessing, controlling, and monitoring the management console** on page **61**: Managing user accounts and assigning permissions.*

***Managing lists** on page **48**: Information about how to manage lists.*

Chapter contents

Introduction to encryption concepts

Cytomic Encryption uses tools integrated in the Windows and macOS operating systems to manage encryption on network computers protected with Advanced EPDR.

To help you understand the processes involved in the encryption and decryption of information, we present some concepts related to the encryption technology we use.

TPM

TPM (Trusted Platform Module) is a chip installed on the motherboard of some desktops, laptops, and servers. Its main aim is to protect user sensitive data, stored passwords, and other information used in login processes.

TPM also detects any changes in the boot events of the computer, for example preventing access to a hard drive from a computer other than the one used for its encryption.

Cytomic Encryption supports TPM versions 1.2 and higher. If possible, use TPM technology along with other supported authentication systems. If you disabled the TPM chip in the BIOS settings of your computer, you might have to manually enable the chip from the BIOS.

Supported authentication types

Login password

On macOS operating systems, the authentication method used is a login password. Compatible with all macOS versions supported by Cytomic Encryption.

PIN

A PIN (Personal Identification Number) is a sequence of numbers that works as a simple password and is requested when you boot a computer that has an encrypted drive. Without the PIN, the boot sequence is not completed and you cannot access the computer. Compatible with all supported versions of Windows.

Extended PIN

If the hardware is compatible, Cytomic Encryption uses an extended or enhanced PIN which combines letters and numbers to increase the complexity of the password.

Because the extended PIN is requested in the computer boot process prior to loading the operating system, BIOS limitations might restrict keyboard input to the 7-bit ASCII table.

Additionally, on computers with a keyboard layout other than EN-US, such as QWERTZ or AZERTY keyboards, there can be errors when you enter the extended PIN. For this reason, Cytomic Encryption checks that the characters entered by the user belong to an EN-US keyboard layout, before setting the extended PIN for the computer encryption process.

Compatible with all supported versions of Windows.

Passphrase

A passphrase is similar to a password, but is typically longer. It consists of alphanumeric characters and is equivalent to the extended PIN.

Cytomic Encryption prompts users for different types of passwords based on these circumstances:

- Passphrase: If the computer has a TPM chip installed.
- Extended PIN: If the computer operating system and hardware support it.
- PIN: If the other options are not valid.

Only available on Windows 8 computers and higher without a TPM chip.

USB key

Enables you to store the encryption key on a USB device formatted with the NTFS, FAT, or FAT32 file system. With a USB key, you do not need to enter a password to boot the computer. However, the USB device with the startup password must be plugged into the computer USB port.

Required on Windows 7 computers without a TPM chip.

Some older PCs cannot access USB drives during the boot process. Verify whether the computers in your organization have access to USB drives from the BIOS.

Recovery key

When Cytomic Encryption detects unusual activity on a protected computer, it prompts the user to enter a BitLocker recovery key. This key is managed from the management console and must be entered to complete the boot process.

Cytomic Encryption stores the recovery keys for all encrypted computer drives that it manages. The management console does not show keys for computers encrypted by users or not managed by Cytomic.

The recovery key is requested in these scenarios:

- A user makes repeated attempts to enter an incorrect PIN or password while the device boots up.
- A Trusted Platform Module (TPM) chip detects a change in the boot sequence.
- Changes are made to the computer motherboard.
- Deletion or disablement of TPM content
- Changes are made to the computer boot settings.
- When the startup process is changed:
    - BIOS update.
    - Firmware update.
    - UEFI update.
    - Changes to the boot sector.
    - Changes to the master boot record.
    - Changes to the boot manager.
    - Changes to the firmware (Option ROM) in certain components that are part of the boot process (video cards, disk controllers, etc).
    - Changes to other components that are part of the initial boot phases.

BitLocker

BitLocker is software installed on some versions of Windows 7 and higher operating systems. It encrypts and decrypts the data stored on computer drives. If not already installed, Cytomic Encryption automatically installs BitLocker on supported drives and then manages the drives.

FileVault

FileVault is built-in software on macOS operating systems. It automatically encrypts all files in a computer hard disk or SSD memory.

System partition

On Windows operating systems, a system partition is a small area of the hard disk which remains unencrypted and is required for the computer to correctly complete the boot process. Cytomic Encryption automatically creates this system partition if it does not already exist.

Encryption algorithm

For Windows, the encryption algorithm Cytomic Encryption uses is AES (256- bit), although computers with drives encrypted by users using other algorithms are also compatible.

For macOS, the algorithm used is AES-XTS.

Cytomic Encryption service overview

The general encryption process covers several areas that you must be aware of to adequately manage network resources that could contain sensitive information or compromising data if a drive were to be lost or stolen:

- **Meeting minimum hardware and software requirements**: See **Cytomic Encryption minimum requirements** to see the limitations and specific conditions applicable to each supported platform.
- **Previous encryption status of the user computer**: Depending on whether BitLocker or FileVault is already being used on the user computer, the process of integration in Cytomic Encryption might vary slightly.
- **Assigning encryption settings profiles**: Determine the encryption status (encrypted or not) of network computers and the authentication methods.
- **Interaction of the user with the encryption process**: The initial encryption process requires user interaction. For more information, see **Encryption of unencrypted drives**.
- **Viewing the encryption status of the network**: Through the widgets/panels in the **Status** menu, side panel **Cytomic Encryption**. For a complete description of the widgets included in Cytomic Encryption, see **Cytomic Encryption module panels/widgets** . Filters are also supported to find computers in lists according to their status. For more information, see **Available filters**.
- **Restriction of encryption permissions to security administrators**: The role system described in **Understanding permissions** on page **72** covers the encryption feature and the ability to view the encryption status of network computers.
- **Access to recovery keys**: Where the user forgets their password or PIN/passphrase, or when the TPM chip detects an irregular situation on a computer it protects, the network administrator can centrally obtain the recovery key and send it to the user. For more information, see **Obtaining a recovery key**.

General features of Cytomic Encryption

Supported authentication types

Cytomic Encryption supports various methods to authenticate encrypted disks. The operating system version and the presence of a Trusted Platform Module (TPM) chip determine the type of authentication to use. The supported authentication methods are (in the order we recommend them):

Windows

- **Security Processor (TPM) and Password**: Compatible with all supported versions of Microsoft Windows. The TPM chip must be enabled in the BIOS, and a PIN must be established.
- **Security Processor (TPM)**: Compatible with all supported versions of Microsoft Windows. The TPM chip must be enabled in the BIOS, except in Windows 10, where it is automatically enabled.
- **USB drive**: Requires a USB key and a computer that can read USB devices while booting. Required on Windows 7 computers without a TPM chip.
- **Password**: Only available on computers than run Windows 8 or higher without a TPM chip.

macOS

On macOS operating systems, the authentication method used is a login password. Compatible with all macOS versions supported by Cytomic Encryption. See **Supported Windows operating systems**.

By default, Cytomic Encryption uses an encryption method that includes the use of a TPM chip, if available. If you choose an authentication method not included in the above list, the management console shows a warning indicating that the computer will not be encrypted.

Supported storage devices

Cytomic Encryption supports these internal storage devices:

Windows and macOS

- Fixed storage drives on a computer (system and data).

Windows

- Used storage space on virtual hard drives (VHD).
- Removable hard drives.
- USB drives.

These storage devices are not supported:

- Dynamic hard drives.
- Small partitions.

- Other external storage devices.

Cytomic Encryption minimum requirements

The minimum requirements are divided into these categories:

- Supported Windows operating systems.
- Supported macOS operating systems.
- Hardware requirements for Windows computers.

Supported Windows operating systems

- Microsoft Windows 7 (Ultimate, Enterprise)
- Microsoft Windows 8/8.1 (Pro, Enterprise)
- Microsoft Windows 10 (Pro, Enterprise, Education)
- Microsoft Windows 11 (Pro, Enterprise, Education)
- Windows Server 2008 R2, Windows Server 2012, and higher (includes Server Core editions)

Supported macOS operating systems

- macOS 10.15 Catalina
- macOS 11.0 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma

Hardware requirements for Windows computers

- Trusted Platform Module (TPM) 1.2 and higher (if used to authenticate).
- USB key and a computer that can read USB drives from the BIOS (Windows 7).

For macOS operating systems, there are no specific hardware requirements.

Management of computers according to their prior encryption status

Management of computers by Cytomic Encryption

For a computer on the network to be managed by Cytomic Encryption, it must meet the following conditions:

- It must meet the minimum requirements described in section **Cytomic Encryption minimum requirements**.
- The computer must have received, at least once, a settings profile from the management console that establishes the encryption of its drives, and these have been encrypted successfully.

Computers that previously had some drives encrypted and have not received a settings profile to encrypt their drives are not managed by Cytomic Encryption and, therefore, the administrator does not have access to the recovery key or the status of the computer.

However, computers that have received a settings profile to encrypt their drives are managed by Cytomic Encryption regardless of their previous status (encrypted or not).

Uninstallation of the Advanced EPDR agent

Regardless of whether a computer is managed by Cytomic Encryption or not, if its drives are encrypted, when uninstalling Advanced EPDR they are left as they are. However, centralized access to the recovery key is lost.

If the computer is subsequently reinstated in Advanced EPDR, the last stored recovery key is displayed.

Encryption and decryption on Windows computers

Encryption of unencrypted drives

Encryption begins when the Advanced EPDR agent, installed on a computer, downloads encryption settings. A wizard on the computer guides the user through the encryption process.

The number of encryption steps to take depends on the type of authentication chosen by the network administrator and the previous status of the computer. If any of the steps fails, the agent reports it to the management console and the process stops.

You cannot encrypt computers from a remote desktop session. You must restart the computer and enter a password before the operating system is loaded, and this is not possible with a standard remote desktop tool
If there is a patch installation or uninstallation task in progress managed by Cytomic Encryption, the encryption process begins when that task has completed.

This section describes the entire encryption process, whether feedback is shown to the computer user, and whether a restart is required:

Step	Process on the computer	User interaction
1	The agent receives settings from the encryption module. The settings establish the encryption of drives.	None
2	If a computer is a server and does not have BitLocker installed, it is downloaded and installed.	The computer user is prompted to restart the computer to complete the install. If the user chooses to postpone the restart, they are prompted again during the next login. Requires restart.
3	If a computer has no previous encryption, a system partition is created.	The computer user must restart the computer to complete the creation of the partition. If the user chooses to postpone the restart, they are prompted again during the next login. Requires restart.
4	If a group policy exists that conflicts with the settings in Cytomic Encryption, an error message shows and the process stops. The group policies configured by Cytomic Encryption are: In the Local Group Policy Editor, navigate to: Local Computer Policy > Computer Configuration > Administrative Templates > Windows	If you have not defined global group policies that conflict with the local policies defined by Cytomic Encryption, no message appears.

Step	Process on the computer	User interaction
	Components > BitLocker Drive Encryption > Operating System Drives. Select Not Set for the specified policies to avoid this error.	
5	If a computer has a TPM chip installed, the computer user might have to enable the TPM chip from the BIOS for the computer.	The computer must restart for the user to access the BIOS. On Windows 10 systems, you do not need to changer the BIOS settings but the restart is required. The restart in step 3, if required, combines with this one.
6	If a computer uses a USB device for authentication, prepare it.	The computer user must insert the USB device when the computer boots.
7	If a computer uses a PIN for authentication, prepare it.	The computer user must type the PIN. If alphanumeric characters are used and the hardware is not compatible with those characters, error -2144272180 appears. In that case, you must enter a numerical PIN.
8	If a computer uses a passphrase for authentication, prepare it.	The computer user must type the passphrase.
9	A recovery key is generated and sent to the Cytomic cloud. After it has been received, the process continues on the user computer.	None.
10	Check that the hardware on the computer is compatible with the encryption technology. The encryption process begins.	Restart the computer to check the hardware used in the various authentication methods. Requires restart.
11	Drive encryption.	The encryption process begins. It runs in the background, without any impact to

Step	Process on the computer	User interaction
		users. The length of the process varies depending on the drive that is encrypted. On average, encryption takes approximately 2-3 hours. Users can use and shut down computers normally. In the latter case, the process continues when the computer is restarted.
12	The encryption process takes place silently, without any impact to users.	Depending on the authentication method selected, the user might need to plug a USB key, enter a PIN, a passphrase, or nothing when the computer boots.

Table 15.1: Steps for encrypting unencrypted drives

Encryption of previously encrypted drives

If a computer already has encrypted drives, Cytomic Encryption modifies certain parameters so that the drives can be centrally managed. The actions taken are as follows:

- If a computer user selects an authentication method that differs from the method specified in the settings profile, a prompt shows on the user's computer that asks for passwords or other hardware resources. If it is not possible to use an authentication method compatible with the operating system, and specified by the network administrator, the existing encryption method remains in place. Cytomic Encryption does not manage the computer.
- If the encryption algorithm is not AES-256, Cytomic Encryption makes no encryption changes to the computer drive. Cytomic Encryption manages the computer.
- If both encrypted and unencrypted drives exist, ll drives are encrypted with the same authentication method.
- To unify authentication methods, if a previous authentication method requires a password, and the method is compatible with the authentication methods supported by Cytomic Encryption, a prompt shows on the user's computer that requests the password.
- If computer user encryption settings differ from those configured by the administrator, to minimize the encryption process, no changes are made.
- When you manage a drive with Cytomic Encryption, at the end of the process, Cytomic generates a recovery key and sends it to the Cytomic cloud.

Encryption of new drives

f you create a new drive entry after the encryption process is complete, Cytomic Encryption encrypts the drive immediately and according to the encryption settings.

Decrypting drives

There are three scenarios:

- If Cytomic Encryption uses settings to encrypt a computer, Cytomic Encryption can also decrypt it.
- If a computer was previously encrypted and the agent assigns encryption settings settings on install, Cytomic Encryption sees the computer as encrypted and you can use Cytomic Encryption settings to decrypt the computer.
- If a computer was previously encrypted and the agent does not assign encryption settings on install, Cytomic Encryption does not class the computer as encrypted and you cannot use Cytomic Encryption settings to decrypt the computer.

Local editing of BitLocker settings

When using BitLocker to manually decrypt a drive from the Control Panel in Microsoft Windows, changes made to local settings automatically revert to settings made in the management console. The way that Cytomic Encryption responds to a change of this type is as follows:

- **Disable automatic locking of a drive**: It reverts to automatic locking.
- **Remove the password for a drive**: A new password is requested.
- **Decrypt a drive previously encrypted by** Cytomic Encryption: The drive is automatically encrypted.
- **Encrypt a decrypted drive**: If the Cytomic Encryption settings profile implies decrypting drives, the user action takes precedence and the drive is not decrypted.

Encrypting and decrypting external hard drives and USB drives

Because users can connect and disconnect external storage devices from their computers at any time, the way Cytomic Encryption works with these devices is as follows:

- If the workstation or server does not have BitLocker installed and running, the agent does not download the required packages and the device is not encrypted. Nor are any messages shown to the user.
- If the computer has BitLocker installed and running, a pop-up message is shown to the user prompting them to encrypt the device in these following situations:
    - Each time a user connects an unencrypted drive.
    - If there is an unencrypted device connected to the computer at the time the administrator enables the encryption settings profile from the web console.

- The message shows for five minutes. Regardless of whether the user agrees to encrypt the device or not, they are able to use it normally, unless a settings profile has been configured that prevents the use of unencrypted devices. For more information, see **Write to removable storage drives** on page **396**.
- The encryption process does not require the creation of a system partition.
- If the external storage device is already encrypted by a solution other than Cytomic Encryption, and the user connects it to their computer, the encryption message is not shown and the device can be used normally. Cytomic Encryption does not send the recovery keys to the web console.
- If a settings profile has been configured for the device control feature that prevents this type of hardware from being connected to the computer, the encryption message is not shown to the user. For more information, see **Device control (Windows computers)** on page **353**.
- Unless configured otherwise, you can use an unencrypted drive. However, in Cytomic Data Watch settings, if you enable the **Write to removable storage drives** option, and Cytomic Encryption or BitLocker did not encrypt the drive, you cannot write to the drive. For more information, see **Write to removable storage drives** on page **396**.
- To decrypt a device encrypted by Cytomic Encryption, the user can use BitLocker manually.
- Only the used space of a drive is encrypted.
- The same key encrypts all partitions on the external drive.

If you remove an external drive while encryption is in progress, the contents of the drive might be corrupted.

Cytomic Encryption response to errors

- **Errors in the hardware test**: The hardware test runs every time the computer is started up until it is passed, at which time the computer automatically begins encryption.
- **Error creating the system partition**: Many of the errors that occur when creating the system partition can be rectified by the user (for example, lack of space). Periodically, Cytomic Encryption will automatically try to create the partition.
- **User refusal to enable the TPM chip**: The computer will show a message at startup asking the user to enable the TPM chip. Until this condition is resolved, the encryption process will not start.

Obtaining a recovery key

Users are prompted to enter the recovery key:

- **Windows**: When the user has lost their PIN/passphrase/USB device, or the Trusted Platform Module (TPM) chip detects a change in the computer boot sequence.
- **macOS**: When the user has lost their login password, or a change is detected in the computer boot sequence.

Cytomic Encryption stores the recovery keys for all encrypted computer drives that it manages. Therefore, you can obtain these recovery keys through the web management console. To obtain a recovery key, you need this data depending on the operating system installed on the computer:

- **Windows**: You need the recovery key ID. The recovery key ID is a unique 40-digit string associated with each encrypted drive.
- **macOS**: You need the ID of the recovery key associated with the computer. The same recovery key is used for all drives on a Mac computer.

Required permissions

Permission	Access type
Access recovery keys for encrypted drives	To obtain and find the recovery key for an encrypted drive.

Table 15.2: Permissions required to obtain a recovery key

Obtaining the recovery key ID for an encrypted drive (Windows computers)

When a user makes repeated attempts to enter an incorrect PIN or password while the device boots up, they are prompted to enter a BitLocker recovery key:

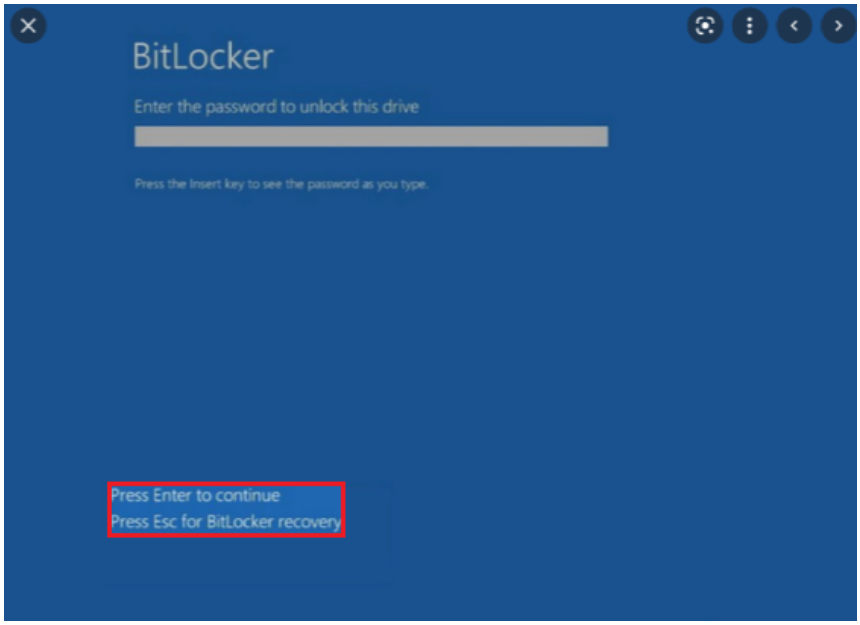


Figure 15.1: Accessing the recovery key ID for an encrypted drive
Figure 15.2:

Press **ESC** to access the screen that shows the recovery key ID for the encrypted drive:

Figure 15.3: Recovery key ID for an encrypted drive

In the case of a recovery key ID for an encrypted partition, the screen shows only the first eight digits of the recovery key ID:

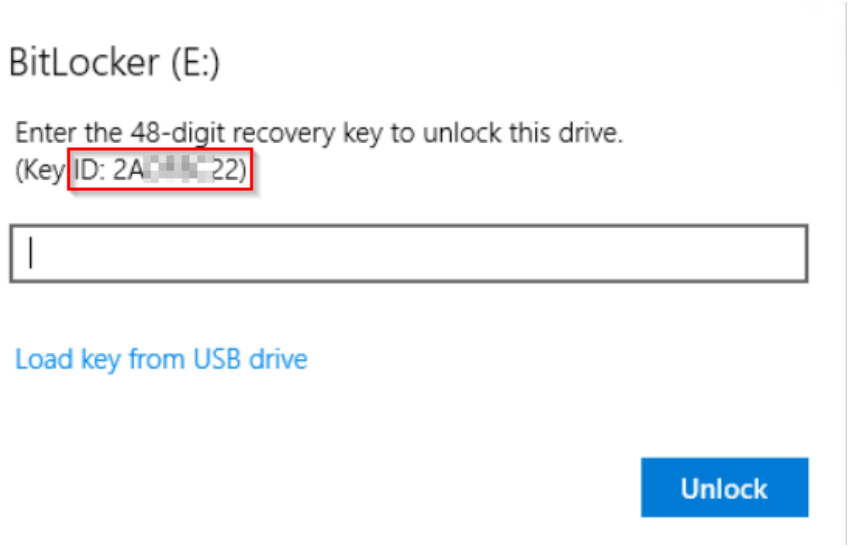


Figure 15.4: Recovery key ID for an encrypted disk partition

For more information about the encryption of drives on computers, see section ***Encryption and decryption on Windows computers****.*

Obtaining the ID of the recovery key associated with a computer (macOS computers)

When you try to access an encrypted computer, the login screen shows a message that contains the ID of the recovery key associated with the computer. The screen also recommends that you contact the encryption settings administrator.

Obtaining a recovery key

- From the top menu, select **Computers**. Select the computer you want to obtain the recovery key for.
- On the **Details** tab, **Data protection** section, click the **Get recovery key** link. To obtain a removable drive recovery key, click **View encrypted devices on this computer**.

  The **Get recovery key** dialog box opens and shows the IDs of the encrypted drives on the computer.
- Click the encrypted drive ID of the key you want to recover. The **Get recovery key** dialog box opens.
- Click **Copy recovery key** and send it to the user.

Finding a recovery key

If the user has visibility of all the computers in an account, the search results also include the IDs of drives on computers that were deleted.

Finding a recovery key from the Encrypted Computers widget

- From the top menu, select **Status**. From the side menu, select **Full Encryption**.
- In the **Encrypted Computers** widget, click **Recovery key search**.

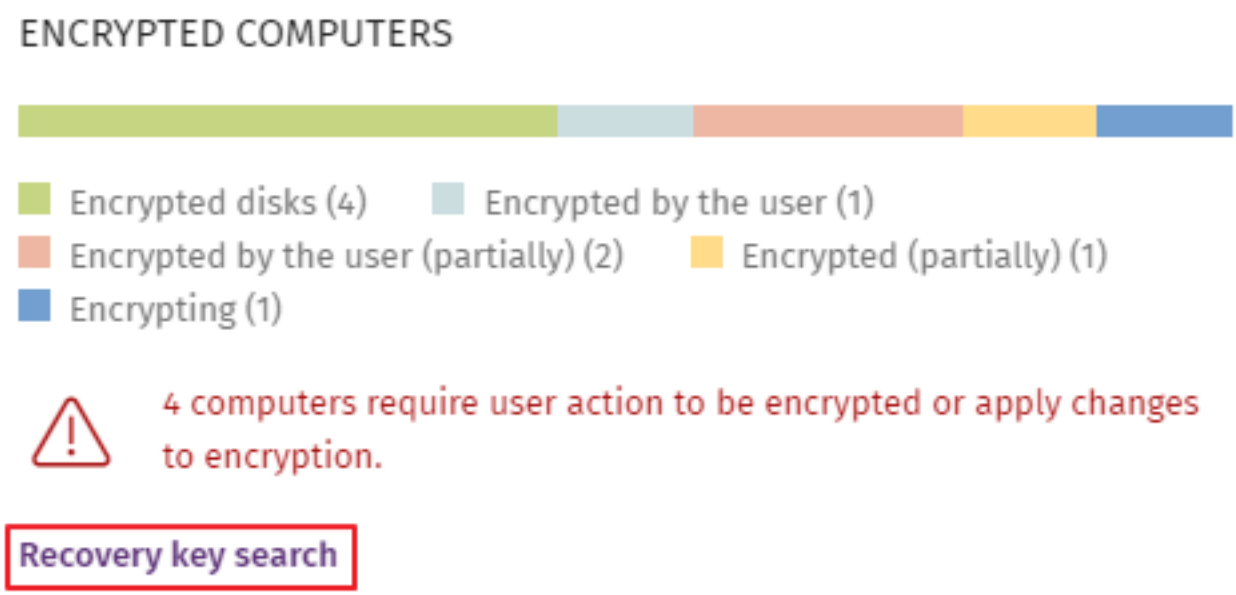


Figure 15.5: Finding a recovery key

- Type the ID of the recovery key you want to find. The recovery key that the user can use to unlock the encrypted drive is shown.
- In the case of a recovery key ID for an encrypted partition, enter the first eight digits. The recovery key that the user can use to unlock the encrypted disk partition is shown.

> *If the first eight digits of a recovery key are the same for more than one key, all keys appear in the search results.*

Finding a recovery key from the Computer Details page

- From the top menu, select **Computers**. Select the computer you want to find the recovery key for.

- On the **Details** tab, **Data protection** section, click the **Get recovery key** link. To obtain a removable drive recovery key, click **View encrypted devices on this computer**.

  The **Get recovery key** dialog box opens and shows the IDs for all encrypted drives on the computer.

- To find another recovery key, click **Find another key**.

Cytomic Encryption module panels/widgets

Accessing the dashboard

From the top menu, select **Status**. From the side menu, select Cytomic Encryption.

Required permissions

You do not need additional permissions to access the widgets associated with **Cytomic Encryption**.

Encryption status

This widget shows the computers that support Cytomic Encryption and their encryption status.

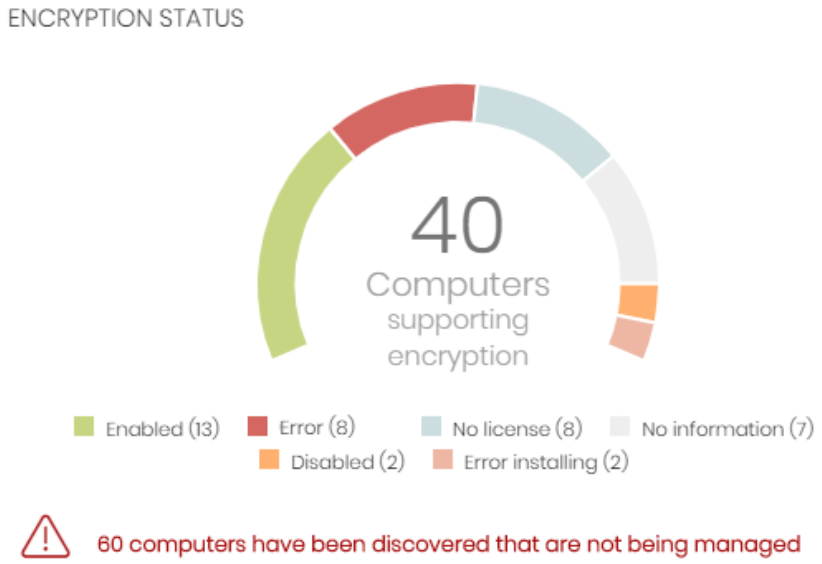


Figure 15.6: Encryption Status panel

Meaning of the data displayed

Data	Description
Enabled	Computers with Cytomic Encryption installed. Settings are assigned to encrypt the computer, and there are no reports of any encryption or installation errors.
Disabled	Computers with Cytomic Encryption installed. Settings are assigned to not

Data	Description
	encrypt the computer, and there are no reports of any encryption or installation errors.
Error	Computers not able to perform actions that are specified in the encryption or decryption settings.
Error installing	Computers, when required, not able to download and install BitLocker.
No license	Computers that are compatible with Cytomic Encryption, but do not have a Advanced EPDR license assigned.
No information	Computers with a recently assigned license that have not reported their status to the server, or computers with an expired agent.

Table 15.3: Description of the data displayed in the Encryption Status panel

Lists accessible from the panel

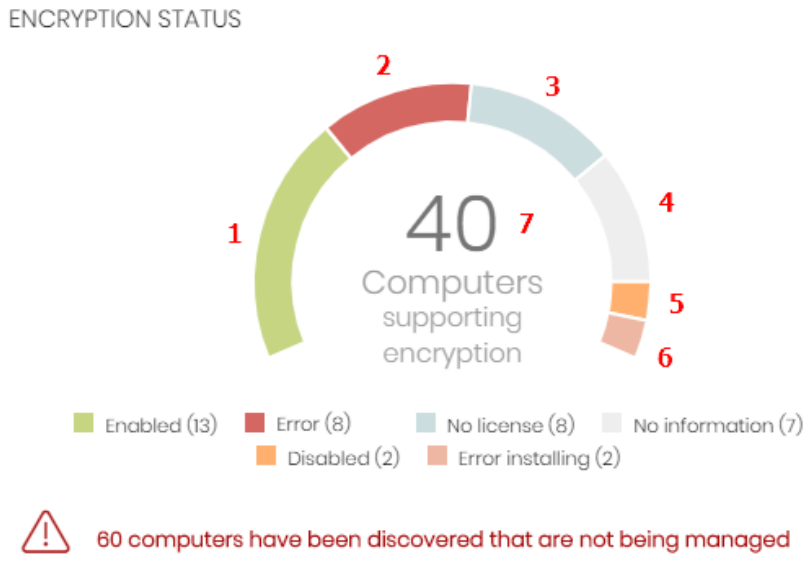


Figure 15.7: Hotspots in the Encryption Status panel

Click the hotspots shown in **Figure 15.7:** to open the **Encryption status** list with these predefined filters:

Hotspot	Filter
(1)	Encryption status = Enabled.

Hotspot	Filter
(2)	Encryption status = Error.
(3)	Encryption status = No license. The computer does not have a Advanced EPDR license assigned.
(4)	Encryption status = No information.
(5)	Encryption status = Disabled.
(6)	Encryption status = Error installing.
(7)	No filter.

Table 15.4: Lists accessible from the Encryption Status panel

Computers supporting encryption

This widget shows computers that support encryption technology, grouped by type. The color green indicates devices that support encryption, and the color red indicates devices that do not.

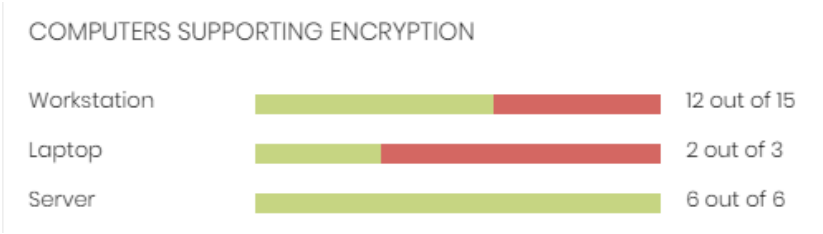


Figure 15.8: Computers Supporting Encryption panel

Meaning of the data displayed

Data	Description
Workstation - green	Workstations that support encryption.
Workstation - red	Workstations that do not support encryption.
Laptop - green	Laptops that support encryption.
Laptop - red	Laptops that do not support encryption.
Server - green	Servers that support encryption.

Data	Description
Server - red	Servers that do not support encryption.

Table 15.5: Description of the data displayed in the Computers Supporting Encryption panel

Lists accessible from the panel

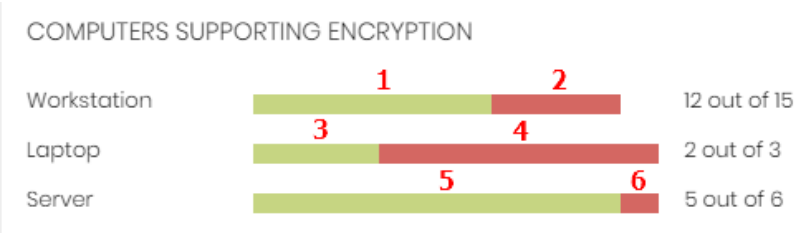


Figure 15.9: Hotspots in the Computers Supporting Encryption panel

Click the hotspots shown in **Figure 15.9:** to open the **Encryption status** list with these predefined filters:

Hotspot	Filter
(1)	Computer type = Workstation.
(2)	Computer list filtered by **Encryption not supported**.
(3)	Computer type = Laptop.
(4)	Computer list filtered by **Encryption not supported**.
(5)	Computer type = Server
(6)	Computer list filtered by **Encryption not supported**.

Table 15.6: Lists accessible from the Computers Supporting Encryption panel

Encrypted computers

This widget shows the encryption status of computers that support Cytomic Encryption.

For more information about how to search for recovery keys, see section ***Obtaining a recovery key***.

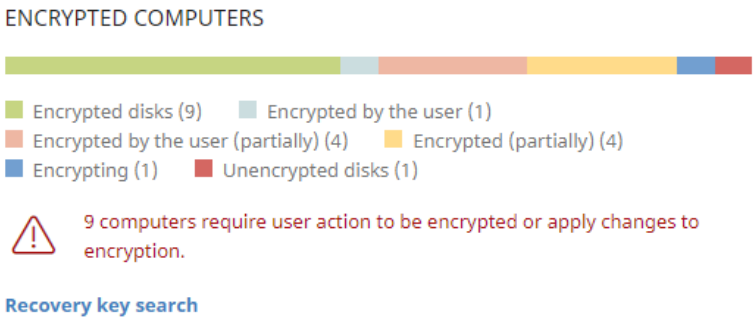


Figure 15.10: Encrypted Computers panel

Meaning of the data displayed

Data	Description
Unknown	Disks encrypted with an authentication method that Cytomic Encryption does not support.
Unencrypted disks	Neither the user or Cytomic Encryption has encrypted a disk.
Encrypted disks	Cytomic Encryption has encrypted all disks.
Encrypting	At least one disk is currently in the encryption process.
Decrypting	At least one disk is currently in the decryption process.
Encrypted by the user	A user encrypted some or all of the disks.
Encrypted by the user (partially)	A user encrypted some or all of the disks. Cytomic Encryption encrypts or decrypts the remainder.
Encrypted (partially)	Cytomic Encryption encrypted at least one of the disks. The remaining disks are unencrypted.

Table 15.7: Description of the data displayed in the Encrypted Computers panel

Lists accessible from the panel

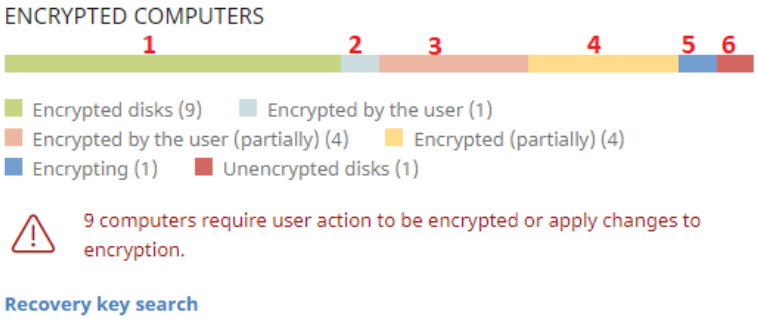


Figure 15.11: Hotspots in the Encrypted Computers panel

Click the hotspots shown in **Figure 15.11:** to open the **Encryption status** list with these predefined filters:

Hotspot	Filter
(1)	Disk encryption = Encrypted disks.
(2)	Disk encryption = Encrypted by the user.
(3)	Disk encryption = Encrypted by the user (partially).
(4)	Disk encryption = Encrypted (partially).
(5)	Disk encryption = Encrypting.
(6)	Disk encryption = Unencrypted disks.
(7)	Disk encryption = Decrypting.
(8)	Disk encryption = Unknown.

Table 15.8: Lists accessible from the Encrypted Computers panel

Authentication method applied

This widget shows encrypted computers and the type of authentication used. For more information about the supported authentication methods, see **General features of Cytomic Encryption**.

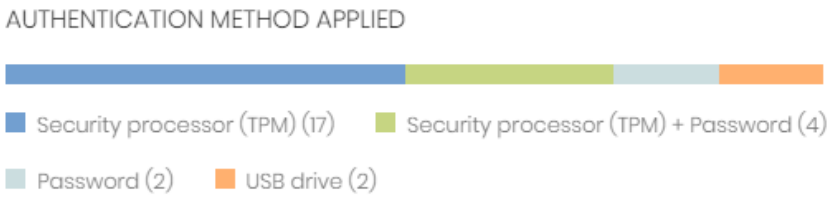


Figure 15.12: Authentication Method Applied panel

Meaning of the data displayed

Data	Description
Unknown	Cytomic Encryption does not support the user-selected authentication method.
Security processor (TPM)	The computer uses a Trusted Platform Module (TPM) chip for authentication.
Security processor (TPM) + Password	While booting, the computer uses a TPM chip and PIN or password for authentication.
Password	• **Windows computers:** While booting, the computer requests a PIN or passphrase for authentication. • **Mac computers:** While booting, the computer requests a password for authentication.
USB drive	While booting, the computer uses a USB key for authentication.
None	The computer has no encrypted disks.

Table 15.9: Description of the data displayed in the Authentication Method Applied panel

Lists accessible from the panel

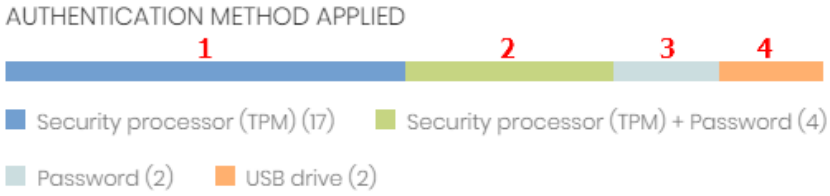


Figure 15.13: Hotspots in the Authentication Method Applied panel

Click the hotspots shown in **Figure 15.13:** to open the **Encryption status** list with these predefined filters:

Hotspot	Filter
(1)	Authentication method = Security processor (TPM)
(2)	Authentication method = Security processor (TPM) + Password
(3)	Authentication method = Password
(4)	Authentication method = USB drive
(5)	Authentication method = Unknown
(6)	Authentication method = None

Table 15.10: Description of the list filters

Cytomic Encryption lists

Accessing the lists

You can access the lists in two ways:

- From the top menu, select **Status**. From the side menu, select **Cytomic Encryption**. Click the relevant widget.

  Or,

- From the top menu, select **Status**. From the side menu, click the **Add** link. A window opens that shows the available lists.
- From the **Data protection** section, select a list to view the associated template. Edit it and click **Save**. The list is added to the side menu.

Required permissions

You do not need additional permissions to access the **Encryption status** list.

Encryption status

This list shows all computers on the network managed by Advanced EPDR and compatible with Cytomic Encryption. It includes filters related to the module to monitor the encryption status of the network.

Field	Comment	Values
Computer	Name of the computer compatible with the	Character string

Field	Comment	Values
	encryption technology.	
Computer status	Agent reinstallation: •  Reinstalling the agent. •  Agent reinstallation error Protection reinstallation: •  Reinstalling the protection. •  Protection reinstallation error. •  Pending restart. Computer isolation status: •  Computer in the process of being isolated. •  Isolated computer. •  Computer in the process of stopping being isolated. "RDP attack containment" mode: •  Computer in "RDP attack containment" mode. •  Ending "RDP attack containment" mode.	Icon
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
Operating system	Operating system and version installed on the workstation or server.	Character string
Hard disk encryption	Cytomic Encryption module status.	• No information • Enabled • Disabled • Error

Field	Comment	Values
		• Install error • No license
Disk status	Encryption status of the computer internal storage media.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted by the user (partially) • Encrypted (partially)
Authentication method	Authentication method selected to encrypt disks.	• All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password • USB drive • None
Last connection	Date when the agent last connected to the Cytomic cloud.	Date

Table 15.11: Fields in the Encryption Status list

*To view a graphical representation of the list data, see the **Encrypted computers** widget.*

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer compatible with the encryption technology.	Character string
IP address	The computer primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
Agent version	Internal version of the Cytomic agent module.	Character string
Installation date	Date when the Advanced EPDR software was successfully installed on the computer.	Date
Last connection date		Date
Platform	Operating system installed on the computer.	Character string
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Updated protection	Indicates whether or not the installed protection module is updated to the latest version released.	Boolean
Protection version	Internal version of the protection module.	Character string
Updated	Indicates whether or not the signature file found	Boolean

Field	Comment	Values
knowledge	on the computer is the latest version.	
Last update	Date when the signature file was last updated.	Date
Hard disk encryption	Cytomic Encryption module status.	• No information • Enabled • Disabled • Error • Install error • No license
Disk status	Encryption status of the computer internal storage media.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted (partially) • Encrypted by the user (partially)
Encryption pending user action	The user must restart the computer or enter data to complete the encryption process.	Boolean
Authentication method	Authentication method selected to encrypt disks.	• All • Unknown • Security processor (TPM) • Security processor (TPM)

Field	Comment	Values
		+ Password • Password • USB drive • None
Encryption date	Date when the first drive was encrypted on a fully encrypted computer (all compatible drives are encrypted).	Date
TPM spec version	Version of the TPM specifications supported by the chip on the computer.	Character string
Encryption installation error date	Date of the last reported installation error.	Date
Encryption installation error	An error occurred installing the Cytomic Encryption module on the computer.	Character string
Encryption error date	Last date when an encryption error was reported on the computer.	
Encryption error	The encryption process returned an error.	Character string

Table 15.12: Fields in the exported file

Filter tool

Field	Comment	Values
Encryption date from	Start point of the date range for fully encrypted computers.	Date
Encryption date to	End point of the date range for fully encrypted computers.	Date
Platform	Operating system installed on the computer.	• All • Windows

Field	Comment	Values
		• macOS
Computer type	Type of device.	• Workstation • Laptop • Server
Disk status	Encryption status of the computer internal storage media.	• Unknown • Unencrypted disks • Encrypted disks • Encrypting • Decrypting • Encrypted by the user • Encrypted (partially) • Encrypted by the user (partially)
Hard disk encryption	Cytomic Encryption module status.	• No information • Enabled • Disabled • Error • Install error • No license
Authentication method	Authentication method selected to encrypt disks.	• All • Unknown • Security processor (TPM) • Security processor (TPM) + Password • Password • USB drive

Field	Comment	Values
		• None
Last connection	Date when the Advanced EPDR status was last sent to the Cytomic cloud.	Date
Encryption pending user action	Indicates whether the user must take action to complete the encryption process.	• All • Yes • No

Table 15.13: Filters available in the list

Computer details page

Click a row in the list to open the computer details page. For more information, see **Computer details** on page **252**.

Encryption settings

Accessing the settings

- From the top menu, select **Settings**. From the side menu, select **Encryption**.
- Click the **Add** button. The settings page opens.

Required permissions

Permission	Access type
Configure computer encryption	Create, edit, delete, copy, or assign encryption settings profiles.
View computer encryption settings	View encryption settings profiles.

Table 15.14: Permissions required to access the encryption settings

Cytomic Encryption settings

Encrypt all hard disks on computers

Specify whether the computers will be encrypted or not. Depending on the previous status of a computer, the way that Cytomic Encryption behaves varies:

- If a computer is encrypted with Cytomic Encryption and you disable **Encrypt all hard disks on computers**, all encrypted drives are decrypted.
- If a computer is encrypted with a product other than Cytomic Encryption, and you disable **Encrypt all hard disks on computers**, there are no changes.
- If a computer is encrypted with a product other than Cytomic Encryption, and you enable **Encrypt all hard disks on computers**, the internal encryption settings are adjusted to match the encryption methods supported by Cytomic Encryption, thereby avoiding re-encrypting the drive. For more information, see **Encryption of previously encrypted drives**.

  With macOS computers, a new recovery key is generated. See **Encryption and decryption on macOS computers**
- If a computer is not encrypted, and you enable **Encrypt all hard disks on computers**, all the computer drives are encrypted. See **Encryption and decryption on Windows computers** and **Encryption and decryption on macOS computers**.

Ask for password to access the computer (Windows computers)

Enable password authentication when a computer or device starts. Depending on the platform and whether there is TPM hardware, two types of passwords are permitted:

- **Computers with TPM**: Require a PIN type password.
- **Computers without TPM**: Require a passphrase.

> *If you disable this option and the computer does not have access to a compatible TPM security processor, the disks are not encrypted.*

Do not encrypt computers that require a USB drive for authentication (Windows computers)

To prevent the use of USB devices supported by Cytomic Encryption in authentication, you can disable them.

> *Only Microsoft Windows 7 without TPM can use USB authentication. If you disable USB devices, these computers are not encrypted.*

Encrypt used disk space only (Windows computers)

To minimize the encryption time, enable **Encrypt used disk space only** to only encrypt sectors of the hard disk that are used. Sectors released after a file is deleted remain encrypted, but the space that

was free before encryption of the hard disk remains unencrypted. It will be accessible to third parties with tools to recover deleted files.

Prompt for removable storage drive encryption (Windows computers)

When a user inserts an unencrypted removable drive in a computer that has Microsoft BitLocker technology enabled, they receive a prompt to encrypt its contents. For more information about this setting, see **Encrypting and decrypting external hard drives and USB drives**.

Available filters

To find network computers with any of the encryption statuses defined in Cytomic Encryption, use the filter tree resources shown in section **Filter tree** on page **214**. The available filters are as follows:

- Encryption:
    - Encryption pending user action.
    - Disk status.
    - Encryption date.
    - Authentication method.
    - Is waiting for the user to perform encryption actions.
- Settings:
    - Encryption.
- Computer:
    - Has a TPM.
- Hardware:
    - TPM - Activated.
    - TPM - Manufacturer.
    - TPM - Owner.
    - TPM - Version.
    - TPM – Spec version.
- Modules:
    - Encryption.

Chapter 16

Program blocking settings

To increase the security of the Windows computers on the network, you can prevent the use of programs you consider dangerous or not compatible with the work of your organization. There are many reasons why you might want to prevent the execution of certain programs:

- Programs which, due to the way they run, use too much bandwidth or establish too many connections, negatively impacting company connectivity if run simultaneously by multiple users.
- Programs that enable users to access contents that might contain security threats.
- Programs that enable users to access contents not related to company activity and which might affect user performance.

For additional information about the program blocking module, see:

Creating and managing settings profiles *on page* ***294****: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*

Accessing, controlling, and monitoring the management console *on page* ***61****: Managing user accounts and assigning permissions.*

Managing lists *on page* ***48****: Information about how to manage lists.*

Chapter contents

Program blocking settings

Accessing the settings

- From the top menu, select **Settings**. From the side menu, select **Program blocking**.
- Click the **Add** button. The **Program blocking** settings page opens.

You can only assign program blocking settings to Windows workstations and servers.

Required permissions

Permission	Access type
Configure program blocking	Create, edit, delete, copy, or assign program blocking settings profiles.
View program blocking settings	View the program blocking settings profiles defined.

Table 16.1: Permissions required to access the program blocking settings

Program blocking settings options

To create a new settings profile or edit an existing profile, enter this information:

Field	Description
Names of the programs to block	Names of the executable files (EXE files) that you want Advanced EPDR to prevent from running. You can paste a list of file names separated by line breaks. Wildcards are not supported.
MD5 or SHA-256 codes of the programs to block	MD5 or SHA-256 codes of the executable files (EXE files) that you want Advanced EPDR to prevent from running. You can paste a list of MD5 or SHA-256 codes separated by line breaks.
Notify computer users about	Specify a custom message to notify users that the security solution blocked a file. The Advanced EPDR agent shows a pop-up message on user

Field	Description
blocked applications	computers when they try to run a blocked application.

Table 16.2: Configuring a program blocking security policy

Do not block operating system programs or components that are necessary to run user programs correctly.
Advanced EPDR does not block any of its programs or modules to make sure the security solution works correctly.

Program blocking module lists

Accessing the lists

You can access the lists in two ways:

- From the top menu, select **Status**. From the side menu, select **Security**. Click the relevant widget.

  Or,

- From the top menu, select **Status**. From the side menu, click the **Add** link. A dialog box opens that shows the available lists.
- From the **Activity control** section, select the **Programs blocked by the administrator** list to view the associated template. Edit it and click **Save**. The list is added to the side menu.

Required permissions

Permission	Access to lists
View detections and threats	Programs blocked by the administrator

Table 16.3: Permissions required to access the blocked program lists

Programs blocked by the administrator

This list shows details of the programs blocked by Advanced EPDR on workstations and servers.

Field	Description	Values
Computer	Computer name.	Character

Field	Description	Values
		string
Path	Path and name of the program blocked by the administrator on the user computer.	Character string
Date	Date when Advanced EPDR blocked the program.	Date

Table 16.4: Fields in the Programs Blocked by the Administrator list

*To view a graphical representation of the list data, go to the **Programs blocked by the administrator** widget.*

Fields displayed in the exported file

Field	Description	Values
Computer	Computer name.	Character string
Software	Name of the program blocked by the administrator on the user computer.	Character string
Path	Path and name of the program blocked by the administrator on the user computer.	Character string
Action	Action taken by Advanced EPDR.	"Blocked" character string
Date	Date when Advanced EPDR blocked the program.	Date
User	Operating system user account under which the blocked program was run.	Character string
MD5	MD5 hash of the program blocked by the administrator.	Character string
SHA-256	SHA-256 hash of the program blocked by the administrator.	Character string

Table 16.5: Fields in the Programs Blocked by the Administrator exported file

Filter tool

Field	Description	Values
Computer	Computer name.	Character string
Hash	MD5 or SHA-256 hash of the file you want to find.	Character string
Compromised program	Name of the program blocked by the administrator.	Character string
Dates	Narrow the scope of the data shown by time period.	• Last 24 hours • Last 7 hours • Last month

Table 16.6: Filters available in the Programs Blocked by the Administrator list

Blocked program details page

Click a row in the list to view detailed information about the blocked program.

Field	Description	Values
Blocked program	Name of the blocked file.	Character string
Computer	Name of the computer where the program was blocked, IP address, and group it belongs to.	Character string
Logged-in user	User account under which the blocked program tried to run.	Character string
Name	Name of the blocked file.	Character string
Path	Storage device and computer folder where the blocked program is located.	Character string
MD5	MD5 hash of the blocked program.	Character string
SHA-256	If included in the detection, SHA-256 hash of the blocked program.	Character string

Field	Description	Values
Detection date	Date the program was blocked.	Date

Table 16.7: Fields in the Blocked Program Details page

Program blocking module panels/widgets

Accessing the dashboard

From the top menu, select **Status**. From the side menu, select **Security**.

Required permissions

Permission	Access to widgets
View detections and threats	Programs blocked by the administrator

Table 16.8: Permissions required to access the program blocking widgets

Programs blocked by the administrator

This widget shows the number of execution attempts recorded across the IT network and blocked by Advanced EPDR based on the settings defined by the network administrator.

Advanced EPDR reports only one incident every 24 hours for each computer-hash pair found on the network.

Figure 16.1: Programs Blocked by the Administrator panel

Meaning of the data displayed

Data	Description
Blocked items	Number of execution attempts recorded across the IT network and blocked by Advanced EPDR in the specified period.

Table 16.9: Description of the data displayed in the Programs Blocked by the Administrator panel

Lists accessible from the panel

Figure 16.2: Hotspots in the Programs Blocked by the Administrator panel

Click the hotspots shown in **Figure 16.2:** to open the **Programs blocked by the administrator** list with these predefined filters:

Hotspot	Filter
(1)	No filter.

Table 16.10: Filters available in the Programs Blocked by the Administrator list

Chapter 17

Authorized software settings

In Hardening and Lock modes of the advanced protection, Advanced EPDR prevents the execution of programs that are unknown to the Cytomic intelligence until they are classified. This behavior could have drawbacks and create minor delays for users in very specific situations, even when the network administrator knows the source of the program and the reason why it has been blocked, for example:

- Specific niche programs with very few users.
- Programs that update automatically from the vendor's website without user interaction.
- Programs whose functions are distributed across hundreds of libraries which are loaded in memory and therefore blocked as and when they are used by the user from the program menus.
- Programs operating on a client-server model, where the client side is hosted on a shared network resource.
- Polymorphic software which dynamically generates executable files.

For more information about the Authorized software module, click the following links:

Creating and managing settings profiles *on page* ***294****: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*
Accessing, controlling, and monitoring the management console *on page* ***61****: Managing user accounts and assigning permissions.*
Advanced protection *on page* ***333****: Configuring Lock and Hardening modes.*

Chapter contents

Authorized software and exclusions

In Advanced EPDR, three features prevent program blocking:

- **Excluded files and paths**: Excludes specific items or areas on the computer from scans. Unknown software will not be prevented from running. Because this can lead to a security hole, we do not recommended this except where there are problems with computer performance. For more information, see **Files and paths excluded from scans** on page **331**.

  Only the folder in the specified path is excluded. Subfolders are not excluded.

- **Unblocking programs in the process of classification**: Temporarily allows blocked programs to run but with a reactive approach. You cannot unblock a program unless it has first been blocked. Because software can consist of several components, and you must unblock each component individually, the process to block and unblock can take some time.
- **Configure authorized software**: Proactive unblocking of unknown programs in the process of classification. This module is useful when advanced protection is in Lock or Hardening mode and finds an unknown program, preventing its use.

Authorized Software settings enable you to approve the execution of executable binary files, excluding script files, standalone DLLs, and other files. When Authorized Software allows a binary file to run, it also allows the execution of all the resources it uses, including all DLLs and other programs it might create or invoke. Advanced EPDR allows the execution of any file originating from an .MSI installer or self-extracting .EXE file approved by Authorized Software.

Software authorized by a partner

By default, you cannot edit or delete the **Authorized Software** settings inherited from a partner. The partner can configure the list of authorized software to be editable. The settings profile shows a label, **Editable Settings**. In this case, you can add authorized software but you cannot delete or edit the list of software defined by the partner.

If your partner changes the status of the settings from editable to non-editable, the authorized software you added will no longer apply. Only the software from the partner applies. If the partner changes the configuration again to be editable, then the authorized software you added is restored and applied.

Authorized software settings

Accessing the settings

- From the top menu, select **Settings**. From the side menu, select **Authorized software**.
- Click **Add**. The **Add settings** page opens.

You can assign authorized software settings to Windows servers or workstations only.

Required permissions

Permission	Access type
Configure authorized software	Create, edit, delete, copy, or assign authorized software settings profiles.
View authorized software settings	View the authorized software settings profiles defined.

Table 17.1: Permissions required to access the authorized software settings

How the Authorized Software module works

Network users can run unknown software which is in the process of classification provided you have permitted it by using an authorized software rule.

After a program has been analyzed, Advanced EPDR classifies the program as goodware or malware. If the program represents a threat, it is blocked regardless of whether it was authorized in these settings.

Authorized Software module settings

Authorized software settings consist of one or more rules, each of which refers to a single software component or a family of software that you want to allow to run before it is classified.

Creating an authorized software rule

Click the **Authorize programs** link to create a rule with this information. Then, click **Authorize**:

Field	Description
Name	Rule name.

Field	Description
MD5 or SHA-256	MD5 or SHA-256 hashes for the programs you want Advanced EPDR to allow to run. See section **Calculating the MD5 or SHA-256 hash of one or more files**.
Product name	Product name value from the header of the file you want to unblock. To view the product name, right-click the program file. Select **Properties**, **Details**.
File path	Path of the program on the server or workstation. System environment variables are accepted.
File name	The name of the file you want to unblock. Wildcards * and ? are accepted.
File version	Version from the header of the file you want to unblock. To view the version, right-click the program file. Select **Properties**, **Details**.
Signature	The digital signature of the file you want to unblock. See section **Getting the thumbprint of a signed program**.

Table 17.2: Configuring an authorized software rule

Deleting an authorized software rule

- Click the  icon next to the authorized software rule you want to delete.
- In the upper-right corner of the page, click **Save** to update the edited authorized software settings profile.

Editing an authorized software rule

- Click the name of an authorized software rule. The **Authorize programs** dialog box opens.
- Edit the rule properties. Click **Authorize**.
- In the upper-right corner of the page, click **Save**. The authorized software settings profile updates.

Copying an authorized software rule

- Click the  icon next to the authorized software rule you want to copy. The **Authorize programs** dialog box opens. The new rule name contains the name of the original rule with the prefix "Copy of".
- Edit the rule properties. Click **Authorize**.

- In the upper-right corner of the page, click **Save**. The authorized software settings profile updates.

Calculating the MD5 or SHA-256 hash of one or more files

There are many tools available to calculate the MD5 or SHA-256 hash of a file. This section describes how to use the PowerShell tool in Windows 10.

- In File Explorer, open the folder with the files. Select **File**, **Open Windows PowerShell**. A window with the command line opens.

Figure 17.1: Command line with the result of the Get-FileHas command

- Enter the following command and replace `$files` with the file path. Wildcards * and ? are accepted.

For MD5:

```
PS c:\folder> Get-FileHash -Algorithm md5 -path $files
```

For SHA-256:

```
PS c:\folder> Get-FileHash -Algorithm sha256 -path $files
```

- To copy the MD5 or SHA-256 hashes to the clipboard, press and hold the `Alt` key, and select the hashes with the mouse pointer. Press `Ctrl + C`.
- To paste all MD5 or SHA-256 hashes from the clipboard to the Advanced EPDR console, click the **MD5** or **SHA-256** field of the authorized software rule and press `Ctrl + V`.
- Click **Authorize**. In the upper-right corner of the page, click **Save**. The authorized software settings profile updates.

Getting the thumbprint of a signed program

- Open Windows PowerShell. Navigate to the directory where the program is located.
- Enter the following command and replace `$file` with the file path.

```
PS c:\folder> Get-AuthenticodeSignature -FilePath $file
```

- Select the character string returned by the command and press `Ctrl + C` to copy it to the clipboard.
- Click the **Signature** field of the authorized software rule and press the keys `Ctrl + V` to paste the thumbprint to the management console.
- Click **Authorize**. In the upper-right corner of the page, click **Save**. The authorized software settings profile updates.

Chapter 18

Detection and management of IOCs

IOC (Indicators of Compromise) is an industry standard that makes it possible to describe certain conditions on IT systems which, if met, could compromise the security of an organization. The concept is similar to that of a signature file, with the main difference being that the format is open. This enables collaboration and the exchanging of security intelligence and allows administrators to easily amplify the detection capabilities of Advanced EPDR.

This chapter describes the tools available in Advanced EPDR for importing and exporting IOCs, looking for IOCs on computers, and rapidly viewing the results.

For more information about the Authorized software module, click the following links:

***Creating and managing settings profiles** on page **294**: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*
***Accessing, controlling, and monitoring the management console** on page **61**: Managing user accounts and assigning permissions.*
***Advanced protection** on page **333**: Configuring Lock and Hardening modes.*

Chapter contents

IOC concepts

In order to understand the processes involved in the use of IOCs, it is useful to be familiar with concepts related to the technologies that support this industry standard.

IOC (Indicator of Compromise)

Indicators of Compromise are descriptions (or rules) of patterns of behavior that could indicate a cyberattack. Unlike a signature file, which has a similar purpose, IOCs have an open format that enables the exchange of security intelligence between the various players involved (vendors, consumers, users, etc.).

There are several standards for describing suspicious patterns of behavior, the most widespread of which is STIX.

STIX (Structured Threat Information Expression)

This is a JSON-based language which describes security threats in a structured and interrelated way for better readability and understanding. It is based on graphs that intuitively represent objects and their relationships.

Each IOC contains a number of entities and relationships that describe in detail an 'artifact' or indicator that identifies the attack: IP addresses or domains that could host C&C (Command & Control) servers, MD5 or SHA hashes of files suspected of containing viruses and other threats, etc.

STIX also enables you to leverage the information described in other formats, such as YARA rules.

Advanced EPDR is compatible with the STIX 2.x standard.

YARA (Yet Another Recursive Acronym)

YARA is a language based on rules that facilitates the creation of descriptions of malware families according to text or binary patterns. These rules consist of a set of strings and boolean expressions which determine their logic and are used in searches on files that are suspected of being infected.

An IOC can include only one YARA rule in its definition, although this rule can be as complex as is required to detect entire families of malware.

Other IOC formats

There are currently several IOC open formats for the exchange of security intelligence which provide similar features. These include OpenIOC and TAXII, among others. Additionally, an IOC format may contain versions that are not compatible with each other, as is the case with STIX 1.x and 2.x.

In order to reuse IOCs described in formats that are incompatible with Advanced EPDR, there are free tools that can make the required conversion in order to convert any IOC into one in STIX 2.x format.

Results generated from the search for IOCs

In order not to overload network computers, Advanced EPDR restricts the depth of complex searches for IOCs by applying the following rules:

- **For simple IOCs or IOCs with one YARA rule**: These look for a single attribute with a specific value. These IOCs return up to 10 results per computer, at which point the search stops.
- **For complex IOCs**: These look for several attributes or an attribute with several values. These IOCs return the first result found on each computer, at which point the search stops.

Given this restriction, the number of results displayed in the lists and widgets may not be complete, especially in the event of massive infections with many files affected on each computer on a network. In such cases, it is guaranteed that at least one result from each computer is displayed, without affecting performance.

IOC workflow

Follow this workflow to successfully identify indicators of compromise on your network:

- Check that the user account used to access the console has the required permissions. See section **IOC management** for more information.
- Import third-party IOCs or create them using the wizard. See section **IOC management** for more information.
- Create an IOC search task. See section **Searching for IOCs on the network** for more information.
- View the IOCs found in the results of the search task, through the list of IOCs, or with the widgets. See sections **Searching for IOCs on the network** and **IOCs dashboard/widgets** for more information.

IOC management

Accessing the IOC gallery

To access the IOC gallery, from the top menu, select **Settings**. From the side menu, select **IOC gallery**. A list appears that shows all imported IOCs.

Required permissions

To view and access the IOCs feature, the **Search for and manage IOCs** permission must be assigned to the user account role. For more information about this permission, see section **Search for and manage IOCs** on page **76**.

IOC search tasks are compatible with Windows computers.

IOC gallery

The IOC gallery shows a list of all IOCs imported or created with the wizard. For each IOC, this information is provided:

Field	Description	Values
Name	Name assigned to the IOC when it was created or imported.	Character string
Description	IOC description field.	Character string
Type	IOC status: • **STIX (Pending approval)**: IOC was imported from an external source and requires approval to update it to the format supported by Advanced EPDR. • **STIX**: IOC was imported from an external source and was approved for use by IOC searches in Advanced EPDR. • **Created by the user**: IOC was created through the web console wizard. It does not require approval to use in searches. For more information, see **Approving an imported IOC**.	Enumeration
Modified	Date the IOC was modified.	Date
Created	Date the IOC was created.	Date

Table 18.1: List of IOCs created or imported

Creating an IOC

- In the upper-right corner of the page, click **Add**. The **Add IOC** page opens.
- Enter a **Name**, **Author**, and **Description**.
- From the **Select a property** drop-down menu, select the attack feature you want to detect

- **File MD5**: Searches for a file with the specified MD5 hash.
- **File SHA-256**: Searches for a file with the specified SHA-256 hash.
- **File name**: Searches for a file with the specified name.
- **File path**: Searches for a file with the specified path.
- **Domain**: Searches for a network connection through TCP or UDP to or from the specified domain.
- **IPv4**: Searches for a TCP or UDP connection to or from the specified IPv4 address.
- **IPv6**: Searches for a TCP or UDP connection to or from the specified IPv6 address.
- **YARA rule**: Searches for a file with content that matches the pattern described in the YARA rule.

- **Select an operator**: Specify how you want to compare the properties found on the computer with the reference value you set in the IOC.
  - **In**: A property found on the computer must match at least one property value specified in the Value text box.
  - **Is equal to**: All properties found on the computer must match exactly the property values you specify in the Value text box.
- **Value**: Type a value for the property you selected.
  - To enter more than one value, type a value and then press **Enter**.
  - Wildcards are not supported.
- **New condition**: Add more conditions to the rule. You can apply logical operators AND/OR.

Logical operators

To combine two or more conditions in the same rule, use the logical Boolean operators AND and OR. When you add two or more conditions to a rule, a drop-down menu appears with available operators. Operators apply to the adjacent conditions.

Rule condition groupings

In a logical expression, parentheses alter the order in which operators that relate rule conditions are evaluated.

To group two or more conditions in parentheses, you must create a group. A gray line connects the rules that are part of the grouping.

Parentheses enable you to group operators at different levels in a logical expression.

Conditions for using YARA rules

An IOC cannot include more than one YARA rule. If you add a YARA rule to an empty IOC,you cannot use other properties. Similarly, if you add other properties to an IOC, the YARA rules are disabled.

If a rule does not comply with the YARA syntax, an error message appears and you cannot save the IOC.

Copying an IOC

To copy an IOC from the **IOC gallery** list:

- Click the ⋮ icon. A context menu opens.
- Select the **Make a copy** option. The **Edit IOC** dialog box opens and shows the same data as the original IOC except for:
- **Name**: Shows the same name as the original IOC, preceded by the "Copy of" text string.
- **ID**: This is not shown. A new **ID** is automatically generated when you save the IOC.

Deleting an IOC

You cannot delete IOCs that are part of a task that is in progress. If you try to do so, an error message appears.

Deleting a single IOC

In the row of the IOC you want to delete, click the context menu icon and select **Delete**. The IOC is deleted from the list. When you delete an IOC, historical data for the IOC remains in the **Detected IOCs** list and **IOCs** dashboard.

Deleting multiple IOCs

- In the IOC list, select the checkbox for each IOC you want to delete.
- Click the drop-down menu icon. Click **Delete**. The **Delete** option also appears in the toolbar at the top of the page.

When you delete multiple IOCs, historical data for the IOC remains in the **Detected IOCs** list and **IOCs** dashboard.

Importing and exporting IOCs

You cannot import an IOC that has the same ID as another IOC that is part of a search task that is in progress. If you try to do so, an error message appears.

Importing an IOC

To import an IOC:

- In the upper-right corner of the page, click  . The Import dialog box opens.
- Click **Select file**. Select a file. Compatible files are in STIX, YARA, or comma-separated value format.
- Click **Import**. The IOC is added to the IOC gallery.
- If an IOC in the import file already exists, you select to:
    - **Replace**: Replaces the existing IOC with the new one.
    - **Ignore**: Ignores the new IOC and keeps the existing one.

Approving an imported IOC

IOCs imported from an external source require an additional step before a search task can use them. This is necessary to make sure that Advanced EPDR can interpret the IOC correctly, because not all entities supported by the STIX 2.x specification are considered when you run a search.

After the IOC has been imported, follow these steps:

- IOCs that require approval display as **STIX (Pending approval)** in the **Type** column of the list.
- Select the IOC you want to approve. The **Edit IOC** dialog box opens.
- If there is a rule in the IOC that Advanced EPDR cannot interpret, a red box appears that reports the situation. The data shown on the edit page corresponds to the sections of the IOC that Advanced EPDR interprets correctly.
- If the rules shown are correct, click **Approve search statement and save** to use the IOC in search tasks.

Advanced EPDR deletes rules in an imported IOC only when running a search task. However, the complete IOC is stored on the Cytomic server and you can see its entities and relationships as well as the original source code.

Exporting a single IOC

- In the row of the IOC you want to export, click . A drop-down menu opens.
- Select **Export**. A JSON file with the IOC definition downloads to your computer.

Exporting multiple IOCs

- Select the checkbox for each IOC you want to export.
- In the toolbar, click **Export**. A JSON file with the IOC definitions downloads to your computer..

Viewing imported IOCs

Graphical representation of an IOC

Click the context menu of an IOC. Select **View original STIX file**. The **STIX file** page opens with a graphical representation and the code of the IOC.

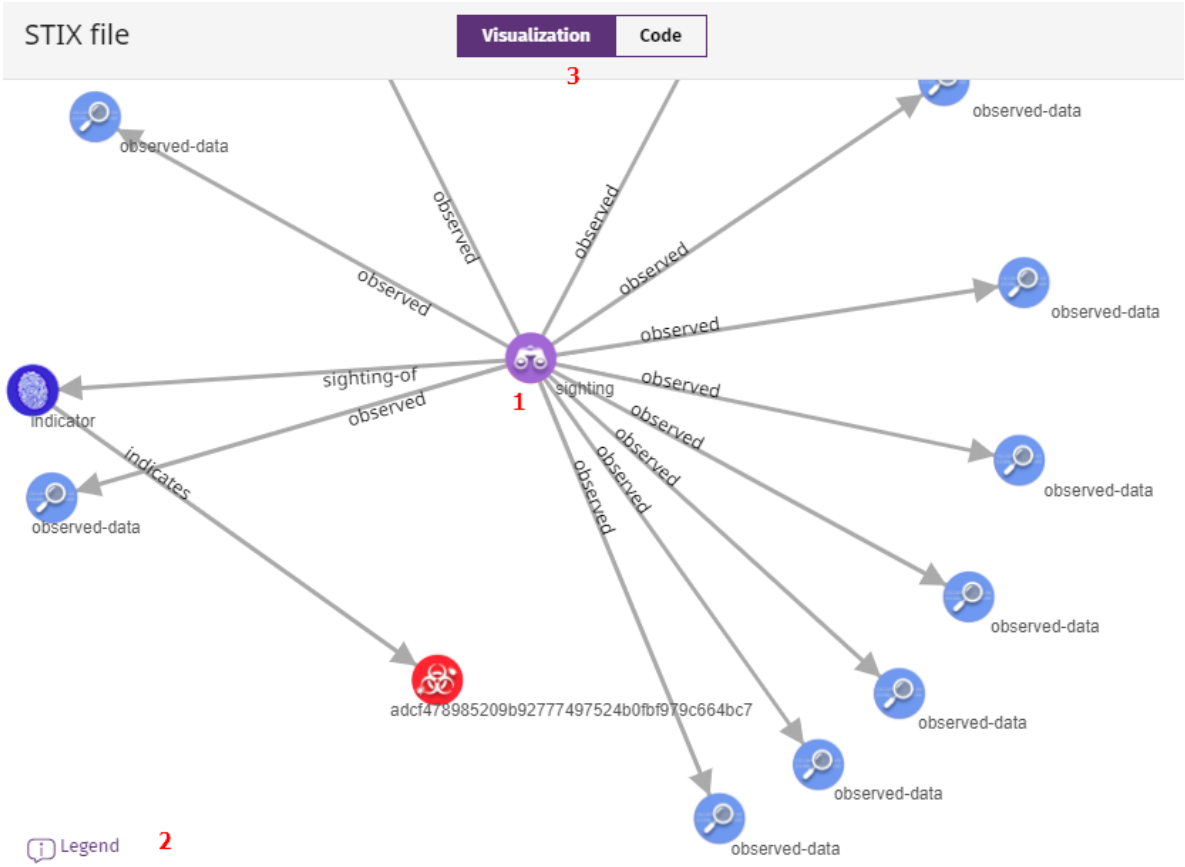


Figure 18.1: Graphical representation of an IOC

In the **STIX file** window, you can:

- Click and drag items in the diagram **(1)**.
- Click **Legend (3)** to view an explanation of each icon in the graph.
- Click **Visualization** and **Code (3)** to review the graphical representation or a code definition of the IOC. The IOC code appears in tab format. You can copy the IOC code to the clipboard.

> *Although the IOC code displays as it was imported, Advanced EPDR might omit sections that are not compatible with its implementation. Search results might not show as expected*

Filtering imported IOCs

To filter items in the IOC list, use the search bar in the **IOC gallery**. Enter the name or description of an IOC to show only items from the list that meet the search criteria.

Searching for IOCs on the network

IOC search tasks are compatible with Windows computers.

Advanced EPDR enables you to use its task engine to configure and run IOC searches on the computers on your network. You can access this engine from the **IOC gallery**, or from the **Tasks** page. For more information about how to manage tasks in Advanced EPDR, see **Tasks** on page **909**.

Permissions required to manage Detect IOCs tasks

To manage **Detect IOCs** tasks, the user account used to access the web console must have the **Search for and manage IOCs** permission assigned to its role. For more information about the permission system, see **Understanding permissions** on page **72**.

Accessing the IOC search

You can perform searches only with approved IOCs.

From the Tasks page

- From the top menu, select **Tasks**. Click **Add task**. Select **Search for IOCs**.

From the IOC gallery

- In the top menu, select **Settings**. From the side menu, select **IOC gallery**.
- Select the checkboxes for the IOC or group of IOCs you want to search for.
- To search for IOCs, if you have selected a single item, click the computer context menu and select **Search for IOCs**. If you have selected more than one IOC, select **Search for IOCs** in the toolbar above. A new IOC search task is created. For more information about how to configure it, see **Configuring an IOC search task**.

Configuring an IOC search task

- Enter general details about the task in the **Name** and **Description** fields.
- In **Recipients**, click the **No recipients selected** link. A page opens where you can select the computers and devices to search.
- Select the types of computers to search: **Workstation**, **Laptop**, or **Server**.
- Click ⊕ to add individual computers or computer groups. Click 🗑 to remove them.
- Click **View computers** to review a list of the computers that will receive the task..
- Select when the task will start:
  - **Starts:** Specify the task start date/time.

Value	Description
As soon as possible (selected)	To start the task as soon as possible within the time interval selected. The computer must be turned on and accessible from the cloud.
As soon as possible (cleared)	The task runs on the date selected in the calendar. Specify whether the time is based on the computer local time or the Advanced EPDR server time.
If the computer is turned off	If the computer is turned off or cannot be accessed, the task will not run. You can specify the task expiration time, from 0 (the task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available). • **Do not run:** The task is immediately canceled if the computer is not available at the selected time. • **Run the task as soon as possible, within:** Specify a time interval during which the task will run if the computer becomes available. • **Run when the computer is turned on:** There is no time limit. The solution waits indefinitely for the computer to be available to run the task.

Table 18.2: Task launch parameters

  - **Maximum run time**: Select how long to retain the task when the computer is off or not available. After that time, the task is canceled returning an error.

Value	Description
No limit	There is no time limit for the task to complete.
1, 2, 8, or 24 hours	There is a time limit for the task to complete. After that time, if the task has not finished, it is canceled returning an error.

Table 18.3: Task duration parameters

- Click **Save**. The task is added to the list of configured tasks. The status shows as **Unpublished** and it is not yet active.
- To publish a task, click the **Publish** button. The task is added to the Advanced EPDR task scheduler, which runs it based on its settings.

IOC search task priority

Task	Behavior
Detection of IOCs	Waits for the search task in progress to finish and then the new task runs.
Patch installation	Runs concurrently with the patch installation task. The patch installation task is not interrupted as this could represent a risk for the integrity of the system.
Scan or disinfection	The scan or disinfection task is canceled and the IOC search task runs. Scan or disinfection tasks created when there is an IOC search task running are not run until the IOC search task is complete.
Cytomic Data Watch search	Runs and does not cancel or stop the Cytomic Data Watch task.
Cytomic Data Watch indexing	Runs and temporarily stops the Cytomic Data Watch task.

Table 18.4: Priority order when you run IOC search tasks

IOC search task behavior with respect to system restarts

IOC search tasks are automatically canceled and restarted (if possible) on user computers when:

- The administrator requests a restart of the computer from the web console.
- The client user requests a restart of the computer locally from the computer.

- The computer restarts automatically to update any components of the installed security software.

Behavior if you manually stop the IOC search task

If you manually stop the IOC search task from the web console, then:

- The IOC search stops as soon as possible on the target computer.
- Detection results up until the time of cancellation are recorded

Lists of found IOCs

Accessing the lists

To access the complete list of all found IOCs:

- In the top menu, click **Status**. Click the **Add** link from the side menu.
- Select the **Detected IOCs** list in the **Security** section.

To access the list for a specific IOC:

- In the top menu, click **Settings**. Click **IOC gallery**.
- Click the ⋮ icon located to the right of the relevant IOC to open its context menu.
- Select **View IOC detections**. The **Detected IOCs** list opens, filtered by the selected IOC.

To view the list of detected IOCs associated with a search task:

- Click **Tasks** in the top menu. A list appears with all created tasks.
- Find the relevant **IOC search** task and click the **View results** link.

Required permissions

To view and access lists related to IOCs, it is necessary for the **Search for and manage IOCs** permission to be assigned to the user account role.

IOCs found in a search task

Field	Description	Values
Computer	Name of the computer with the IOC.	Character string.
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
Status	Task status.	• Pending

Field	Description	Values
		• In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Detected IOCs	Number of IOCs detected on the computer.	Character string
Start date	Date and time the task started.	Date
End date	Date the task ended.	Date

Table 18.5: IOC search results list

Fields in the View detected IOCs list

When you view the results of an IOC search, in the upper-right corner of the page there is the option **View detected IOCs**. Click this link to display the complete list of IOCs found by the search task.

Field	Description	Values
Computer	Name of the computer where the IOC was detected.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
Detected IOC name	Name of the IOC found on the computer.	Character string
Detected IOC description	Description assigned by the administrator when registering the IOC.	Character string

Field	Description	Values
Date	Date when the IOC was detected on the computer.	Date

Table 18.6: Fields in the View detected IOCs list

Filter tool

Field	Description	Values
Status	Task status.	• All statuses • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Detections	Result of the search for IOCs.	• All • No detections • With detections

Table 18.7: Filter tools

Detected IOCs

Shows all IOCs found on the computers on your network by all the IOC search tasks executed. If a task identifies the same IOC more than once on a computer, the duplicate results are deleted.

Field	Description	Value
Computer	Name of the computer where the IOC was detected.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string

Field	Description	Value
Task	Name of the task that detected the IOC.	Character string
IOC name	Detected IOC name.	Character string
Detection date	Date the IOC was detected.	Date

Table 18.8: Fields in the Detected IOCs list

*To see a graphical representation of the list data, go to the **Most detected IOCs** widget.*

Fields displayed in the exported file

Field	Description	Value
Client	Name of the customer account.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer where the IOC was detected.	Character string
IOC name	Detected IOC name.	Character string
IOC description	Description of the IOC found on the computer.	Character string
IOC ID	Internal ID of the IOC. It matches the content of the `id` field in the JSON file.	Character string
Task	Name of the task that detected the IOC.	Character string
Date	Date the IOC search task was run.	Date

Field	Description	Value
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
IP address	IP address of the computer where the IOC was detected.	IP address
Domain	Domain of the computer where the IOC was detected.	Character string
Description	Description of the IOC found on the computer.	Character string

Table 18.9: Fields in the exported table

Fields displayed in the detailed Excel export file

Field	Description	Value
Client	Name of the customer account.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer where the IOC was detected.	Character string
IOC name	Detected IOC name.	Character string
IOC description	Description of the IOC found on the computer.	Character string
IOC ID	Internal ID of the IOC. It matches the content of the `id` field in the JSON file.	Character string
Task	Name of the task that detected the IOC.	Character string
Date	Date the IOC search task was run.	Date
Group	Folder within the Advanced EPDR folder tree the	Character string

Field	Description	Value
	computer belongs to.	
IP address	IP address of the computer where the IOC was detected.	IP address
Domain	Domain of the computer where the IOC was detected.	Character string
Description	Description of the IOC found on the computer.	Character string
Detected item	Identifies the items defined in the IOC that have been detected on the computer.	• Name, path, and hash of the file • IP address and port • Domain and port

Table 18.10: Fields displayed in the detailed Excel export file

Filter tools

Field	Description	Value
Dates	Date the IOC was detected.	• Last 24 hours • Last 7 hours • Last month • Custom range
Computer type	Type of device the IOCs were detected on.	• Workstation • Laptop • Server

Table 18.11: Filters available in the Detected IOCs list

Detected IOC page

Click any of the rows in the list to open the **Detected IOC** page with detailed information.

Field	Description	Values
Name	Detected IOC name.	Character string
Detection date	Date the IOC was detected.	Date
Computer	Name of the computer where the IOC was detected.	Character string
Identifier	Internal ID of the IOC. It matches the content of the `id` field in the JSON file.	Character string
Description	Description assigned to the IOC.	Character string
Pattern (STIX)	Attribute and value of the STIX definition used to find the potential threat.	Character string
Modified	Date the IOC was modified.	Date
Created	Date the IOC was created.	Date
Detected items	Identifies the items defined in the IOC that have been detected on the computer.	• Name, path, and hash of the file • IP address and port • Domain and port

Table 18.12: Fields in the Detected IOC page

IOCs dashboard/widgets

Accessing the dashboard

To access the IOCs dashboard, click **Status** in the top menu. Click **IOCs** in the side panel.

Required permissions

To access the IOCs dashboard, it is necessary for the **Search for and manage IOCs** permission to be assigned to the user account role.

Last IOC search tasks

Shows a list of the last IOC search tasks created. This widget comprises several links that enable you to manage the IOC search tasks on a customer's network:

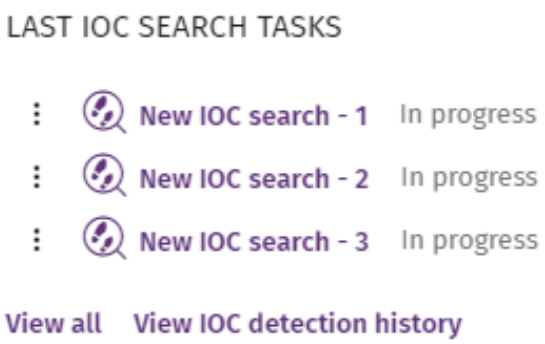


Figure 18.2: Last IOC search tasks widget

- Click a task to edit its settings.
- Click the **View all** link to go to the list of IOC tasks.
- Click **View IOC detection history** to access the **Detected IOCs** list with all completed detection tasks (failed and successful).
- Click the context menu icon in each task to see the task results.

Most detected IOCs

Shows a graph with the IOCs detected on the computers on the network during the selected time period. The results are presented in a treemap chart.

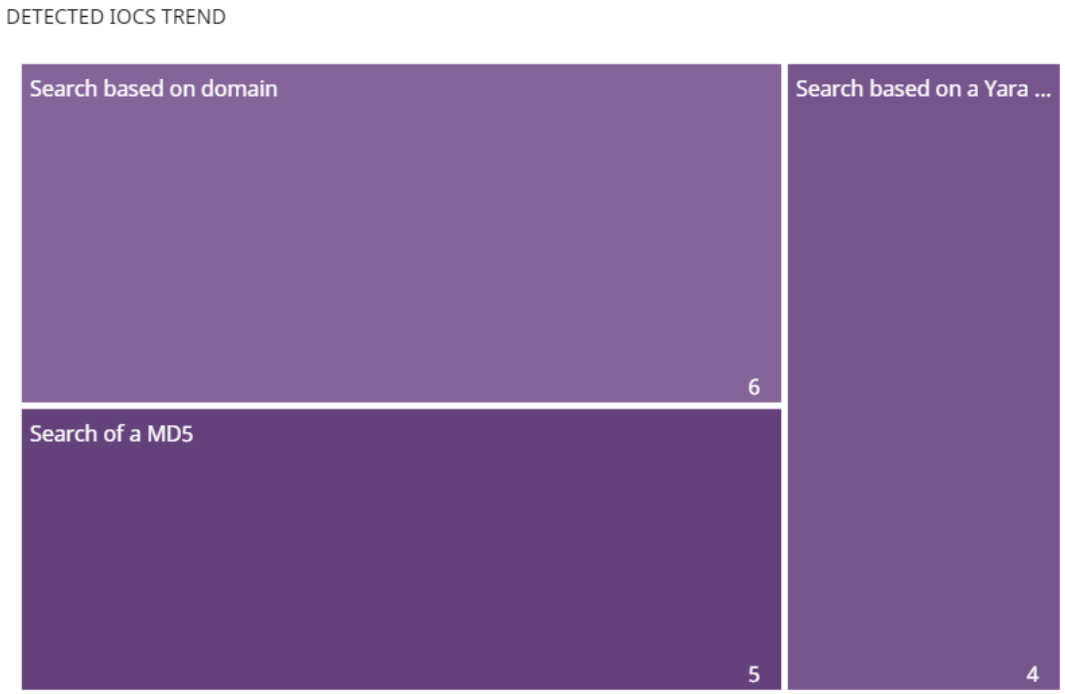


Figure 18.3: Most detected IOCs widget

Meaning of the data displayed

Data	Description
IOC name	Detected IOC name. The rectangle has a surface area which is proportionate to the number of times that the specific IOC has been detected as a percentage of all IOCs detected on the customer's network.
Number of detections	Number of computers on which each IOC has been found. Search tasks identify each IOC only once on each computer.

Table 18.13: Description of the data displayed in the Most detected IOCs panel

Lists accessible from the panel

Click the rectangles shown in figure **Figure 18.2:** to open the **Detected IOCs** list filtered by the selected IOC.

Detected IOCs trend

Shows a line graph illustrating the number of IOCs detected over time.

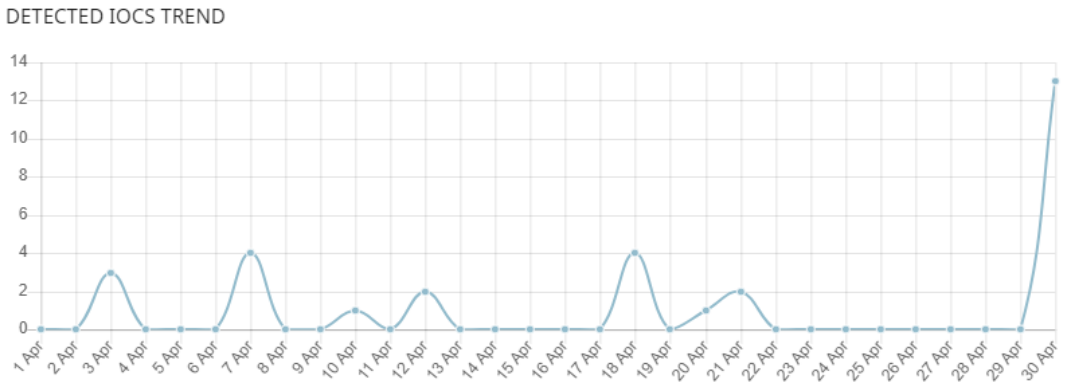


Figure 18.4: Detectec IOCs trend panel

Meaning of the data displayed

Data	Description
Data	Graphical representation of the number of IOC detections.
Y axis	Number of IOCs detected.
X axis	Date of the IOC detections.

Table 18.14: Description of the data displayed in the Detectec IOCs trend panel

Lists accessible from the panel

Click the data points on the chart in **Table 18.5:** to open the **Detected IOCs** list filtered by the selected date.

Chapter 19

Indicators of attack settings

In cyberattacks that target companies, hackers try to break through security defenses by deploying a series of coordinated actions. These actions take place over long periods of time and use multiple strategies and infection vectors. Many such actions may appear innocuous individually but, taken as a whole, they can be part of an ongoing cyberattack.

The Advanced EPDR basic user license includes a cross-threat hunting service. This service inspects the data flow sent by the security software installed on a customer computers by using advanced automated analysis technologies to identify indicators of attacks in progress. Finally, a team of specialists (hunters) sift through these indicators which are represented on the administrator console as IOA (Indicators of Attack) detections.

An IOA detection is an indicator shown on the Advanced EPDR administrator console when a pattern of events likely to belong to a cyberattack is detected. It could therefore act as an early warning of an infection, alerting the administrator to a potential attack in progress, though it could also be an alert of a cyberattack that has managed to penetrate the company defenses.

Because the existence of an IOA detection can reveal the existence of an imminent danger, Advanced EPDR enables the launching of an automatic response to minimize the attack surface.

For more information about the indicators of attack module, see:

Creating and managing settings profiles *on page* ***294****: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*
The management console *on page* ***35****: Information about how to manage user accounts and assign permissions.*
Managing lists *on page* ***48****: Information about how to manage lists.*

Chapter contents

Introduction to IOA concepts

This section details the concepts that you must know to understand the processes involved in the detection of IOAs, and in the execution of remedial actions (automatic and manual).

Event

An action executed by a process on a user computer and monitored by Advanced EPDR. Events are sent to the Cytomic cloud in real time as part of the telemetry. Automated analysis advanced technologies, analysts, and threat hunters analyze them in their context to determine whether they could be part of the Cyber Kill Chain (CKC) of a cyberattack.

Indicator

A sequence of unusual actions found in the events generated on a customer computer and which could be part of an early-stage cyberattack.

Indicator of attack (IOA)

An indicator that is highly likely to be a cyberattack. These are generally attacks in early stages or in exploit phase. These attacks do not normally use malware, as adversaries usually exploit the operating system own tools to execute the attack and thereby hide the traces of their activity. We recommend that you contain or remedy attacks as soon as possible.

To help manage IOA detections, Advanced EPDR gives each one a status which can be manually edited by you:

- **Pending**: The detection is pending investigation and/or resolution. You must verify whether the attack is real and take the necessary measures to mitigate it. All new detections are generated with the status 'Pending'.
- **Archived**: The detection was investigated and the remedial actions were taken, or were unnecessary because it was a false positive. You closed the detection.

Advanced EPDR shows relevant detection information, such as the MITRE tactic and technique used, the events recorded on the computer that generated the detection, and, if available, these reports:

- **Advanced attack investigation**: Includes information about the computer involved, a detailed description of the tactics and techniques used, recommendations to mitigate the attack, and the sequence of events that triggered the detection. See **Fields on the IOA Details page**.
- **Attack graph**: Includes an interactive diagram that shows the sequence of events that triggered the detection. See **Graphs**.
- **Investigation**: Opens the investigation console to show all the telemetry collected on the computer at the time the detection occurred. To make searches easier, the management console shows the latest event that generated the IOA detection. You can review events generated up to five days before the detection occurred, on the day the detection occurred, and one day after it.

Advanced indicators of attack

Advanced indicators of attack provide in-depth monitoring of the applications on your computers, detect suspicious behavior, and determine whether the event is an IOA.

The mere presence of this type of detection does not mean that an attack is taking place. You must analyze the advanced indicator of attack to determine whether it is an attack or not.

Advanced EPDR shows relevant information about advanced IOA detections, such as the MITRE tactic and technique used, the fields in the event recorded on the computer that generated the detection, and these reports:

- **Investigation**: Opens the investigation console to show all the telemetry collected on the computer at the time the detection occurred. To make searches easier, the management console shows the latest event that generated the advanced IOA detection. You can review events generated up to five days before the detection occurred, on the day the detection occurred, and one day after it.
- **Activity**: Shows a list of the events that triggered the advanced IOA detection.

Advanced indicators of attack are compatible only with Windows computers.

Grouped advanced indicators of attack

Grouped advanced indicators group together indicators that have the same tactic (see **Tactic (Why)**). They behave exactly the way advanced indicators of attack do, except for:

- When you review the details of a grouped IOA, the information shown refers only to the tactic. See **Information associated with IOAs**
- All the IOAs that make up a grouped IOA have the same tactic. There are 14 grouped advanced IOAs, one for each tactic available in the MITRE ATT&CK framework.

This is a list of all grouped advanced IOAs supported in the management console:

Tactic	Name	Description	Severity
TA0001	Initial Access	The adversary is trying to get into your network.	Medium
TA0002	Execution	The adversary is trying to run malicious code.	Medium
TA0003	Persistence	The adversary is trying to maintain their foothold.	Medium
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.	Medium
TA0005	Defense Evasion	The adversary is trying to avoid being detected.	Medium
TA0006	Credential Access	The adversary is trying to steal account names and passwords.	Medium
TA0007	Discovery	The adversary is trying to figure out your environment.	Medium
TA0008	Lateral Movement	The adversary is trying to move through your environment.	Medium
TA0009	Collection	The adversary is trying to gather data of interest to their goal.	Medium
TA0010	Exfiltration	The adversary is trying to steal data.	Medium
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.	Medium
TA0012	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.	Medium
TA0013	Resource Development	The adversary is trying to establish resources they can use to support	Medium

Tactic	Name	Description	Severity
		operations.	
TA0014	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.	Medium

Table 19.1: List of available grouped advanced indicators of attack

Compatibility of advanced IOAs with third-party security solutions

Cytomic follows all standards recommended by OS manufacturers to make sure its security products are compatible with other antivirus and EDR solutions. Advanced IOAs are implemented with hooks. If multiple security solutions that use this interception technology exist on a computer, there might be compatibility issues. We recommend that you enable only one hook-based technology on user computers.

In Advanced EPDR, the technologies that use hooks are:

- Anti-exploit protection. See **Anti-exploit** on page **338**.
- Advanced code injection. See **Anti-exploit** on page **338**.
- Advanced IOAs.

CKC (Cyber Kill Chain)

In 2011, Lockheed-Martin drafted a framework or model for defending computer networks. This framework stated that cyberattacks occur in phases and each of them can be interrupted through certain controls. Since then, the Cyber Kill Chain (CKC) has been adopted by IT security organizations to define the phases of cyberattacks. These phases range from remote reconnaissance of the target assets to data exfiltration.

MITRE Corporation

The MITRE Corporation is a not-for-profit company that operates federally-funded Research and Development centers to address security issues. It offers practical solutions in the fields of defense and intelligence, aviation, civil systems, national security, judiciary, health, and cybersecurity. The MITRE Corporation is the creator of the MITRE ATT&CK framework.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a set of resources developed by the MITRE Corporation to describe and categorize cybercriminal activities based on observations from around the world. ATT&CK is a structured list of known attack behaviors categorized into tactics and techniques and shown as a matrix. The MITRE ATT&CK matrix is a useful

resource to develop defensive, preventive, and remedial strategies for organizations. For more information about the ATT&CK matrix, go to **https://attack.mitre.org/**.

Technique (How)

In ATT&CK terminology, techniques represent the method (or the strategy) that an adversary uses to achieve a tactical objective. In other words, the 'how'. For example, to access credentials (tactic), an adversary executes a data dump (technique).

Sub-Technique (How)

In ATT&CK terminology, sub-techniques represent the "how" of a specific technique. They refer to the processes or mechanisms used by adversaries to achieve the objective of a tactic. For example, password spraying is a type of brute force attack to accomplish the objective of the Credential Access tactic.

Tactic (Why)

In ATT&CK terminology, tactics represent the ultimate motive or goal of a technique. It is the tactical objective of the adversary: the reason to take an action.

Managing indicators of attack detections

To create, edit, or delete settings profiles or resources associated with indicators of attack, the user account that accesses the Advanced EPDR console requires the ***Configure indicators of attack (IOA)*** *permission. To list settings profiles or resources associated with indicators of attack, you require the* ***View indicators of attack (IOA) settings*** *permission. See* ***Managing roles and permissions*** *on page* ***69***

Advanced EPDR enables you to manage indicators of attack detections and show computers on your network where indicators of attack were detected:

- **Showing IOA detections on the network**
- **Searching for computers where a specific IOA was detected**
- **Searching for IOA detections for a computer**
- **Searching for interrelated computers and IOAs**
- **Archiving one or more IOA detections**
- **Marking IOA detections as pending**
- **Showing a detection details and recommendations**

Showing IOA detections on the network

- From the top menu, select **Status**. From the side menu, select **Indicators of attack (IOA)**.
- At the top of the page, select the time period for which you want to show data.
- The **Threat Hunting Service** widget shows the events, indicators, and indicators of attack detected during the selected time period.
- Click the **Indicators of attack** area. The **Indicators of attack (IOA)** list opens and shows all IOAs detected during the selected time period.

For more information about this widget, see **Threat Hunting Service**.

Searching for computers where a specific IOA was detected

- From the top menu, select **Status**. From the side menu, select **Indicators of attack (IOA)**.
- In the **Detected indicators of attack (IOA)** or **Indicators of attack (IOA) mapped to the MITRE ATT&CK matrix** panel, click a type of IOA.
- The **Indicators of attack (IOA)** list opens filtered by the selected type of attack.

For more information about these widgets, see **Indicators of attack (IOA) mapped to the MITRE ATT&CK matrix** and **Indicators of attack (IOA)**.

Searching for IOA detections for a computer

- From the top menu, select **Status**. From the side menu, select **Indicators of attack (IOA)**.
- In the **Indicators of attack (IOA) by computer** panel, select a computer. The **Indicators of attack (IOA)** list opens filtered by the selected computer.

For more information about this widget, see **Indicators of attack (IOA) by computer**.

Searching for interrelated computers and IOAs

- From the top menu, select **Status**.
- From the side menu, click **Add**. A dialog box opens that shows all available lists.
- In the **Security** section, select **Indicators of attack (IOA)**. The **New list: Indicators of attack (IOA)** page opens.
- Each detection that appears in the **Indicators of attack (IOA)** list has a context menu with these options:
    - **View the IOAs detected on this computer** : Shows the **Indicators of attack (IOA)** list filtered by the **Computer** field.

- **View computers on which this IOA was detected** : Shows the **Indicators of attack (IOA)** list filtered by the **Indicator of attack** field.

For more information about these lists, see **Indicators of Attack (IOA) module lists**.

Archiving one or more IOA detections

When the cause for a detection is resolved, or the detection is a false positive, you can archive it:

- From the top menu, select **Status**. From the side menu, in **My lists**, click the **Add** link. The **Add list** dialog box opens and shows the available templates.
- In the **Security** section, select the **Indicators of attack (IOA)** template. The list of IOAs detected opens with no filters applied.
- Set the required filters and click the **Filter** button.
- Click the context menu for the detection you want to archive. Select **Archive IOA** . The detection status changes to **Archived**.

Or:

- Select the checkboxes for the detections you want to archive.
- In the toolbar, click **Archive IOA** . The detection status changes to **Archived**.

Marking IOA detections as pending

Advanced EPDR marks the detections it adds as pending to indicate they require attention. Additionally, when you have not analyzed or resolved the cause of a detection, you can mark it as pending further review. You can also change an archived detection to pending.

- From the top menu, select **Status**. From the side menu, in **My lists**, click the **Add** link. The **Add list** dialog box opens and shows the available templates.
- In the **Security** section, select the **Indicators of attack (IOA)** template. The list opens with no filters applied.
- Set the required filters and click the **Filter** button.
- Click the context menu for the detection you want to investigate. Select **Mark IOA as pending** . The status of the indicator of attack changes to **Pending**.

Or:

- Select the checkboxes for the detections you want to investigate.
- In the toolbar, click **Mark IOA as pending** . The detection status changes to **Pending**.

Showing a detection details and recommendations

- From the top menu, select **Status**. From the side menu, in **My lists**, click the **Add** link. The **Add list** dialog box opens and shows the available templates.
- In the **Security** section, select the **Indicators of attack (IOA)** template. The list opens with no filters applied.
- Set the required filters and click the **Filter** button.
- From the list, select an indicator of attack. The **Details** page opens. See **Details page**.

Detection and protection against RDP attacks

Among the cyberattacks that target companies, RDP brute force attacks are the most frequently used by adversaries, especially where systems are directly exposed to the Internet. Advanced EPDR detects and protects network computers against attacks that use the RDP (Remote Desktop Protocol) as an infection vector.

Using the RDP protocol, users connect to remote computers and run processes that enable them to use resources on another computer. In the case of non-legitimate users, this protocol can also be used to facilitate lateral movements within a corporate network and access other resources hosted on the IT infrastructure.

When you enable the RDP attacks toggle in the settings profile (see **Enabling and modifying IOA detection** on page **621**), Advanced EPDR executes these actions on the recipient computers:

- Logs remote access attempts via RDP on each protected computer over the last 24 hours, which originated outside the customer network.
- Determines whether the computer is subject to an RDP brute force attack.
- Detects if any of the computer accounts have already been compromised to access resources on the system.
- Blocks RDP connections to mitigate the attack.

IOA detection associated with an RDP attack

When a computer receives a large number of RDP connection attempts that try to initiate a remote session but fail due to invalid credentials, Advanced EPDR generates a **Brute-force attack against RDP** detection.

RDP containment modes

Initial RDP attack containment mode

When a computer protected by Advanced EPDR receives a large number of RDP connection attempts that fail due to invalid credentials, the security software generates a **Brute-force attack against RDP** IOA and puts the computer into **Initial RDP attack containment** mode. In this mode, RDP

access to the computer is blocked from IPs outside the customer network that have sent a large number of connection attempts over the last 24 hours. To allow access by one or more of these IPs, use the **Trusted IPs** list in the **Indicators of attack (IOA)** settings. See **Trusted IPs**.

Restrictive RDP attack containment mode

When the attacker is able to successfully log in to an account that previously failed due to invalid credentials, the computer in **Initial RDP attack containment** mode moves to the **Restrictive RDP attack containment** mode. The security software generates a **Credentials compromised after brute-force attack on RDP** IOA. The account is considered to be compromised. All external RDP connections that have tried to connect at least once with the target computer in the previous 24 hours are blocked.

Configuring the response to an RDP attack

When Advanced EPDR detects an RDP attack or intrusion, there are two response options: report only, or report and block the attack.

To configure the response to an RDP attack:

- In the **Indicators of attack** settings profile assigned to the computer, click the **Advanced settings** link in the **RDP attacks** section. The settings options associated with this IOA appear.
- Select the required option from **Response on workstations** and/or **Response on servers**:
    - **Report and block RDP attacks**: Advanced EPDR generates a **Brute-force attack against RDP** detection in the console and puts the attacked computer into the appropriate containment mode.
    - **Report only**: Advanced EPDR only generates a **Brute-force attack against RDP** detection in the console.

For more information, see **Indicators of attack (IOA) settings options**.

Finding network computers in RDP attack containment mode

You can use these resources to find computers in containment mode:

- The **XX computers in RDP attack containment mode** list in the **Threat hunting service** widget. See **Threat Hunting Service**.
- The filters available in the **Computer protection status** list. See **Computer protection status** on page **683**.
- The **Computer protection status** exported file. See **Computer protection status** on page **683**.
- A computer tree filter. See **Filter computers in RDP attack containment mode** on page **221**.

Viewing a computer containment status

The console shows the containment status of computers through these resources:

- The **Computer protection status** list, through the  icon. See **Computer protection status** on page **683**.
- The **Computer protection status** exported list, in the **RDP attack containment mode** column. See **Computer protection status** on page **683**.
- The **Encryption status** list, through the  icon. See **Encryption status** on page **563**
- The **Encryption status** exported list, in the **RDP attack containment mode** column. See **Encryption status** on page **563**
- The **Patch management status** list, through the  icon. See **Patch management status** on page **478**.
- The **Patch management status** exported list, in the **RDP attack containment mode** column. See **Patch management status** on page **478**.
- The **Data Control status** list, through the  icon. See **Cytomic Data Watch status** on page **409**.
- The **Data Control status** exported list, in the **RDP attack containment mode** column. See **Cytomic Data Watch status** on page **409**.
- The **Computers** list, through the  icon. See **Computers list** on page **228**.
- The **Computers** exported list, in the **RDP attack containment mode** column. See **Computers list** on page **228**.
- The **Indicators of attack (IOA)** list, in the **Action** column. See **Indicators of attack (IOA)**.
- The **Indicators of attack (IOA)** exported list, in the **Action** column. See **Indicators of attack (IOA)**.
- The alerts on the **Computer details** page. See **Computers in containment mode** on page **257**.
- The **IOA details** page, in the **Computer** field. See **Details page**.

Automatic termination of RDP attack containment mode

Twenty-four hours after containment mode begins, Advanced EPDR evaluates the number of connection attempts via RDP. If it is below default threshold, Advanced EPDR automatically ends RDP attack containment mode. If the attempts continue, then the containment mode continues for another 24 hours.

IPs blocked during containment mode continue to be blocked even after the RDP attack has finished. This way, over time, the security software learns the IP addresses that cybercriminals use to attack a customer network and, when all of them have been blocked, the attack is rendered ineffective and it is no longer necessary to use containment mode.

Manual termination of RDP attack containment mode

When you consider the network secure and there is no longer any danger of an RDP attack, you can manually end RDP attack containment mode for a computer:

- **From the lists specified in** Viewing a computer containment status:
  - Open one of the lists and select the checkboxes associated with the computers. The toolbar appears.
  - Click the **End RDP attack containment mode** icon  .

Or:

- Click the context menu to the right of the computer. A drop-down menu appears with the available options.
- Select the option **End RDP attack containment mode**  .
- **From the computer details page:**
  - Open one of the lists specified in **Viewing a computer containment status** and select the computer. The **Computer details** page opens.
  - Click **End RDP attack containment mode**.

When you manually end containment mode, the management console immediately sends the command to all recipient computers. When the device is accessible and has real- time communication enabled, the action is executed immediately. If the security software is unable to contact the computer, the computer moves to **Ending RDP containment mode** status and:

- A flashing icon  appears in the lists specified in **Viewing a computer containment status**.
- A warning message appears on the **Computer details** page.
- A warning message on the **IOA details** page.

*See **Configuring real-time communication** on page **317**.*

The computer continues in containment mode until the command is executed correctly. The security software sends the command again every 4 hours for the next 7 days If the action is unable to complete, the security software management console shows the computer status in **RDP attack containment** mode.

After you manually end containment mode, Advanced EPDR takes these actions:

- All IPs recorded and blocked on the computer are released.
- The computer allows RDP connections.

If the security software automatically ends containment mode, it does not release the IPs and continues to block them.

Configuring indicators of attack (IOA)

Accessing the settings

- From the top menu, select **Settings**. From the side menu, select **Indicators of attack (IOA)**.
- Click **Add**. The **Add settings** page opens.

You can assign indicators of attack (IOA) settings profiles to Windows, Linux, and macOS workstations and servers.

Required permissions

Permission	Access type
Configure indicators of attack (IOA)	Create, edit, delete, copy, or assign indicators of attack (IOA) settings profiles.
View indicators of attack (IOA) settings	View the indicators of attack (IOA) settings profiles defined.

Table 19.2: Permissions required to access the indicators of attack (IOA) settings

Enabling and modifying IOA detection

By default, Advanced EPDR assigns an indicators of attack (IOA) settings profile to all computers on the network, with all types of IOAs enabled. To disable the detection of a specific type of IOA:

- From the top menu, select **Settings**. From the side menu, select **Indicators of attack (IOA)**.
- Click the **Add** button. The **Add settings** page opens.
- Select the IOAs that Advanced EPDR must search for in the telemetry generated by the computers.

To select specific advanced indicators of attack, you must enable all of them by clicking the toggle.

- Select the computers that you want to receive the new settings profile. Click **OK**.

For more information about how to manage settings profiles, see **Managing settings** on page **287**.

Indicators of attack (IOA) settings options

To enable and disable the IOAs that you want to monitor, use the corresponding toggle:

Field	Description
Brute-force attack against RDP **Credentials compromised after brute-force attack on RDP**	Detects large numbers of remote login attempts over the RDP protocol.
Other IOAs	Cytomic periodically updates the list of indicators of attack to reflect new strategies used by cybercriminals.
Advanced indicators of attack	List of the advanced indicators of attack you want to search for on workstations and servers. Available only for Windows computers.

Table 19.3: Types of indicators available in the indicators of attack (IOA) settings

Enabling and disabling advanced IOA technology

Advanced IOA generation leverages new technologies and collects more telemetry data from devices. This technology could affect device performance on multi-user servers and in specific situations. To disable this technology completely, disable the **Advanced IOA** toggle.

Disabling advanced IOAs individually does not disable the technology and does not substantially improve performance.

Information associated with IOAs

From the **Indicators of attack (IOA)** list, click the icon next to the name of an IOA. A dialog box opens that shows information about the IOA (name, risk, description, recommendations, MITRE, etc.). For more information, see **Table 19.10:** .

Automatic response to RDP attacks

Field	Description
Response on workstations	• **Report and block RDP attacks**: Generates an IOA and blocks RDP attacks. See **Detection and protection against RDP attacks**. • **Report only**: Generates an IOA.
Response on servers	• **Report and block RDP attacks**: Generates an IOA and blocks RDP attacks. See **Detection and protection against RDP attacks**. • **Report only**: Generates an IOA.

Table 19.4: Automatic response actions for RDP IOAs

Trusted IPs

Enter a list of IP addresses for computers you consider secure. These IPs are reported but not blocked. You can enter individual IP addresses separated by commas, or IP address ranges separated by a dash.

Indicators of Attack (IOA) module lists

Accessing the lists

You can access the lists in two ways:

- From the top menu, select **Status**. From the side menu, select **Indicators of attack (IOA)**. Click the relevant widget.

Or:

- From the top menu, select **Status**. From the side menu, click the **Add** link. A dialog box opens that shows the available lists.
- In the **Security** section, select the **Indicators of attack (IOA)** list to see the corresponding template. Edit it and click **Save**. The list is added to the side menu.

Required permissions

Permission	Access to lists
View detections and threats	• Indicators of attack (IOA)

Table 19.5: Permissions required to access the Indicators of Attack (IOA) lists

Indicators of attack (IOA)

This list shows details of the IOAs detected on workstations and servers by Advanced EPDR.

- Each detection refers to a single computer and IOA type. If the same chain of suspicious events occurs on multiple computers, a separate detection is generated for each computer.
- If the same pattern-computer-type triplet is detected multiple times, detections are grouped and the security software shows the number of repetitions in the **Occurrences** field. For more information about the grouping algorithm, see **Groups of IOA-generated detections**.

Field	Comment	Values
Computer	Name of the computer where the IOA was detected.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
Indicator of attack	Name of the internal rule that detected the pattern of events that triggered the detection.	Character string
Occurrences	Number of occurrences of the detection. For more information about the grouping algorithm applied, see **Groups of IOA-generated detections**.	Number
Risk	Impact of the IOA detected: • Critical • High • Medium • Low • Unknown	Enumeration
Action	Type of action taken by Advanced EPDR on brute-force attack against RDP IOAs: • Reported • Attack blocked See **Automatic response to RDP attacks**.	Enumeration
Status	• **Archived**: The detection no longer requires	Enumeration

Field	Comment	Values
	administrator attention because it was a false positive or was resolved. • **Pending**: The detection has not been investigated by the administrator. See **Indicators of attack (IOA)**.	
Date	Date and time the IOA was last detected.	Date

Table 19.6: Fields in the Indicators of Attack (IOA) list

Fields displayed in the exported file

Field	Comment	Values
Indicator of attack	Name of the rule that detected the pattern of events that triggered the detection.	Character string
Occurrences	Number of occurrences of the detection. For more information about the grouping algorithm applied, see **Groups of IOA-generated detections**.	Number
Risk	Impact of the IOA detected: • Critical • High • Medium • Low • Unknown	Enumeration
Action	Type of action taken by Advanced EPDR: • Reported • Attack blocked See **Automatic response to RDP attacks**.	Enumeration
Status	• **Archived**: The detection no longer requires administrator attention because it was a false positive or was resolved.	Enumeration

Field	Comment	Values
	• **Pending**: The detection has not been investigated by the administrator. See **Indicators of attack (IOA)**.	
Date	Date and time the IOA was last detected.	Date
Date archived	Date the detection was last archived.	Date
Time until archived	The time elapsed between when the IOA was detected and when you verified it and took remedial action where necessary.	Date
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
IP address	The computer primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Brief description of the strategy used by the adversary.	Character string

Table 19.7: Fields in the Indicators of Attack (IOA) exported file

Filter tool

Field	Description	Values
Search computer	Computer name.	Character string
Risk	Impact of the IOA detected: • Critical • High • Medium • Low • Unknown	Enumeration

Field	Description	Values
Action	Type of action taken by Advanced EPDR: • Reported • Attack blocked See **Automatic response to RDP attacks**.	Enumeration
Tactic	Category of the attack tactic that generated the detection, mapped to the MITRE matrix. To quickly find a specific tactic, enter the search terms in the text box. Click the  icon and select the tactic that you want to filter the list by.	Character string
Dates	Time period when the detection was generated.	• Last 24 hours • Last 7 hours • Last month
Status	Status of the detection.	• Pending • Archived
Indicator of attack	Name of the IOA that generated the detections to search for. To quickly find detections generated by a specific IOA, enter the search terms in the text box under the filter name. Click the  icon and select the IOA that you want to filter the list for.	Character string
Technique	Category (and sub-category, if available) of the attack technique that generated the IOA, mapped to the MITRE matrix. • When you filter by a technique, the list shows detections generated by IOAs that have that technique or one of its sub-technique associated. • When you filter by a sub-technique, the list shows detections generated by IOAs that have that specific sub-technique associated.	Character string

Field	Description	Values
	Techniques are identified by a character string in the TXXXX format. Sub-techniques are identified by a character string in the TXXXX.YYY format. To quickly find a specific technique, enter the search terms in the text box. Click the icon and select the technique that you want to filter the list by.	

Table 19.8: Filters available in the Indicators of Attack (IOA) list

Details page

Click an item in the list to open its details page. This page shows a detailed description of when and where the detection occurred, as well as details of the pattern of events that led to the detection.

Advanced IOAs also show the **Activity** tab. This tab shows all events that are part of the potential attack.

Field	Comment	Values
Status	Status of the detection, and date the status was assigned.	• Pending • Archived
Detection date	Date and time the IOA was last detected.	Date
Indicator of attack (IOA)	Name of the rule that detected the pattern of events that triggered the detection.	Character string
Risk	Impact of the IOA detected: • Critical • High • Medium • Low • Unknown	Enumeration
Description	Description of the chain of events detected on the computer, and the consequences it could	Character string

Field	Comment	Values
	have if the attack achieves its objectives.	
Advanced attack investigation **(Not available for advanced IOAs)**	Report with full details of the IOA that triggered the detection. • Computer ID and date. • Detected IOA type name. • Detailed description of the internal functionality of the IOA that triggered the detection, mapped to the MITRE tactic and technique used. • Operating system tools used in the attack. • Computer details. • Attack severity. • Status of the computer with respect to the attack. • Progress status of the attack. • Users logged in at the time of the attack. • IPs/URLs accessed. • Daily repetitions of the attack. • Diagram of the chain of processes involved in the attack. • Advice for mitigating or remediating the attack. Reports are available for a month after the detection is generated. After this period, they are no longer accessible. Also, reports show events that have been part of the attack for the 30 days prior to the detection of the IOA.	Button
View attack graph **(Not available for advanced IOAs)**	Interactive diagram of the sequence of events that led to the detection. See **Graphs**.	Button
Action	Type of action taken by Advanced EPDR:	Enumeration

Field	Comment	Values
	• Reported • Attack blocked See **Automatic response to RDP attacks**.	
Recommendations	Remedial actions recommended by Cytomic.	Character string

Table 19.9: Fields on the IOA Details page

Details tab

Field	Comment	Values
Computer	Name and group of the affected computer. If the computer is in containment mode, the **End RDP attack containment mode** button appears. See **Manual termination of RDP attack containment mode**.	Character string
Detected occurrences	Number of occurrences of the IOA. For more information about the grouping algorithm applied, see **Groups of IOA-generated detections**.	Number
Last event	Date and time the event that triggered the IOA occurred.	Date
View full activity details	Available for advanced IOAs. See **Activity tab**.	
View computer investigation	See **Investigation tab**.	
Other details	Data in JSON format that includes fields relevant to the event that led to the generation of the IOA. See **Format of the events contained in telemetry data** on page **957**.	Character string
Tactic	Category of the attack tactic that generated the IOA, mapped to the MITRE matrix.	Character string
Technique	Category of the attack technique that generated the IOA, mapped to the MITRE matrix. It is identified by a	Character string

Field	Comment	Values
	character string in the TXXXX format.	
Sub-technique	Sub-category (if available) of the attack technique that generated the IOA, mapped to the MITRE matrix. It is identified by a character string in the TXXXX.YYY format.	Character string
Platform	Operating system and environments where MITRE has previously recorded this type of attack.	Character string
Description	Details of the tactics and techniques used by the IOA detected, according to the MITRE matrix.	Character string

Table 19.10: Fields on the IOA Details page

Activity tab

The details page for an advanced IOA shows an additional tab: **Activity**. This tab shows a list of all the events that triggered the detection. It enables you to see the sequence of steps taken by the malicious software and confirm or dismiss the attack.

Field	Comment	Values
Search	Filters the list by the contents of the Date and Action fields. You can type only a partial string.	
Date	When the security software detected the event.	Date
Action	Summary of the event details. To get full details, click the event.	Character string
Export 	Exports the list of events shown in the console to an Excel file.	

Table 19.11: Fields on the Activity tab

Click a row in the table to show the **Event details** side panel. This panel included two tabs:

- **Details**: Shows detailed information for the event. For more information about the meaning of the fields, see **Format of the events contained in telemetry data** on page **957**.
- **MITRE**: Shows detailed MITRE information (for example, tactic, technique, sub-technique, and description). If the advanced IOA is associated with more than one technique, the MITRE tab shows the information in multiple sub-sections, one for each technique. All data on

the MITRE tab is collected from the official website at **https://attack.mitre.org/matrices/enterprise/**.

Field	Description
Tactic	Name of the MITRE tactic associated with the advanced IOA. Tactics are identified by a character string in the TAXXXX format.
Technique	Name of the MITRE technique associated with the advanced IOA. Techniques are identified by a character string in the TXXXX format.
Sub-technique	Name of the MITRE sub-technique associated with the advanced IOA. Sub-techniques are identified by a character string in the TXXXX.YYY format.
Platform	Operating systems affected by the tactic and technique.
Permissions required	Permissions required to run the attack.
Description	Details of the tactics and techniques used by the IOA detected, according to the MITRE matrix.

Table 19.12: Fields on the MITRE tab

Investigation tab

All types of IOAs enable you to open an Cytomic Orion investigation console to show all the telemetry collected on the computer for investigation purposes. To make your analysis easier, the investigation console focuses on the last event that triggered the IOA. You can trace back five days to review the context of the computer where the detection occurred, and trace forward one day to see the effects of the attack on the computer.

For more information about the investigation console, see **Investigation section (5)** on page **275**.

Groups of IOA-generated detections

To prevent too many detections in the management console, Advanced EPDR groups two or more equal detections of the same IOA, showing the number of repetitions in the **Occurrences** field in the list of IOAs or in the **Detected occurrences** field on the IOA details page. To group two or more equal detections, they must be:

- For the same IOA.
- Detected on the same computer.
- Detected close to each other in time.

The grouping algorithm that is used depends on the type of IOA and whether the computer is in Audit mode. For more information about how to enable or disable Audit mode, see **Audit mode** on page **359**.

Detection grouping algorithm for standard IOAs

- The security software logs the first detection and sets the **Detected occurrences** field to 1.
- Equal detections made in the six hours after the first detection was logged are grouped together. The security software sends a detection at the end of each six-hour interval. (The **Detected occurrences** field indicates the total number of detections made.).
- If the security software does not log an equal detection within a six-hour interval, then it does not send a detection for the interval.
- After four intervals (24 hours), the process starts again.

Detection grouping algorithm for advanced IOAs

- The security software logs the first detection and sets the **Detected occurrences** field to 1.
- Equal detections made every hour after the first detection was logged are grouped together. The security software sends a detection at the end of each one-hour interval. (The **Detected occurrences** field indicates the total number of detections made.).
- If the security software does not log an equal detection within the hour interval, then it does not send a detection for the interval.
- After 24 hours, the process starts again.

Detection grouping algorithm for advanced IOAs with Audit mode enabled

Detections are not grouped if the computer is in Audit mode. The security software sends each detection with the **Detected occurrences** field set to 1.

Detection grouping algorithm for RDP attack IOAs

*For more information about the network attack detection algorithm, see **Detection and protection against RDP attacks**.*

Advanced EPDR reports a maximum of 50 equal detections of the Network Attack IOA every 24 hours for each computer. For two detections of a Network Attack IOA to be considered the same, these conditions must be met:

- The target computer must be the same.
- The process involved on the target computer must be the same. Depending on the stage of the attack, this is the process that listens for the operating system RDP requests or any other

process that is run remotely on the computer after a successful login preceded by multiple failed login attempts.

Graphs

To see the details of an IOA detection, open the **Indicators of attack (IOA)** list and select the IOA. See **Accessing the lists**. If the detection has a graph associated with it, the **View attack graph** button appears on the detection details page.

Graph structure

The following is a description of the information panels and tools available in a graph:

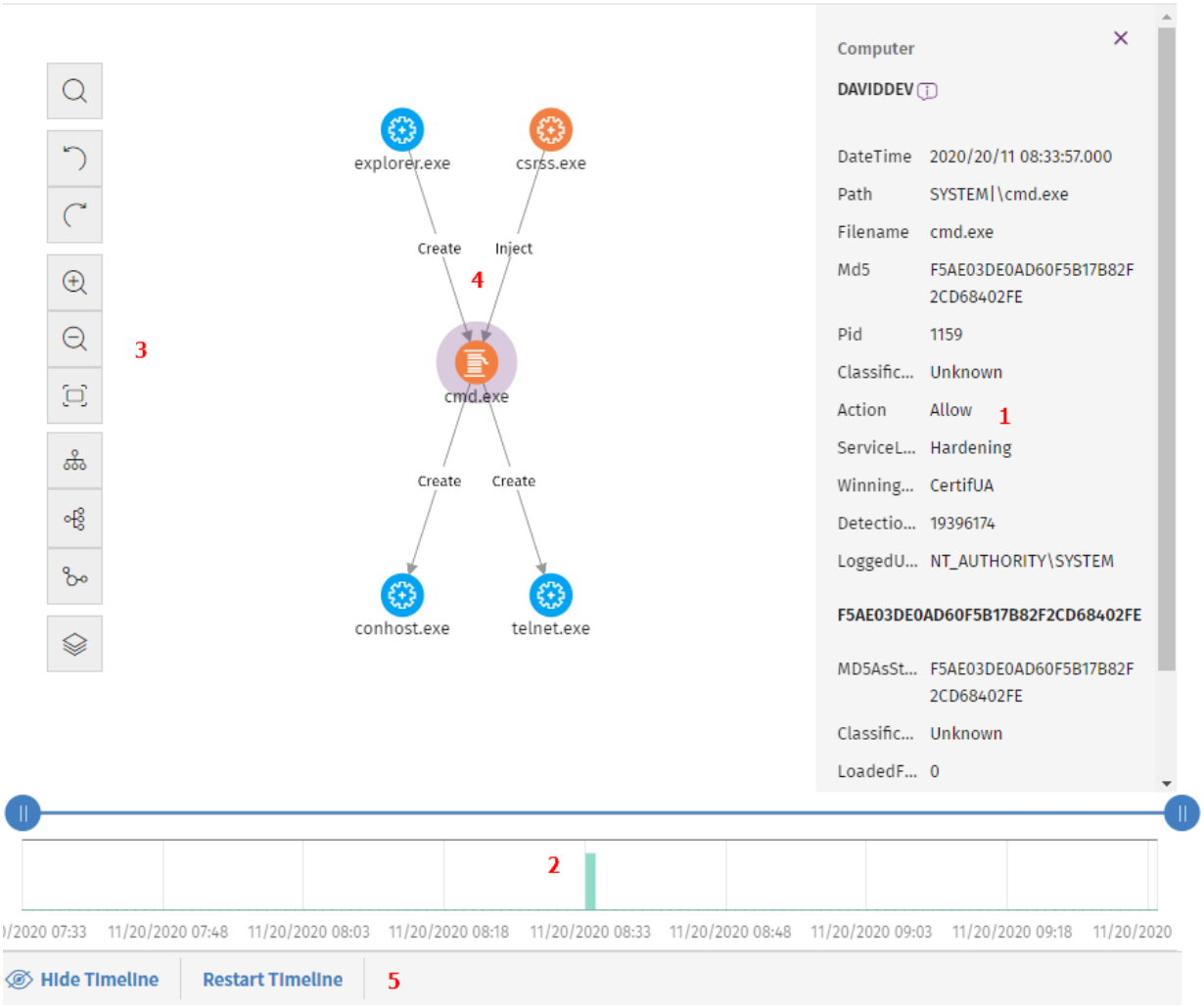


Figure 19.1: Graph and tools

- **Information panel for the selected item (1)**: Shows information pertaining to the selected node or line. For more information about the meaning of the fields, see **Format of the events contained in telemetry data** on page **957**.

- **Timeline (2)**: Shows a histogram with green bars that represent the events carried out by a threat. You can use the timeline to increase or reduce the displayed time period when the events occurred. For more information about how to use this resource, see **Timeline**.
- **Graph toolbar (3)**: Enables you to change the way the graph is shown on the page. See **Graph settings**.
- **Graph (4)**: A graphical representation of a set of events with nodes and arrows to show entities and the relationship between them. The numbers on the arrows indicate the order in which the events were recorded.
- **Timeline controls (5)**: Enable you to hide, show, or reset the timeline. See **Timeline**.

Graph settings

To modify the graph to your needs, use these resources:

- The graph toolbar, on the left side of the page.
- The context menus. To access them, right-click a node or a node group.

By default, the graph is displayed horizontally **(6)** with a sufficient level of zoom to make sure you can see all nodes without having to move the view.

Graph toolbar

- To highlight and find the nodes that match the search criteria you enter, click the **(1)** icon.
- To undo the last action performed on the graph, click the **(2)** icon.
- To redo the last action performed on the graph, click the **(3)** icon.
- To zoom in the graph, click the **(4)** icon.
- To zoom out from the graph, click the **(5)** icon.
- To return to the default zoom setting, click the **(6)** icon.
- To change the graph orientation to horizontal, click the **(7)** icon.
- To change the graph orientation to vertical, click the **(8)** icon.
- To change the graph orientation so that nodes are distributed freely taking advantage of the available space, click the **(9)** icon.
- To show or hide information layers in the graph **(10)**, see **Hiding and showing layers**.

Figure 19.2: Toolbar

Context menus

Right-click a node or node group to open its context menu. Options you cannot use based on the status of the node are disabled and appear dimmed.

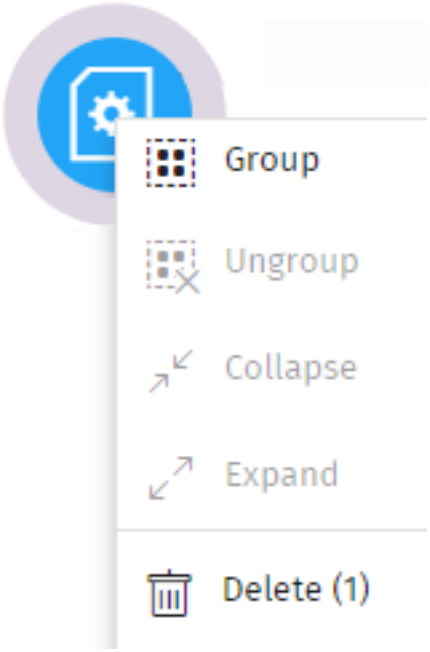


Figure 19.3: Context menu

Hiding and showing layers

To show or hide elements in the graph, click the **(10)** icon. A drop-down menu opens that shows these options:

- **Execution sequence**: Hides or shows numbers on the events to determine the order in which events occurred. See **Arrow styles**.
- **Name of relationships**: Hides or shows the names of the events. See **Format of the events contained in telemetry data** on page **957**.
- **Name of entities**.

Selecting nodes on the graph

- **To select a single node on the graph**: Click the node.
- **To select multiple non-contiguous nodes on the graph**: Press and hold the Ctrl or Shift key and click the nodes you want to select.
- **To select multiple contiguous nodes on the graph**: Press and hold the Ctrl or Shift key, and click an empty area of the graph. Drag the mouse to draw a selection box that covers all the nodes you want to select.

When you select and right-click several nodes on the graph, the options that apply to all selected nodes show in the context menu.

Moving and deleting nodes

To move all nodes and lines on the graph:

Click an empty area of the graph. Drag the graph in the appropriate direction.

To move a single node:

Select the node and drag it to a new location. All lines that connect the node with its neighbors move and adjust themselves to the new location of the node.

To delete a single node using the keyboard:

- Select the node you want to delete. Press the Delete key. A dialog box opens and shows the total number of nodes that will be deleted from the graph. This includes the selected node and its child nodes.
- Click **OK**.

To delete a single node using the mouse:

- Right-click the node you want to delete. The context menu opens.
- Select **Delete (x)**. A dialog box opens and shows the total number of nodes that will be deleted from the graph. This includes the selected node and its child nodes.
- Click **OK**.

To delete multiple nodes:

- Select the nodes you want to delete. Right-click one of the nodes. The context menu opens.
- Select **Delete (x)**. A dialog box opens and shows the total number of nodes that will be deleted from the graph. This includes the selected node and its child nodes.
- Click **OK**.

Grouping nodes

With graphs that contain a large number of items, you can group nodes that are related to one another to simplify the graph.

Node groups can have two states:

- **Expanded**: They show the nodes that make up the group.
- **Collapsed**: They hide the nodes that make up the group.

A node group is an entity with these characteristics:

- The actions taken on a node group affect all nodes that make up the group.
- You can group nodes of different types.
- When you delete a group, you delete all nodes that make up the group from the graph.

- When you collapse a group, all relationships between the nodes in the group and external nodes are represented as if they were established with the group. Arrows that indicate relationships of the same type (same type of event) are also grouped (see).
- The empty area of an expanded group represents the set of nodes in the group. For example, to open the context menu for all nodes in a group, right-click an empty area of the expanded group. Likewise, if you select **Delete**, you will delete all nodes in the group.
- A node belonging to an expanded group behaves in the same way as a node that is not in a group: you can move it individually, open its context menu, delete it, etc.
- A group can consist of nodes only, other groups only, or a combination of nodes and groups.

To group a set of nodes:

- Select multiple nodes on the graph. Right-click one of the nodes. A context menu opens.
- From the menu, select **Group**. A rectangle appears that contains all nodes in the group.

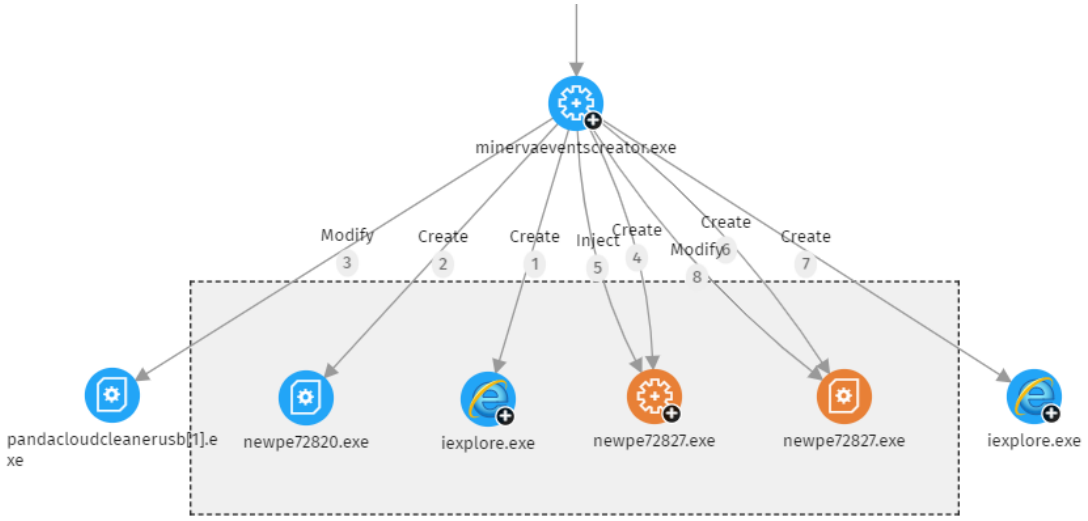


Figure 19.4: Node group

- Right-click an empty area of the rectangle. The context menu for the group opens.
- From the menu, select **Collapse**. The grouped nodes are replaced with a small square and all relationships with the nodes in the group point to the square.

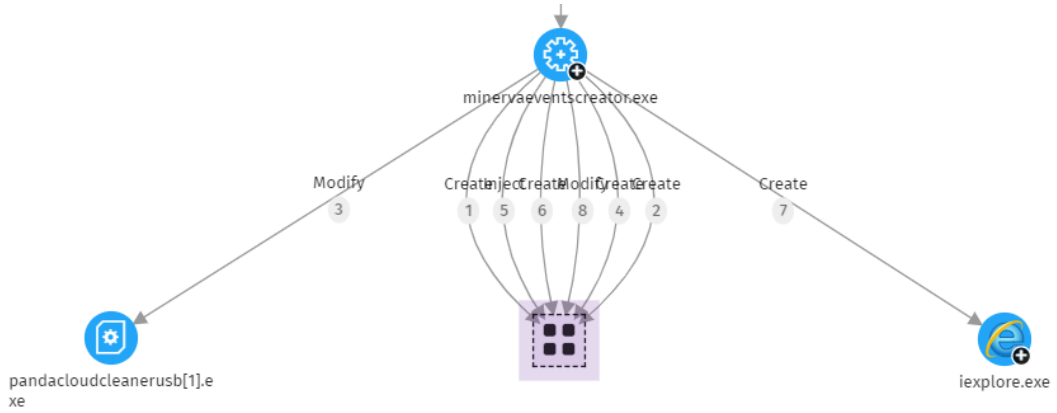


Figure 19.5: Collapsed node group

To expand a collapsed node group:

- Right-click the collapsed node group. A context menu opens.
- Select **Expand**. The previously collapsed nodes appear in the rectangle.

To ungroup nodes:

- Right-click the node group. A context menu opens.
- Select **Ungroup**. The nodes reappear on the graph and the rectangle disappears.

Information about collapsed groups

Types of grouped nodes

A node group can contain nodes classified as goodware, malware, or unclassified. This is indicated by the group color.

Color	Description
	Group with blocked items.
	Group with items classified as goodware.

Table 19.13: Colors used in groups

Number of grouped nodes

In the upper-left corner, you can see the number of nodes that would appear on the graph if the group were not collapsed. This number does not have anything to do with the total number of

nodes (parent nodes, child nodes, etc.) the group can contain. It shows only the number of nodes that were visible prior to being collapsed.

Searching for nodes

The search bar enables you to highlight nodes of interest and access their details quickly.

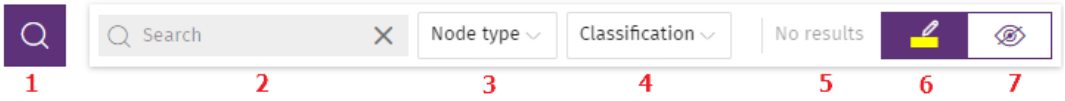


Figure 19.6: Search bar in graphs

- **(1)**: Click to show or hide the search bar.
- **(2)**: Type the character string you want to search for. The search runs in real time on the names and details of nodes only. The content of arrows is excluded from searches. To clear the search, click the ✕ icon.

> *To avoid showing orphan nodes in search results, the parent node is always included, even if it does not match the entered pattern.*

- **(3)**: Restricts searches on graphs to certain types of entities. To extend searches to include more than one type of entity, expand the drop-down menu and select the types of entities that you want to search for. To search across all types of entities again, click **Clear search**. The logical operator that is applied when you run a search across multiple types of entities is OR.
- **(4)** Restricts searches on graphs to the entities that have been classified by Advanced EPDR as the value you select in the drop-down menu. To extend searches to include more than one type of classification, expand the drop- down menu and select the types of classifications that you want to search for. To run a new search ignoring the classification of entities, click **Clear search**. The logical operator that is applied when you run a search across nodes with different classifications is OR.
- The logical operator that is applied when you run a search by entity and by classification simultaneously is AND.
- **(5)**: Indicates the number of nodes that match the search pattern entered. If the highlighting tool is enabled **(4)** and you click the ⌄ icon, a drop-down menu appears:
    - **Select found nodes**: Selects the nodes that match the search pattern entered. To show the context menu, right-click any of the selected items.
    - **Select all nodes except found nodes**: Selects nodes that do not match the search pattern entered. To show the context menu, right-click any of the selected items.

- **(6)**: Highlights found items in yellow.
- **(7)**: Hides items that do not match the search pattern entered.

The searches you run on nodes belonging to an expanded group behave in the aforementioned way. However, with nodes in a collapsed group, they behave differently:

- If the search is performed with the highlighting tool enabled **(6)**, the group is highlighted if any of the nodes in the group match the search criteria. Otherwise, the group is not highlighted.
- If the search is performed with the hiding tool enabled **(7)**, the group is shown if at least one of the nodes in the group matches the search criteria. Otherwise, the group is not shown on the graph.

Timeline

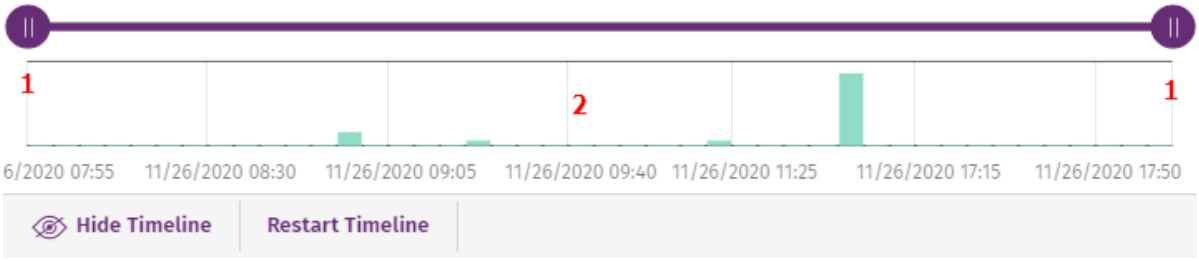


Figure 19.7: Timeline controls

You can blur the nodes and relationships that occurred outside a selected time range. This way, you can concentrate on the data that is more relevant to you.

The timeline includes a histogram with green bars **(2)** that represent the events carried out by a threat. Point to the bars to show a tooltip of the number of events and the date they were logged.

To select a specific interval on the timeline:

- Click **(1)** and drag it to the left or right. The histogram is expanded or reduced to fit the new interval.
- The graph shows the events and nodes that occurred within the interval. Other events and nodes are blurred.

To hide/show the timeline:

- To hide the panel, click **Hide timeline**.
- To show it again, click **Show timeline**.
- Click **Reset timeline** to return the timeline to its default settings.

Information contained in graphs

Graphs provide a graphical representation of the execution tree of an IOA detection, where nodes represent the entities that participate in an operation (such as processes, files, or communication or operation targets) and arrows represent operations. Graphs use color codes, panels, and other resources that provide information about the represented entities and their relationships.

The resources used to present this information are:

- **Node colors**: Indicate the item classification.
- **Node icons**: Indicate the item type.
- **Status icons**: Indicate the action taken on the item.
- **Arrow colors**: Indicate whether the item was blocked or allowed.
- **Arrow styles**: Indicate the number and direction of the actions executed between the nodes.
- **Arrow labels**: When you click the label of an arrow, the right panel shows information about the action taken by the process.
- **Node labels**: When you click the label of a node, the right panel shows information about the entity.

Node colors

Color	Description
	Item classified as malware.
	• Item classified as a PUP. • Item classified as a suspicious item. • Unclassified item.
(Original color)	Item classified as goodware.

Table 19.14: Colors used in graph nodes

Node icons

Icon	Description	Icon	Description
	Process. If it belongs to a known software package, the icon is shown.		Compressed file
	Remote thread		Executable file
	Library		Script file
	Protection		Windows registry branch value
	Folder		URL used in a communication
	Non-executable file		IP address in a communication

Table 19.15: Colors used in graph nodes

Status icons

Icon	Description	Icon	Description
	File deleted		File quarantined

Icon	Description	Icon	Description
	File disinfected		Process deleted

Table 19.16: Icons used to indicate the status of a node

Node labels

They indicate the name of the entity. When you click the label of a node, an information panel appears on the right side of the page. This panel shows a number of fields that describe the entity.

Arrow colors

The color of the arrows indicates whether Advanced EDR or Advanced EPDR allowed the action or blocked it because the process was classified as a threat.

- **Red**: The action was blocked. See the meaning of the actions in the **action** field in **Format of the events contained in telemetry data** on page **957**.
- **Black**: The action was allowed.

Arrow styles

- **Arrow thickness**: Represents the number of times the same type of action was executed between two nodes. The greater the number of actions, the thicker the arrow. When you click an arrow, the information panel shows the dates when the first and last actions in the group occurred.
- **Arrow direction**: Indicates the direction of the action.
- **Numbers**: The numbers on the arrows indicate the order in which the event was recorded.

Arrow labels

They indicate the name of the action taken by the process. When you click the label of an arrow, the information panel shows a number of fields that describe the event that occurred.

Node levels shown by default

By default, the graph is displayed horizontally with the node that triggered the IOA detection at the center of the graph. It is surrounded by a subset of nodes related to the detection:

- **Three node levels above the main node**: The graph shows parent, grandparent, and great-grandparent nodes of the main node.
- **One node level below the main node**: The graph shows child nodes of the main node.

The graph can show up to a maximum of 25 nodes at the same level. When there are more than 25 nodes, the graph shows no nodes to avoid overloading graphs.

Showing child nodes

The  icon in the bottom-left corner of a node indicates that the node has hidden child nodes. To show its child nodes, right-click the node. A context menu opens. Select one of the available options:

- **Show parent**: Shows the parent nodes of the selected node.
- **Show all activity (number)**: Shows all the child nodes of the node regardless of the type. The maximum number of nodes shown is 25. The total number of events that link the parent node with the child node shows.
- **Show children**: Opens a drop-down list. Select the type of child nodes to show and select the number of nodes for each type. The types of nodes include:
    - **Data files**: Files with unidentified information.
    - **Script files**: Files with command sequences.
    - **Downloads**: Data files downloaded from the Internet/network.
    - **DNS**: Domains that failed to resolve the IP.
    - **Windows registry entries**
    - **Compressed files**
    - **PE files**: Executable files.
    - **Remote threads**
    - **IPs**: IP addresses for either end of the communication.
    - **Libraries**
    - **Processes**
    - **Protection**: Action taken by the antivirus.

When you select and right-click several nodes on the graph, the options that apply to all selected nodes show in the context menu.

Indicators of Attack module panels/widgets

From the top menu, select **Status**. From the side menu, select **Indicators of attack (IOA)**.

Required permissions

Permissions	Access to widgets
View detections and threats	• Threat Hunting Service • Detections trend • Indicators of attack (IOA) mapped to the MITRE ATT&CK matrix • Detected indicators of attack (IOA) • Indicators of attack (IOA) by computer

Table 19.17: Permissions required to access the Indicators of Attack widgets

All widgets, except Threat Hunting Service, show only information generated by the computers on the network that are visible to the role associated with the administrator account used to access the console.

Advanced EPDR shows detections with the Pending status in widgets when it detects suspicious activities on the customer network. See **Introduction to IOA concepts**.

For more information about the IOA detection grouping strategies implemented in Advanced EPDR, see **Groups of IOA-generated detections**.

Threat Hunting Service

This widget shows a summary of the events, indicators, and IOAs for all computers and devices on the network, for a selected time, to help you determine if there are intrusion attempts.

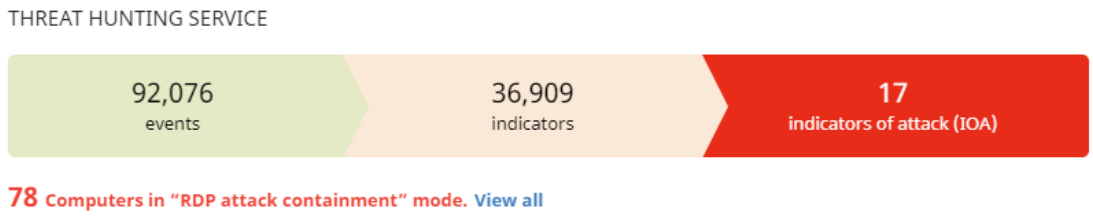


Figure 19.8: Threat Hunting Service panel

Meaning of the data displayed

Data	Description
Events	Number of actions carried out by programs installed on protected computers and monitored by Advanced EPDR. These events are received as part of the telemetry and are stored on the Cytomic platform to look for suspicious behavior patterns. This counter includes all detections on the network, regardless of the

Data	Description
	visibility assigned to the account that accesses the Advanced EPDR console.
Indicators	Number of suspicious event patterns detected in the event data flow. This counter includes all detections on the network, regardless of the visibility assigned to the account that accesses the Advanced EPDR console.
Indicators of attack (IOA)	Number of indicators that are highly likely to be an attack.
Computers in RDP attack containment mode	Number of computers that experienced an attack through the RDP protocol and are in RDP attack containment mode.

Table 19.18: Description of the data displayed in the Threat Hunting Service panel

Lists accessible from the panel

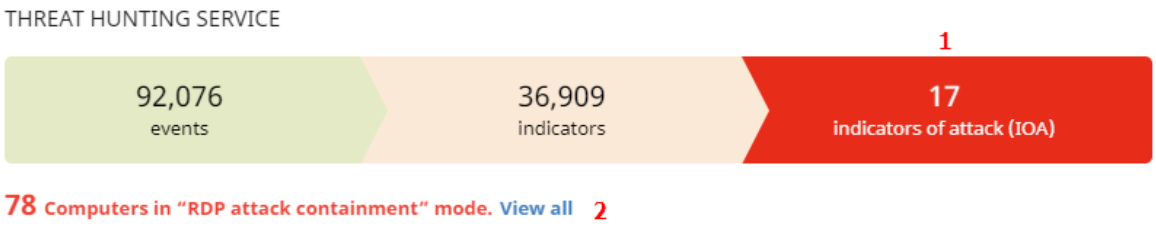


Figure 19.9: Hotspots in the Threat Hunting Service panel

Click the hotspots shown in **Figure 19.9:** to open these lists with these predefined filters:

Hotspot	List	Filter
(1)	Indicators of attack (IOA)	No filter.
(2)	Computer protection status	"RDP attack containment" mode = Yes

Table 19.19: Filters accessible from the Threat Hunting Service panel

Detections trend

This widget includes a line and bar graph that shows the number of indicators, pending IOA detections, and archived IOA detections over time.

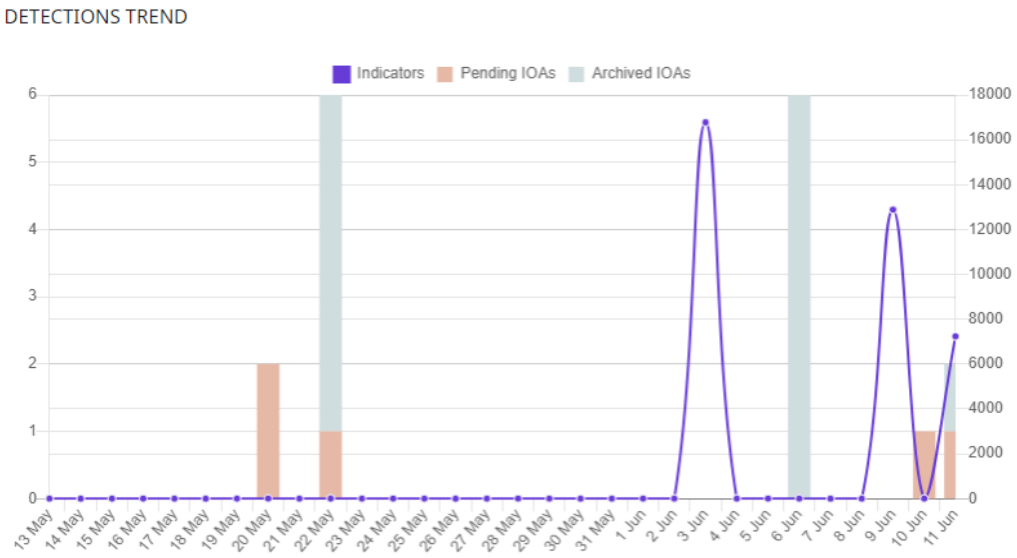


Figure 19.10: Detections Trend panel

To represent the different scales in the same diagram, the graph has two Y-axes:

- The Y-axis on the left measures recorded pending and archived detections.
- The Y-axis on the right measures indicators detected.

Meaning of the data displayed

Data	Description
Indicators	Number of suspicious patterns detected in the event flow received.
Pending IOAs	Number of suspicious patterns that are highly likely to indicate an attack. An administrator has not analyzed or resolved the IOA.
Archived IOAs	Number of IOAs that an administrator has analyzed or resolved and marked as Archived.

Table 19.20: Description of the data displayed in the Detections Trend panel

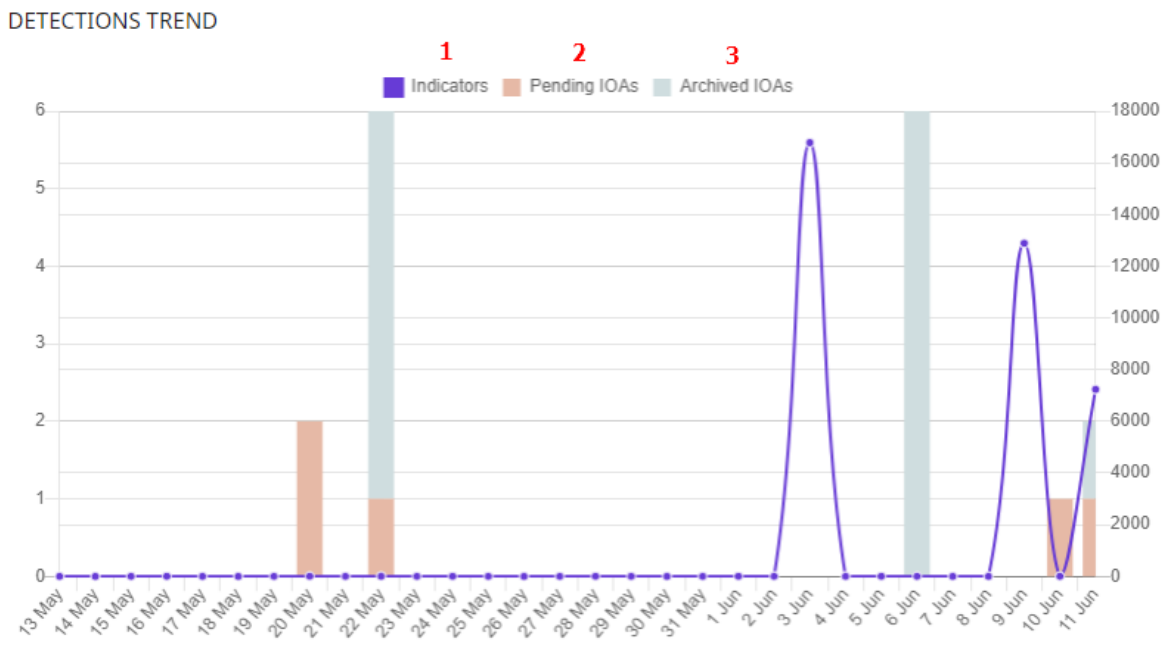


Figure 19.11: Hotspots in the Detections Trend panel

Click the hotspots shown in **Figure 19.11:** to open the **Indicators of attack (IOA)** list with these predefined filters:

Hotspot	Filter
(1)	None
(2)	Status = Pending
(3)	Status = Archived

Table 19.21: Filters available in the Indicators of Attack (IOA) list

Indicators of attack (IOA) mapped to the MITRE ATT&CK matrix

This widget shows a table of the number of IOAs detected during the selected time period, arranged by MITRE tactic and technique.

Point to a box to view:

- The name and code of the tactic/technique
- The total number of detections
- The number of pending detections

An IOA detection has at least one tactic and one technique associated with it. However, not all IOA detections have sub-techniques associated with them.

To view the sub-techniques associated with an IOA detection, click **Show sub-techniques**.

Figure 19.12: Indicators of Atack (IOA) Mapped to the MITRE ATT&CK Matrix panel

Meaning of the data displayed

Data	Description
Red number	Number of detections recorded, with Pending status, which use the specified tactic, technique, and sub-technique.
Black number	Total number of recorded detections (pending + archived) that use the specified tactic, technique, and sub-technique.
Show sub-techniques link	Shows the sub-techniques associated with the IOA. For each sub-technique, the panel shows the total number of pending detections (in red) or pending and archived detections (in black) that have that sub-technique associated with them.

Table 19.22: Description of the data displayed in the Indicators of Attack (IOA) Mapped to the MITRE ATT&CK Matrix panel

Lists accessible from the panel

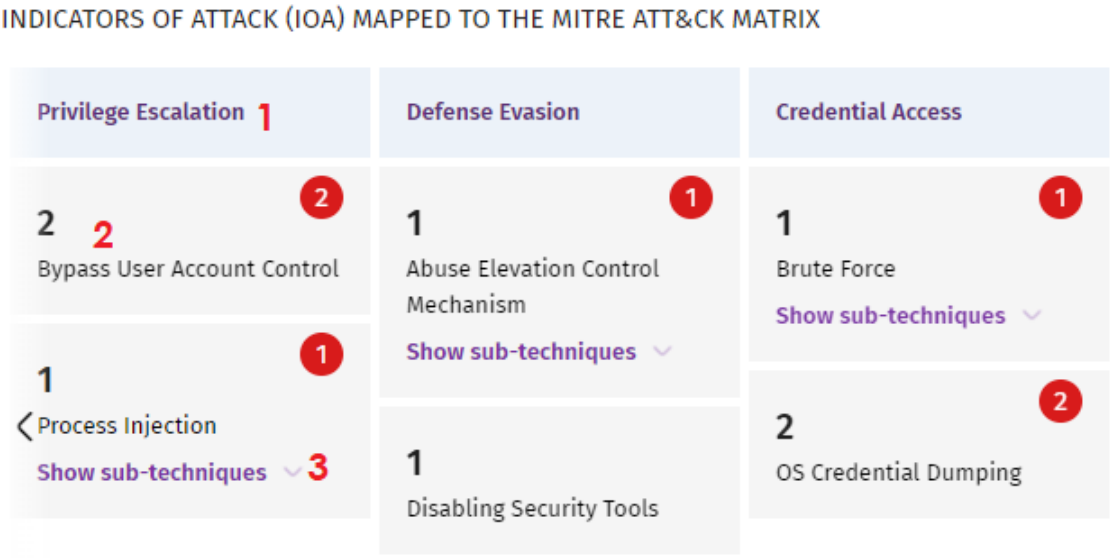


Figure 19.13: Hotspots in the Indicators of Attack (IOA) Mapped to the MITRE ATT&CK Matrix panel

Click the hotspots shown in **Hotspots in the Indicators of Attack (IOA) Mapped to the MITRE ATT&CK Matrix panel** to open the **Indicators of attack (IOA)** list with these predefined filters:

Hotspot	Filter
(1)	Tactic = The tactic selected in the widget
(2)	• Tactic = The tactic selected in the widget • Technique = The technique selected in the widget
(3)	Sub-technique = The sub-technique selected in the widget

Table 19.23: Filters available in the Indicators of Attack (IOA) list

Detected indicators of attack (IOA)

This widget shows the distribution of IOA detections by type recorded during the selected time period. The greater the number of detections of a particular type, the larger the box within the widget.

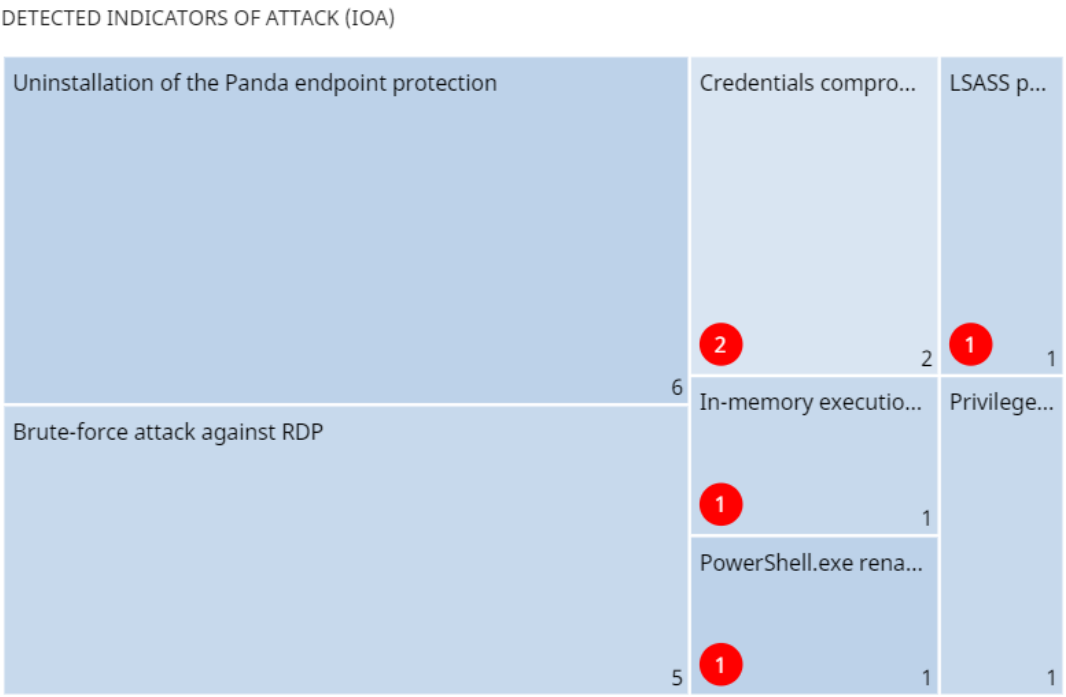


Figure 19.14: Detected Indicators of Attack (IOA) panel

Meaning of the data displayed

Data	Description
Red number	Number of pending detections of a given type recorded during the selected period.
White number	Total number of recorded detections (pending + archived) of a given type recorded during the selected period.

Table 19.24: Description of the data displayed in the Detected Indicators of Attack (IOA) panel

Lists accessible from the panel

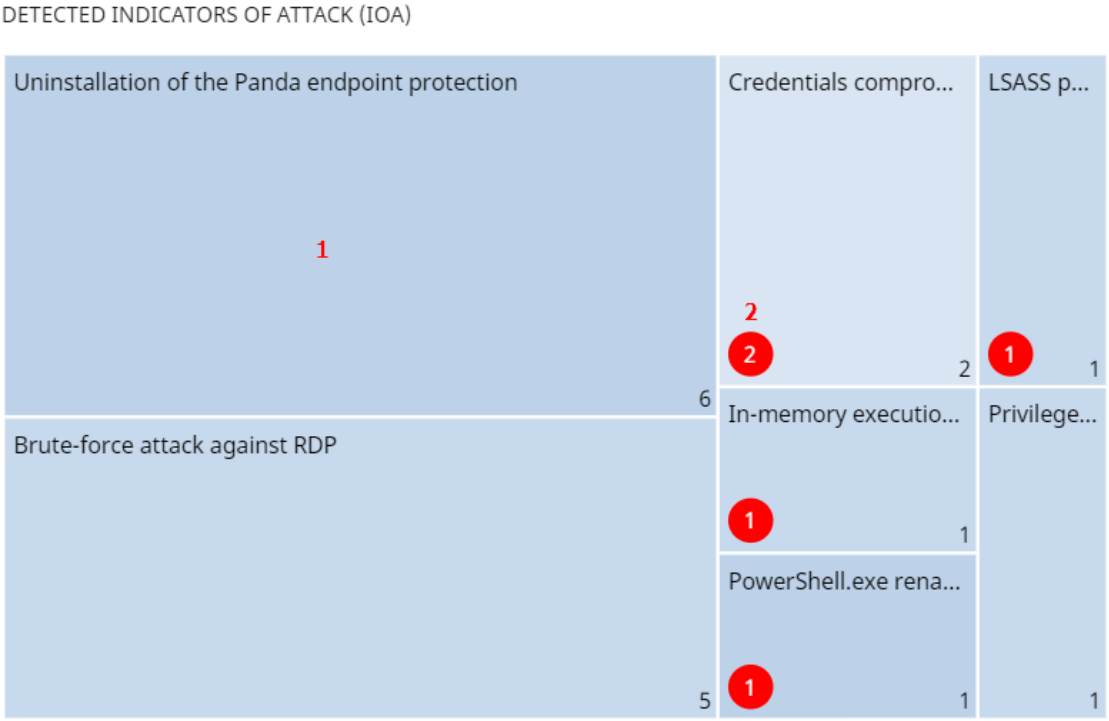


Figure 19.15: Hotspots in the Detected Indicators of Attack (IOA) panel

Click the hotspots shown in **Figure 19.15:** to open the **Indicators of attack (IOA)** list with these predefined filters:

Hotspot	Filter
(1)	Indicator of attack = The indicator of attack selected in the widget
(2)	• Indicator of attack = The indicator of attack selected in the widget • Status = Pending

Table 19.25: Filters available in the Indicators of Attack (IOA) list

Indicators of attack (IOA) by computer

This widget shows the distribution of detections for each computer on the network during the time period. The greater the number of detections on a particular computer, the larger the box within the widget.

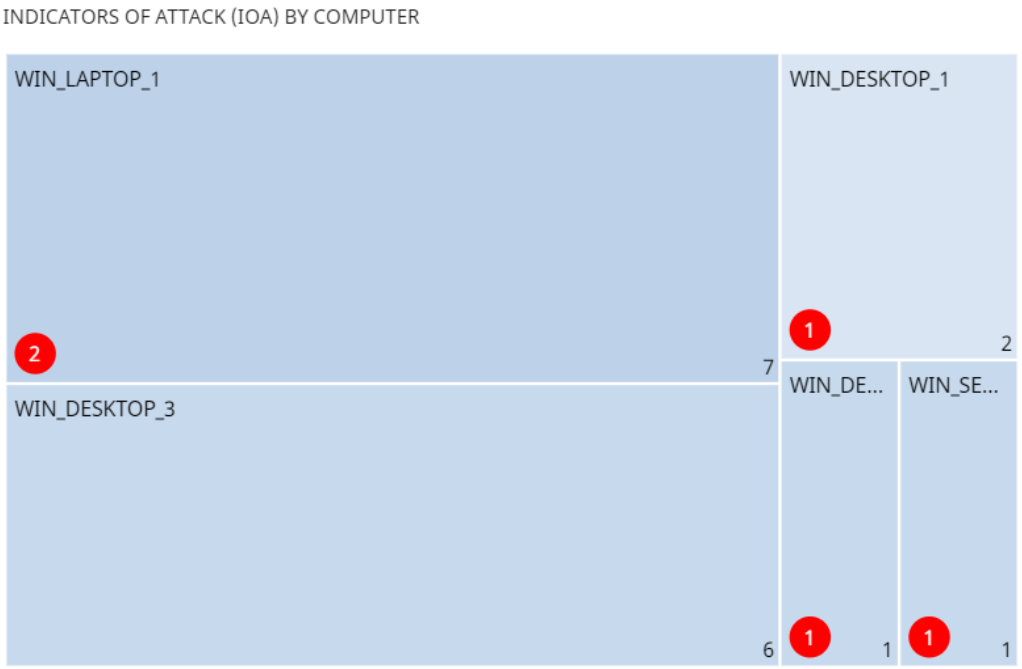


Figure 19.16: Indicators of Attack (IOA) by Computer panel

Meaning of the data displayed

Data	Description
Red number	Number of pending detections recorded on a specific computer during the selected period.
White number	Total number of recorded detections (pending + archived) on a specific computer during the selected period.

Table 19.26: Description of the data displayed in the Indicators of Attack (IOA) by Computer panel

Lists accessible from the panel

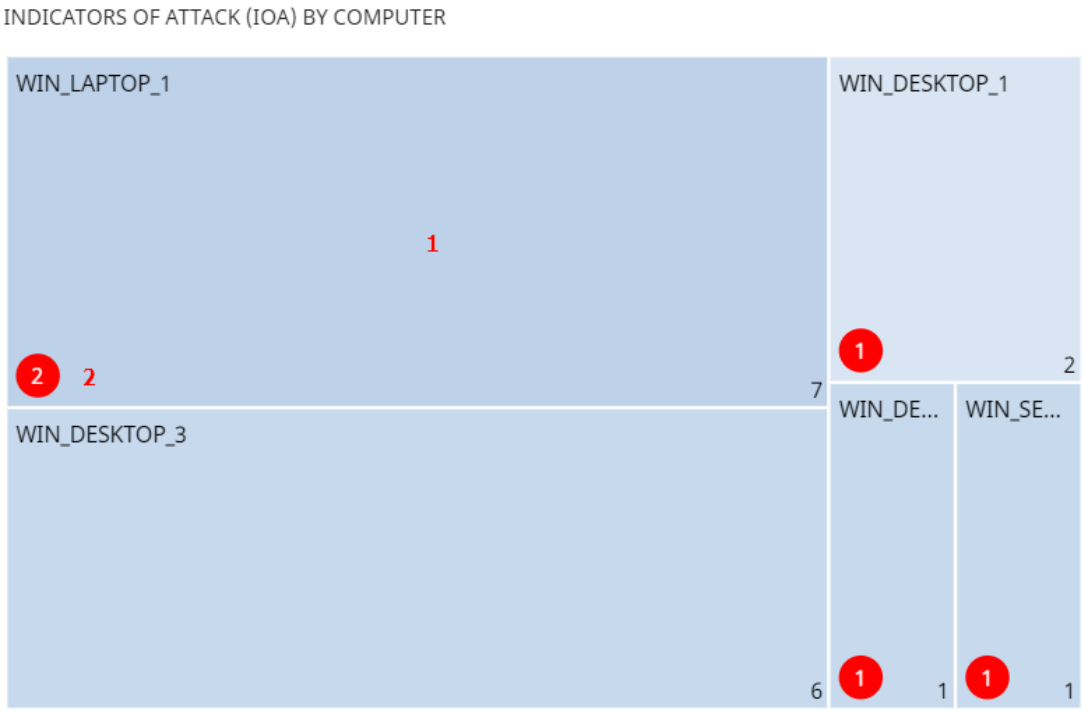


Figure 19.17: Hotspots in the Indicators of Attack (IOA) by Computer panel

Click the hotspots shown in **Figure 19.17:** to open the **Indicators of attack (IOA)** list with these predefined filters:

Hotspot	Filter
(1)	Computer
(2)	• Computer • Status = Pending

Table 19.27: Filters available in the Indicators of Attack (IOA) list

MDR service settings

The MDR service settings page appears in the Advanced EPDR console only if the customer has purchased this service from a partner. Before you fill in this form, contact your partner.

WatchGuard MDR (Managed Detection and Response) is a 24/7 cybersecurity service that enables partners to provide a managed detection and response service to customers with minimum investment in a SOC (Security Operations Center). The service monitors the security of computers in the organization, searching for threats, detecting attacks, investigating, and providing guided recommendations about how to restore affected assets and improve customer security.

The MDR service leverages innovative technologies that use artificial intelligence algorithms. Additionally, the service is fully managed by a team of cybersecurity experts, which improves customer security and cyber resilience overall and minimizes detection and response times.

For more information about the MDR module, see:
***Creating and managing settings profiles** on page **294**: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*
***Accessing, controlling, and monitoring the management console** on page **61**: Managing user accounts and assigning permissions.*

Chapter contents

MDR service settings

Accessing the settings

In the top menu, select **Settings**. In the side menu, select **MDR**. The service allows only one settings profile, which you establish at account level and applies to all computers on the managed IT network.

Required permissions

Permission	Access type
Configure MDR	Create, edit, and delete MDR settings profiles.
View MDR settings	View MDR settings profiles.

Table 19.28: Permissions required to access the MDR settings

MDR setting options

MDR settings enable customers to send partners up-to-date information about the IT network they manage. With that information, the partner can determine the cybersecurity resources they need to correctly provide the detection, protection, and response service.

To create or edit an MDR settings profile when you modify your IT infrastructure, enter the relevant information in these fields.

General

Field	Description
Customer business vertical	Specify the industry or vertical your business belongs to.
Number of business locations	Specify the number of branch offices your business has.
Number of employees	Specify the number of employees who have one or more managed devices.
Includes remote employees	Specify the number of people who have one or more managed devices and work outside the business office.

Table 19.29: MDR general settings

Technology

Field	Description
Operating systems	Specify the operating systems in use in the network. Include computers that are not protected by Cytomic products.

Field	Description
Hardware devices	Specify the vendor name and types of hardware devices in the network for early identification of possible existing vulnerabilities. Include devices not protected by Cytomic products.
Critical computers	Specify computers that provide a critical service for your business. You can add individual computers or computer groups.

Table 19.30: Network technology settings

Response plan

Field	Description
Allow WG Security Operations Center to isolate computers on the customer network	Specify whether Cytomic is authorized to use the computer isolation feature to respond to a compromised system. For more information about how to isolate computers, see **Computer isolation** on page **888**.
Exceptions	Specify computers for which Cytomic cannot use the computer isolation feature to respond to a compromised system. For more information about how to isolate computers, see **Computer isolation** on page **888**.

Table 19.31: Response plan settings

Reports

Specify email addresses to receive weekly and monthly executive reports. Separate email addresses with commas. The maximum number of email addresses you can specify for each type of report is three.

Chapter 20

Malware and network visibility

Advanced EPDR provides administrators with three large groups of tools for viewing the health and safety of the IT network they manage:

- The dashboard, with real-time, up-to-date information.
- Custom lists of incidents, detected malware, and managed devices along with their status.
- Network status reports with information collected and consolidated over time.

For more information about consolidated reports, see ***Scheduled sending of reports and lists*** *on page* ***865****.*

The visualization and monitoring tools determine, in real time, the network security status as well as the impact of any security breach that may occur in order to facilitate the implementation of appropriate security measures.

Chapter contents

Security module panels/widgets

Advanced EPDR shows an overview of the security status of the entire IT network or specific computers through widgets:

- **IT network**: From the top menu, select **Status**. From the side menu, select **Security**  . A page opens and shows counters that display the security status of the computers that are visible to you. For more information about how to set the computer groups that are visible to the account used to access the management console, see **Managing roles and permissions** on page **69**. For more information about how to restrict the visibility of the groups defined in a role, see **Filter by group icon** on page **39**.
- **Computer**: From the top menu, select **Computers**. Select a computer from the network. Select the **Detections** tab. A page opens and shows counters that display the security status of the selected computer. See **Detections section (4) for Windows, Linux, and macOS computers** on page **274**.

The following is a description of the different widgets implemented on the Advanced EPDR dashboard, their areas and hotspots, as well as their tooltips and what they mean.

Protection status

This widget shows computers where Advanced EPDR is working correctly and computers with errors or problems installing or running the product. The status of the network computers is represented with a circle with different colors and associated counters.

The bottom of the widget shows the number of computers that are in Audit more, if any. For more information, see **Audit mode** on page **359**.

The sum of all percentages can be greater than 100% as the status types are not mutually exclusive. A computer can have different statuses at the same time.

The panel provides a graphical representation and percentage of computers with the same status.

The total number of computers and devices at the center of the widget includes iOS devices. The widget includes no other information about iOS devices. iOS devices do not have advanced or antivirus protection. For more information, see ***Security settings for iOS devices** on page **366***.

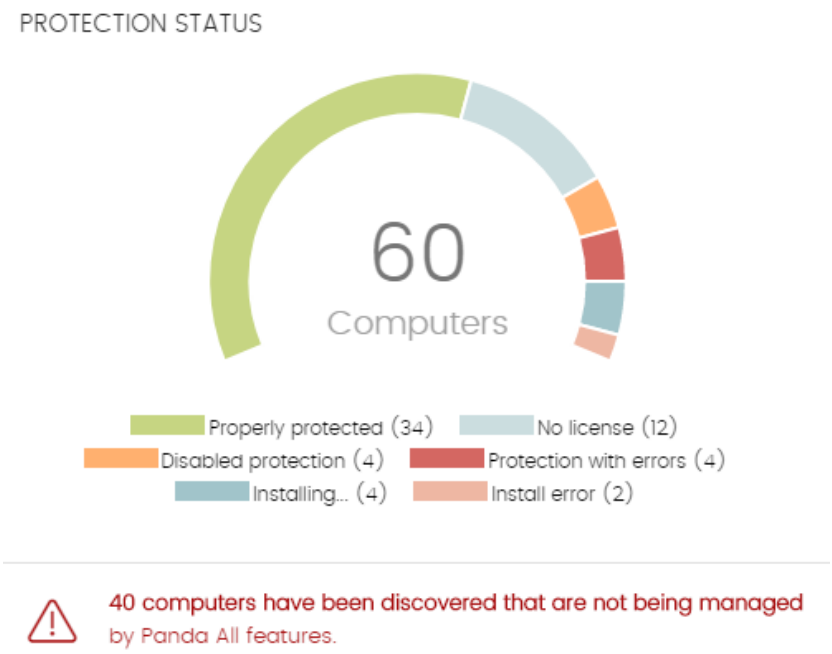


Figure 20.1: Protection Status panel

Meaning of the data displayed

Data	Description
Properly protected	Percentage of computers where Advanced EPDR installed without errors and is working correctly.
Installing...	Percentage of computers on which Advanced EPDR is currently being installed.
No license	Computers that are unprotected because there are insufficient licenses or because an available license has not been assigned to the computer.
Disabled protection	Computers where neither the antivirus protection nor the advanced protection is enabled, provided the latter is available for the operating system of the computer in question.
Protection with errors	Computers with Advanced EPDR installed, but whose protection module does not respond to the requests sent from the Cytomic servers.
Install error	Computers on which the installation process could not be completed.

Data	Description
Central area	Number of computers with a Cytomic agent installed.

Table 20.1: Description of the data displayed in the Protection Status panel

Lists accessible from the panel

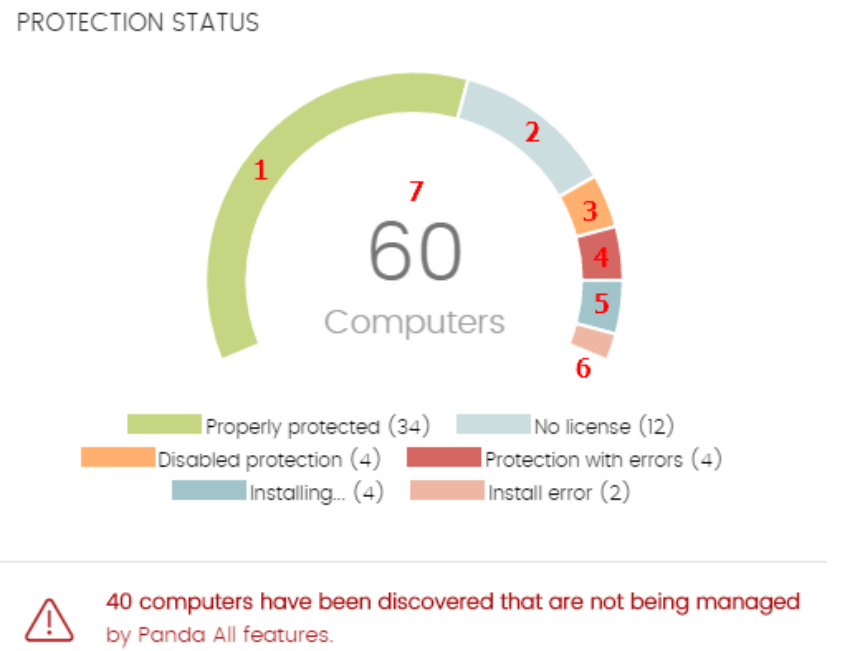


Figure 20.2: Hotspots in the Protection Status panel

Click the hotspots shown in **Figure 20.2:** to open the **Computer protection status** list with these predefined filters:

Hotspot	Filter
(1)	Protection status = Properly protected.
(2)	Protection status = Installing...
(3)	Protection status = Disabled protection.
(4)	Protection status = Protection with errors.
(5)	Protection status = No license.
(6)	Protection status = Install error.

Hotspot	Filter
(7)	No filter.

Table 20.2: Filters available in the Computer Protection Status list

Offline computers

This widget shows the number of computers that have not connected to the Cytomic cloud for a number of days. These computers might be susceptible to security problems and require attention.

Figure 20.3: Offline Computers panel

Meaning of the data displayed

Data	Description
72 hours	Number of computers that have not reported their status in the last 72 hours.
7 days	Number of computers that have not reported their status in the last 7 days.
30 days	Number of computers that have not reported their status in the last 30 days.

Table 20.3: Description of the data displayed in the Offline Computers panel

Lists accessible from the panel

Figure 20.4: Hotspots in the Offline Computers panel

Click the hotspots shown in **Figure 20.4:** to open the **Offline computers** list with these predefined filters:

Hotspot	Filter
(1)	Last connection = More than 72 hours ago.
(2)	Last connection = More than 7 days ago.
(3)	Last connection = More than 30 days ago.

Table 20.4: Filters available in the Offline Computers list

Outdated protection

This widget shows the number of computers with a signature file that is more than three days older than the latest released file. It also shows the computers with an antivirus engine that is more than seven days older than the latest released engine. These computers might be vulnerable to attacks from threats.

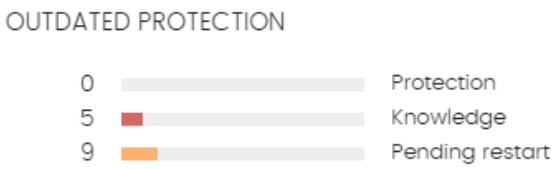


Figure 20.5: Outdated Protection panel

Meaning of the data displayed

The panel shows the percentage and number of computers that are vulnerable because their protection is out of date, under three concepts:

Data	Description
Protection	The computer has had a version of the antivirus engine older than the latest released engine for at least seven days.
Knowledge	The computer has not updated its signature file for at least three days.
Pending restart	The computer requires a restart to complete the update.

Table 20.5: Description of the data displayed in the Outdated Protection panel

Lists accessible from the panel

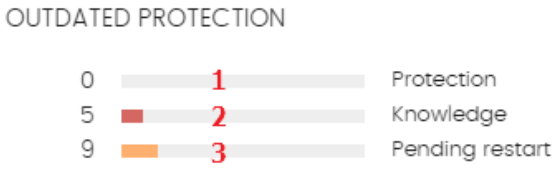


Figure 20.6: Hotspots in the Outdated Protection panel

Click the hotspots shown in **Figure 20.6:** to open the **Computer protection status** list with these predefined filters:

Hotspot	Filter
(1)	Updated protection = No.
(2)	Updated knowledge = No.
(3)	Updated protection = Pending restart.

Table 20.6: Filters available in the Computers with Out-of-Date Protection list

Malware/PUP activity

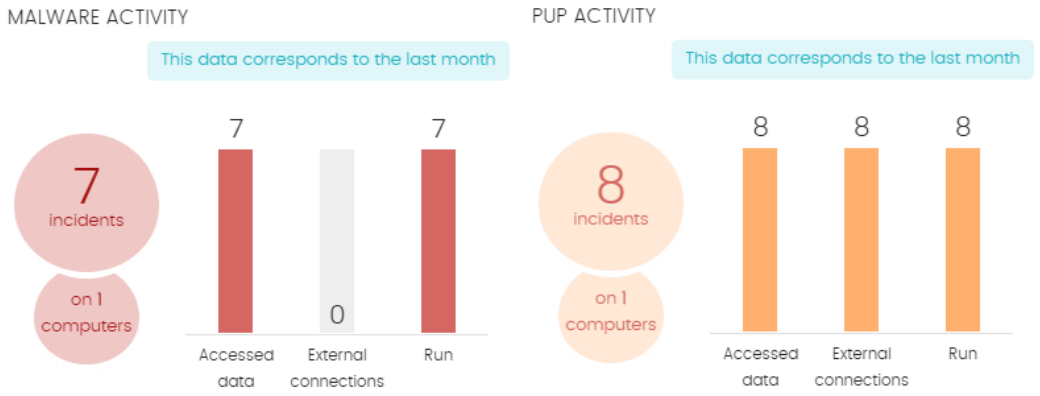


Figure 20.7: Malware/PUP Activity panel

This widget shows incidents detected in processes run by the Windows workstations and servers on the network, as well as their file systems. Incidents are reported by real-time scans.

The threats copied from computers on the network show the IP address of the computer from which an infection originated, as well as the number of times that IP address was the source of a detection (in parentheses). To open the Malware Activity list, click the IP address. See **Malware/PUP activity**.

To prevent too many detections of the same threat in the console, Advanced EPDR registers the same incident a maximum of two times every 24 hours. If an incident occurs multiple times in five minutes, the security software only registers the first incident.

For some specific types of malware, Advanced EPDR generates a maximum of five incidents every 24 hours for each computer and threat pair found on the network.

Meaning of the data displayed

Data	Description
Number of incidents	Number of incidents/alerts and number of computers where they were detected.
Accessed data	Number of alerts in which the threat accessed user information on the computer hard disk.
External connections	Number of alerts where there were connections to other computers.
Run	Number of malware that successfully ran on the network.
Threats copied from computers on the network	IP address of the computer from which an infection originated, as well as the number of times that IP address was the source of a detection.

Table 20.7: Description of the data displayed in the Malware/PUP Activity panels

The Malware Activity, PUP Activity, and Exploit Activity panels show data over a maximum period of one month. Should you set a longer time period, an explanatory text appears above the list.

Lists accessible from the panel

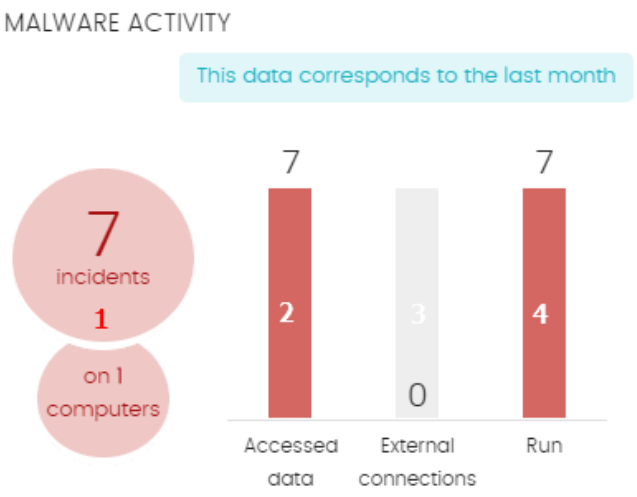


Figure 20.8: Hotspots in the Malware/PUP Activity panels

Click the hotspots shown in Figure 20.8: to open the **Malware activity** or **PUP activity** list with these predefined filters:

Hotspot	Filter
(1)	Threat type = Malware or PUP.
(2)	Accessed data = True.
(3)	External connections = True.
(4)	Run = True.

Table 20.8: Filters available in the Malware/PUP Activity list

Exploit activity

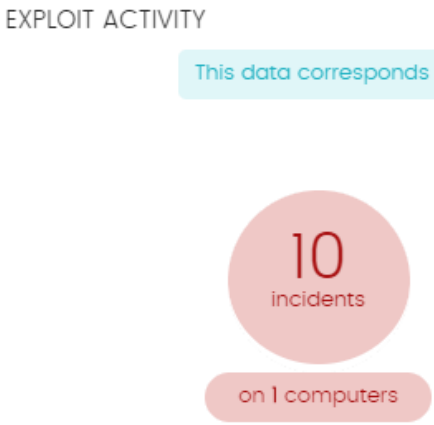


Figure 20.9: Exploit Activity panel

The Advanced EPDR Exploit Activity widget shows the number of vulnerability exploit attacks against Windows computers on the network.

Advanced EPDR reports an incident in the Exploit Activity widget for each computer and different exploit attack pair found on the network. If an attack repeats several times, the security software reports a maximum of 10 incidents reports every 24 hours for each computer-exploit pair found.

Meaning of the data displayed

Data	Description
Number of incidents/attacks	Number of incidents/attacks and number of computers where they were detected.

Table 20.9: Description of the data displayed in the Exploit Activity panel

Lists accessible from the panel

Regardless of where you click in the panel, the **Exploit activity** list opens and shows a list of all the exploits detected across the network over the last month.

Network attack activity

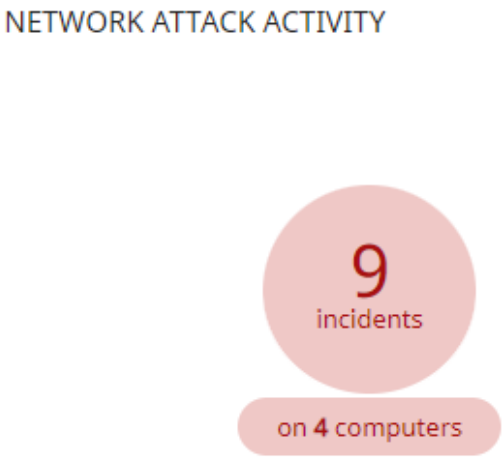


Figure 20.10: Network Attack Activity panel

This widget shows the number of attempted network attacks against Windows computers on the network.

Advanced EPDR creates a single incident per hour for each group of attacks of the same type with the same source IP address.

For more information about network attack types, see **https://www.pandasecurity.com/en/support/card?id=700145**.

Meaning of the data displayed

Data	Description
Number of incidents	Number of incidents detected.
Computers	Number of computers where network attacks were detected or blocked.

Table 20.10: Description of the data displayed in the Network Attack Activity panel

Lists accessible from the panel

Regardless of where you click in the panel, the **Network attack activity** list opens and shows a list of all the attacks over the last seven days.

Classification of all programs run and scanned

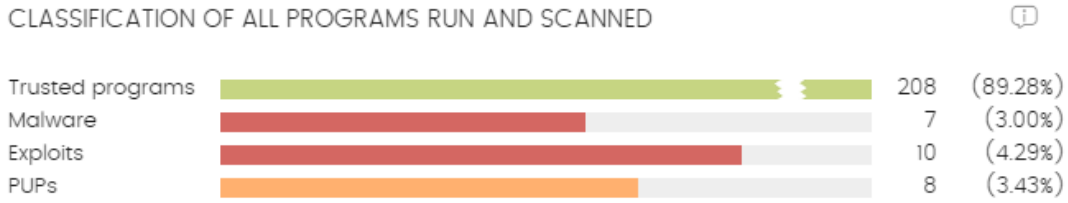


Figure 20.11: Classification of All Programs Run and Scanned panel

This widget shows the processes and programs run in your organization for the selected time period and their classification (for example, trusted programs or malware).

Meaning of the data displayed

The panel shows four horizontal bars, along with the number of events associated with each category and a percentage over the total number of events.

> *The data in this panel is for the entire IT network, not only computers that the administrator has permissions for. Programs under classification appear in the panel after the security software classifies them.*

Data	Description
Trusted programs	Programs run in the selected period that the security software classified as trusted.
Malware	Programs that tried to run in the selected period, and the security software classified as malware, zero-day threats, or targeted attacks.
Exploits	Exploit attacks that compromised or tried to compromise trusted programs on computers.
PUPs	Programs that tried to run in the selected period, and the security software classified as PUPs.

Table 20.11: Description of the data displayed in the Classification of All Programs Run and Scanned panel

Lists accessible from the panel

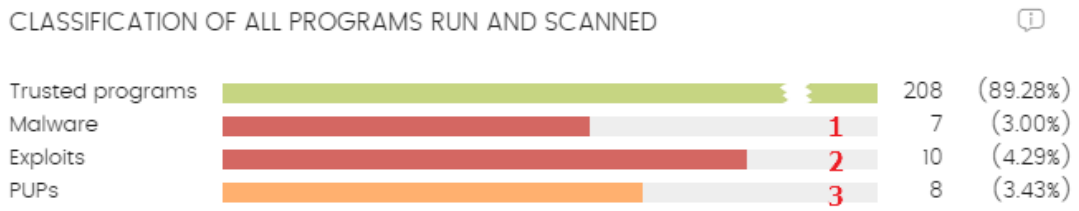


Figure 20.12: Hotspots in the Classification of All Programs Run and Scanned panel

Click the hotspots shown in **Figure 20.12:** to open lists with these predefined filters:

Hotspot	Filter
(1)	Malware activity list.
(2)	Exploit activity list.
(3)	PUP activity list.

Table 20.12: Lists accessible from the Classification of All Programs Run and Scanned panel

Detections by advanced security policies

This widget shows the total number of blocked suspicious scripts and unknown programs that used advanced infection techniques.

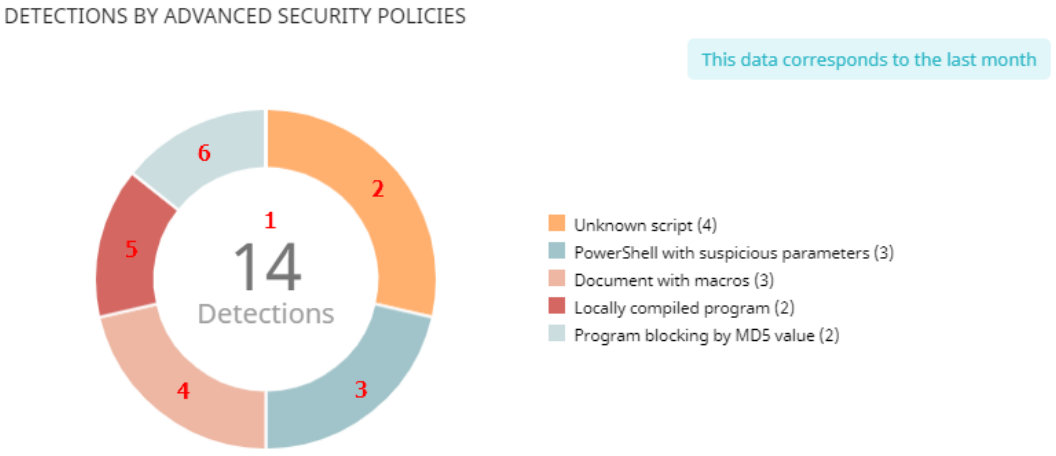


Figure 20.13: Detections by Advanced Security Policies panel

Advanced EPDR reports incidents in the Detections by Advanced Security Policies panel when it detects suspicious activities on the network.

Detection grouping

To prevent the same detection from appearing many times, Advanced EPDR reports the first detection separately. Then, all other detections of the same type made every hour after the first detection are grouped together in a single detection.

To determine if two detections are of the same type, Advanced EPDR creates a key for each detection with these data:

- Device identifier
- Advanced security policy rule that generated the detection
- MD5 hash of the item involved in the detection for these rules:
    - Unknown scripts
    - Locally compiled programs
    - Documents with macros
    - Registry modification to run when Windows starts
    - Block programs

Meaning of the data displayed

Data	Description
Detections	Total detections made by the advanced security policies.
PowerShell with suspicious parameters	Number of times the PowerShell interpreter received suspicious parameters that could result in the execution of dangerous operations on the protected computer.
PowerShell run by the user	Number of attempts to run a monitored PowerShell script by an interactive account capable of executing dangerous operations on the protected computer.
Unknown script	Number of attempts to run a script that has not yet been classified by the Cytomic security intelligence.
Locally compiled program	Number of attempts to run a program that is unknown to the Cytomic security intelligence because was compiled on the user computer.
Document with macros	Number of attempts to open an Office document with macros.
Registry modification to run when Windows starts	Number of times a program tried to add a Windows registry key to gain persistence on the computer and load itself along with the operating system on every system restart.
Program blocking	Number of times a program was blocked because it was included in the

Data	Description
by MD5 value	MD5 blocklist set by you.
Program blocking by name	Number of times a program was blocked because it was included in the name blocklist set by you.

Table 20.13: Description of the data displayed in the Detections by Advanced Security Policies panel

Lists accessible from the panel

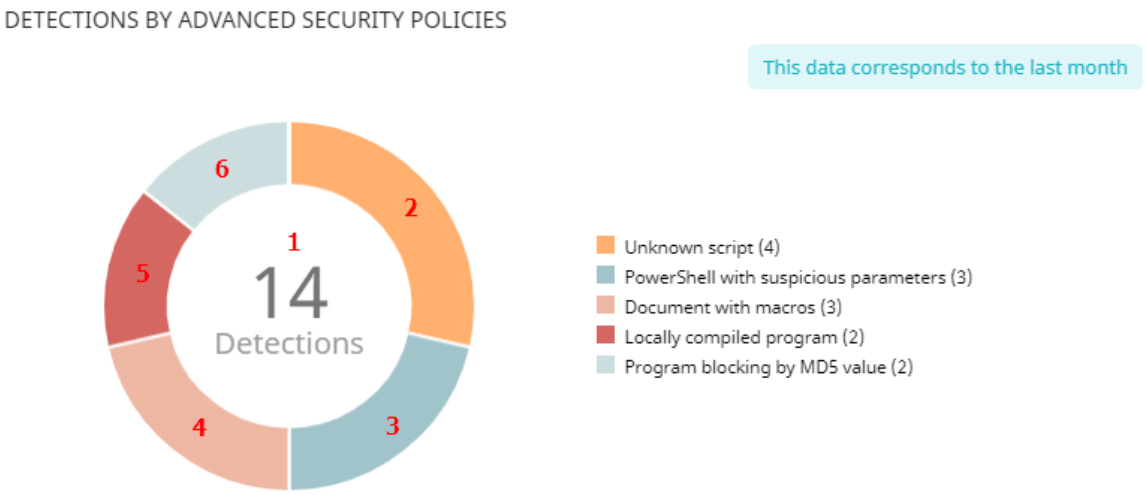


Figure 20.14: Hotspots in the Detections by Advanced Security Policies panel

Click the hotspots shown in **Figure 20.14:** to open the **Blocks by advanced security policies** list with these predefined filters:

Hotspot	Filter
(1)	No filter.
(2)	Applied policy = Unknown script.
(3)	Applied policy = PowerShell with suspicious parameters.
(4)	Applied policy = Document with macros.
(5)	Applied policy = Locally compiled program.
(6)	Applied policy = Program blocking by MD5 value.

Table 20.14: Filters available in the Blocks by Advanced Security Policies list

Threats detected by the antivirus

This widget shows all intrusion attempts that Advanced EPDR detected in the selected time period.

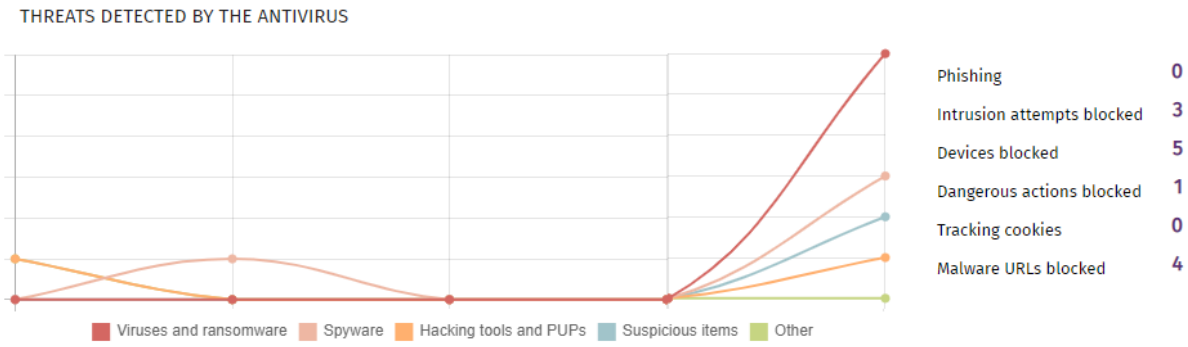


Figure 20.15: Threats Detected by the Antivirus panel

The data covers all infection vectors and all supported platforms. Administrators can get specific data (volume, type, form of attack) related to the malware.

Meaning of the data displayed

This panel includes two sections: a line chart and a summary list.

The line chart represents detections on the network over time, split into malware categories:

Data	Description
Viruses and ransomware	Programs that enter computers and IT systems in a number of ways, causing effects that range from simply annoying to highly destructive and irreparable.
Hacking tools and PUPs	Programs used by hackers to perform actions that cause problems for the user of the affected computer (control the computer, steal confidential information, scan communication ports, etc.).
Suspicious items	Files with a high probability of being malware after having been analyzed by our heuristic technologies. This type of technology is used only in the on-demand scans performed from scheduled tasks. In this type of scan, the investigated file is not executed. Therefore, the security software has far less information to evaluate the file's behavior, which reduces the classification accuracy. To compensate for the reduced accuracy of the static scan, the heuristic technologies are used.
Phishing	A technique for obtaining confidential information from users fraudulently. The targeted information includes passwords, credit card numbers, and bank account details.

Data	Description
Other	Hoaxes, worms, Trojans, and other types of viruses.

Table 20.15: Description of the data displayed in the Threats Detected by the Antivirus panel

The list to the right of the chart shows events that you might want to monitor to look for symptoms or potentially dangerous situations.

Data	Description
Dangerous actions blocked	Detections made by analyzing local behavior.
Intrusion attempts blocked	Detections of malformed network traffic specially crafted to cause an execution error in one of the components on the targeted computer that leads to unwanted system behavior.
Devices blocked	Detection of a user attempt to use a device whose access is restricted according to the settings established by the network administrator in the Device Control module.
Tracking cookies	Detection of cookies used to track the web activity of users.
Malware URLs blocked	Web addresses that point to pages containing malware.

Table 20.16: Description of the data displayed in the Threats Detected by the Antivirus panel

Lists accessible from the panel

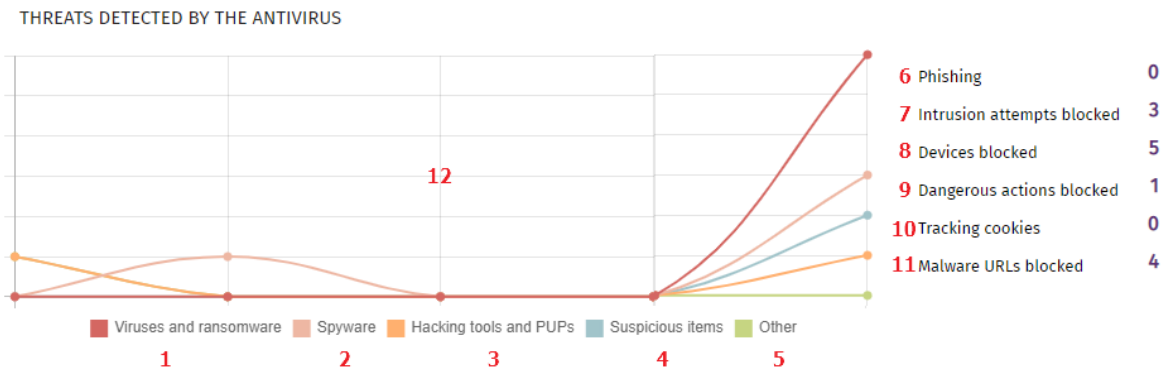


Figure 20.16: Hotspots in the Threats Detected by the Antivirus panel

Click the hotspots shown in **Figure 20.16:** to access these list with these predefined filters:

Hotspot	List	Filter
(1)	Threats detected by the antivirus.	Threat type = Viruses and ransomware.
(2)	Threats detected by the antivirus.	Threat type = Spyware.
(3)	Threats detected by the antivirus.	Threat type = Hacking tools and PUPs.
(4)	Threats detected by the antivirus.	Threat type = Suspicious items.
(5)	Threats detected by the antivirus.	Threat type = Other.
(6)	Threats detected by the antivirus.	Threat type = Phishing.
(7)	Intrusion attempts blocked	No filter.
(8)	Devices blocked	No filter.
(9)	Threats detected by the antivirus.	Threat type = Dangerous actions blocked.
(10)	Threats detected by the antivirus.	Threat type = Tracking cookies.
(11)	Threats detected by the antivirus.	Threat type = Malware URLs.
(12)	Threats detected by the antivirus.	No filter.

Table 20.17: Filters available in the Threats Detected by the Antivirus list

Web access

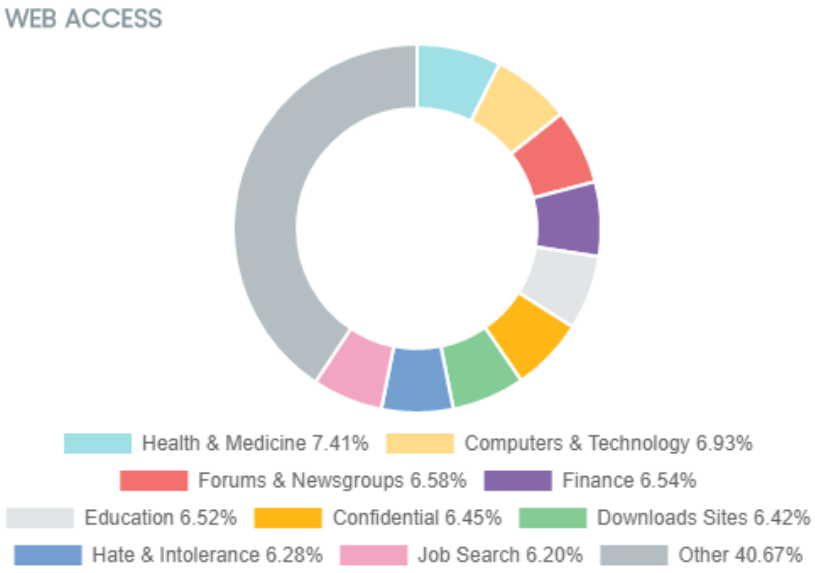


Figure 20.17: Web Access panel

This widget shows a pie chart with the categories of web pages most visited by users on the network.

Meaning of the data displayed

The pie chart shows the ten most visited web page categories supported by Advanced EPDR when categorizing the pages accessed by users.

The pie chart key shows the percentage of web page requests for each category.

Lists accessible from the panel

Click the categories shown in **Figure 20.17:** to open the **Web access by computer** list with these predefined filters:

Hotspot	Filter
Any	Category = Selected category.

Table 20.18: Filters available in the Web Access by Computer list

Top 10 most accessed categories

This widget shows the number of visits and the number of computers that have accessed the 10 most visited web page categories.

Each category shows the total number of visits in the selected date range, and the number of computers that accessed it one or more times.

Top 10 most accessed categories

Category	Access attempts	Computers
Health & Medicine	1,153	11
Hate & Intolerance	1,124	11
Illegal Drugs	1,049	11
Dating & Personals	1,014	10
Gambling	1,013	11
Finance	1,009	10
Criminal Activity	983	11
Government	972	10
Downloads Sites	957	11
Streaming Media & Downloads	953	10

See full report

Figure 20.18: Most Accessed Categories panel

Lists accessible from the panel

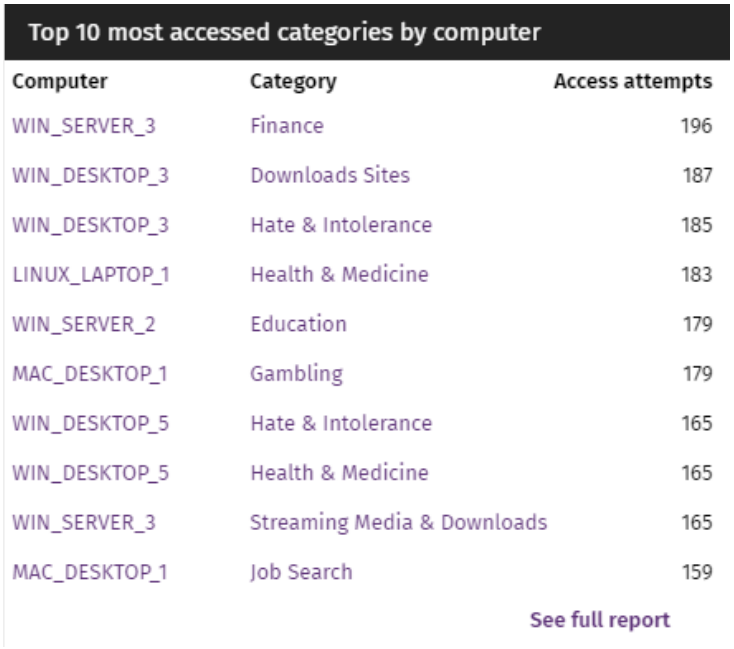
Click the panel to open the **Web access by computer** list with different predefined filters depending on the area clicked.

Hotspot	Filter
Category	Category = Selected category.
See full report	Opens the Web Access by Category list with no filters.

Table 20.19: Filters available in the Web Access by Computer list

Top 10 most accessed categories by computer

This widget shows the number of web page visits, ordered by category, of the 10 computers that used the Web the most.



Top 10 most accessed categories by computer

Computer	Category	Access attempts
WIN_SERVER_3	Finance	196
WIN_DESKTOP_3	Downloads Sites	187
WIN_DESKTOP_3	Hate & Intolerance	185
LINUX_LAPTOP_1	Health & Medicine	183
WIN_SERVER_2	Education	179
MAC_DESKTOP_1	Gambling	179
WIN_DESKTOP_5	Hate & Intolerance	165
WIN_DESKTOP_5	Health & Medicine	165
WIN_SERVER_3	Streaming Media & Downloads	165
MAC_DESKTOP_1	Job Search	159

See full report

Figure 20.19: Top 10 Most Accessed Categories by Computer panel

Lists accessible from the panel

Click the hotspots shown in figure **Figure 20.19:** to open the **Web access by computer** list with these predefined filters:

Hotspot	Filter
Computer	Computer = Selected computer.
Category	Category = Selected category.
See full list	No filter.

Table 20.20: Filters available in the Web Access by Computer list

Top 10 most blocked categories

This widget shows the 10 most frequently blocked web page categories, the number of access attempts blocked, and the number of computers that tried to access them and were blocked.

Top 10 most blocked categories

Category	Denied access attempts	Computers
Health & Medicine	1,157	11
Criminal Activity	1,123	11
Hate & Intolerance	1,062	11
Finance	1,020	10
Government	999	10
Illegal Drugs	985	11
Computers & Technology	929	11
Gambling	918	11
Entertainment	915	10
Unknown	908	11

See full report

Figure 20.20: Hotspots in the Most Blocked Categories panel

Lists accessible from the panel

Click the hotspots shown in **Figure 20.20:** to open the **Web access by computer** list with these predefined filters:

Hotspot	Filter
Category	Category = Selected category.
See full list	Opens the Web Access by Category list with no filters.

Table 20.21: Filters available in the Web Access by Computer list

Top 10 most blocked categories by computer

This widget shows the computer-category pairs with the most visits blocked, the name of the computer, the web content category, and the number of access attempts denied for each computer-category pair.

Top 10 most blocked categories by computer

Computer	Category	Denied access attempts
LINUX_LAPTOP_1	Health & Medicine	198
WIN_DESKTOP_5	Criminal Activity	184
WIN_SERVER_2	Unknown	181
LINUX_LAPTOP_1	Job Search	181
WIN_DESKTOP_2	Hate & Intolerance	179
WIN_DESKTOP_5	Health & Medicine	179
WIN_SERVER_3	Finance	178
WIN_SERVER_2	Education	173
MAC_DESKTOP_1	Job Search	171
WIN_DESKTOP_3	Hate & Intolerance	165

Figure 20.21: Top 10 Most Blocked Categories by Computer panel

Lists accessible from the panel

Click the hotspots shown in **Figure 20.21:** to open the **Web access by computer** list with these predefined filters:

Hotspot	Filter
Computer	Computer name = Selected computer.
Category	Category = Selected category.
See full list	No filter.

Table 20.22: Filters available in the Web Access by Computer list

Security module lists

The security lists show the information collected by Advanced EPDR in connection with computer protection activities. They provide highly detailed information because they contain the raw data used to generate the widgets.

There are two ways to access the security lists:

- From the top menu, select **Status**. From the side panel, select **Security**. Click any of the available widgets to access its associated list. Depending on the item you click on the widget, you access different lists with predefined filters.

  Or

- From the top menu, select **Status**. From the **My lists** side panel, click **Add**. A dialog box opens that shows all lists available in Advanced EPDR.
- Select any of the lists in the **Security** section. The list opens with no filters applied.

Select any of the entries on the list to open a new page with more details about that particular item.

Computer protection status

This list shows all computers on the network, with filters that enable you to search for computers and mobile devices that are unprotected for some specific reason.

To ensure correct operation of the security software, the computers on the network must communicate with the Cytomic cloud. For the list of URLs that must be accessible from your computers, see section **Access to service URLs** on page **953**.

Field	Description	Values
Computer	Computer name.	Character string
Computer status	Agent reinstallation: •  Reinstalling the agent. •  Agent reinstallation error. Protection reinstallation: •  Reinstalling the protection. •  Protection reinstallation error. •  Pending restart. Computer isolation status: •  Computer in the process of being isolated. •  Isolated computer. •  Computer in the process of stopping being isolated. "RDP attack containment" mode:	Icon

Field	Description	Values
	•  Computer in "RDP attack containment" mode. •  Ending "RDP attack containment" mode. Verbose mode: •  Computer in Verbose mode.	
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string •  'All' group •  Native group •  Active Directory group
Advanced protection	Advanced protection status.	•  Installing •  Error. If it is a known error, the cause of the error appears. If it is an unknown error, the error code appears instead. •  Enabled •  Disabled •  No license
Antivirus	Antivirus protection status.	•  Installing •  Error. If it is a known error, the cause of the error appears. If it is an unknown error, the error code appears instead. •  Enabled

Field	Description	Values
		• Disabled • No license
Updated protection	Indicates whether or not the installed protection module is updated to the latest version released. Point the mouse to the field to see the version of the installed protection.	• Updated • Not updated (7 days without updating since last release) • Pending restart
Knowledge	Indicates whether or not the signature file found on the computer is updated to the latest version. Point the mouse to the field to see the date that the file was last updated.	• Updated • Not updated (3 days without updating since last release)
Connection to knowledge	Indicates whether the computer can communicate with the Cytomic cloud to send monitored events and download security intelligence.	• Connection OK • One or more services are not accessible • — Information not available
Last connection	Date when the Advanced EPDR status was last sent to the Cytomic cloud.	Date

Table 20.23: Fields in the Computer Protection Status list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation

Field	Description	Values
		• Laptop • Server • Mobile device
Computer	Computer name.	Character string
IP address	The computer primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer.	Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Agent version	Internal version of the Cytomic agent module.	Character string
Installation date	Date when the Advanced EPDR software was successfully installed on the computer.	Date
Last update on	Date the agent was last updated.	Date
Platform	Operating system installed on the computer.	• Windows • Linux • macOS • Android
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string
Updated protection	Indicates whether or not the installed protection module is updated to the latest version	Binary value

Field	Description	Values
	released.	
Protection version	Internal version of the protection module.	Character string
Updated knowledge	Indicates whether or not the signature file found on the computer is the latest version.	Binary value
Last update on	Date the signature file was last updated.	Date
Advanced protection **File antivirus** **Mail antivirus** **Web browsing antivirus** **Firewall Device control** **Web access control** **Program blocking** **Anti-Theft**	Status of the associated protection.	• **Not installed** • **Error**: If it is a known error, the cause of the error appears. If it is an unknown error, the error code appears instead. • **Enabled** • **Disabled** • **No license**
Advanced protection mode (Windows)	Current configuration of the advanced protection module. Operating mode.	• Audit • Hardening • Lock
Advanced protection mode (Linux)	Current configuration of the advanced protection module. Malicious activity detection.	• Audit • Do not detect • Block
Isolation status	Indicates whether or not the computer is isolated from the rest of the network.	• Isolated • Not isolated
Error date	If an error occurred installing	Date

Field	Description	Values
	Advanced EPDR, date and time of the error.	
Installation error	If an error occurred installing Advanced EPDR, error description.	Character string
Installation error code	Shows codes that identify the installation error occurred.	Codes are separated by ";": • Error code • Extended error code • Extended error subcode
Other security products	Name of any third-party antivirus product found on the computer at the time of installing Advanced EPDR.	Character string
Connection for web protection	Shows the status of the connection between the computer and the servers that store the dangerous URL database.	• OK • With problems
Connection for collective intelligence	Shows the status of the connection between the computer and the servers that store signature files and security intelligence.	• OK • With problems
Connection for sending events	Shows the status of the connection between the computer and the servers that receive the events monitored on protected computers.	• OK • With problems
"RDP attack containment" mode	Status of the "RDP attack containment" mode.	• All • No • Yes

Table 20.24: Fields in the Computer Protection Status exported file

Filter tool

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Search computer	Computer name.	Character string
Last connection	Date when the Advanced EPDR status was last sent to the Cytomic cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago
Updated protection	Indicates whether or not the installed protection is updated to the latest version released.	• All • Yes • No • Pending restart
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS • Android

Field	Description	Values
Updated knowledge	Indicates whether or not the signature file found on the computer is the latest version.	Binary value
Connection to knowledge servers	Indicates whether the computer can communicate with the Cytomic cloud to send monitored events and download security intelligence.	• **All** • **OK** • **With problems**: One or more services are not accessible
Protection status	Status of the protection module installed on the computer.	• Installing... • Properly protected • Protection with errors • Disabled protection • No license • Install error
Isolation status	Computer isolation status.	• Not isolated • Isolated • Isolating • Stopping isolation
"RDP attack containment" mode	Status of the "RDP attack containment" mode.	• All • No • Yes

Table 20.25: Filters available in the Computer Protection Status list

Computer Details page

Click a row in the list to open the computer details page. For more information, see **Computer details** on page **252**.

Malware/PUP activity

This list shows the threats detected on the computers protected by Advanced EPDR. It provides you with the necessary information to find the source of a problem, assess the severity of an incident and, if required, take the necessary remediation measures and update the organization security policies.

Field	Comment	Values
Computer	Name of the computer where the threat was detected.	Character string
Threat	Name of the detected threat.	Character string
Path	Full path to the infected file.	Character string
Run sometime	The threat ran and the computer might be compromised.	Binary value
Accessed data	The threat accessed data on the user computer.	Binary value
Made external connections	The threat communicated with remote computers to send or receive data.	Binary value
Action	Action taken on the malware.	• Quarantined • Blocked • Disinfected • Deleted • Detected • Allowed (audit mode)
Date	Date when the threat was detected on the computer.	Date

Table 20.26: Fields in the Malware/PUP Activity list

Fields displayed in the exported file

The context menu of the Malware/PUP Activity list shows two options: Export and Export List and Details. This section describes the content of the file generated when you select Export. For more information about the Export List and Details option, see ***Exported Excel files*** *on page* ***844****.*

Field	Comment	Values
Computer	Name of the computer where the threat was detected.	Character string
Threat	Name of the detected threat.	Character string
Path	Full path to the infected file.	Character string
Action	Action taken on the malware.	• Quarantined • Blocked • Disinfected • Deleted • Allowed • Allowed (audit mode)
Run	The threat ran and the computer might be compromised.	Binary value
Accessed data	The threat accessed data on the user computer.	Binary value
External connections	The threat communicated with remote computers to send or receive data.	Binary value
Excluded	The threat was excluded by you to allow it to run.	Binary value
Date	Date when the threat was detected on the computer.	Date
Dwell time	Time that the threat was on the customer network	Character string

Field	Comment	Values
	without classification.	
User	User account under which the threat was run.	Character string
MD5	MD5 hash of the detected file.	Character string
SHA-256	SHA-256 hash of the detected file.	Character string
Infection source computer	Name of the computer, if the infection attempt originated from another computer on the customer network.	Character string
Infection source IP address	IP address of the computer, if the infection attempt originated from another computer on the customer network.	Character string
Infection source user	The user that was logged in to the computer the infection attempt originated from, if applicable.	Character string

Table 20.27: Fields in the Malware/PUP Activity exported file

Filter tool

Field	Comment	Values
Search	• **Computer**: Device on which the threat was detected. • **Threat**: Name of the threat. • **Hash**: String that identifies the file. • **Infection source**: Search by the user, IP address, or name of the computer the infected file came from.	Character string
Type	Type of threat.	• Malware • PUP
Dates	Set a time period, from the current moment back.	• Last 24 hours • Last 7 days

Field	Comment	Values
		• Last month • Last year
Run	The threat ran and the computer might be compromised.	Binary value
Action	Action taken on the threat.	• Quarantined • Blocked • Disinfected • Deleted • Allowed • Detected
Accessed data	The threat accessed data on the user computer.	Binary value
External connections	The threat communicated with remote computers to send or receive data.	Binary value

Table 20.28: Filters available in the Malware/PUP Activity list

Details page

This page shows detailed information about the program classified as malware/PUP. See **Malware and PUP detection** on page **820**.

Exploit activity

This list shows all computers with programs compromised by vulnerability exploit attempts. It provides you with the necessary information to find the source of a problem, assess the severity of an incident and, if required, take the necessary remediation measures and update the organization security policies.

Field	Comment	Values
Computer	Name of the computer where the threat was detected.	Character string
Compromised program or driver	Program affected by the exploit attack, or vulnerable driver loaded.	Character string

Field	Comment	Values
Exploit technique	Identifier of the technique used to exploit the program or driver vulnerability.	Character string
Exploit run	Indicates whether the exploit managed to run or was blocked before it could affect the vulnerable program.	Binary value
Action	• **Allowed (audit mode)**: The user is informed that the exploit has carried out its programmed actions. Because audit mode is enabled, threats are detected, but they are not blocked or removed. See **Audit mode** on page **359** • **Allowed**: The anti-exploit protection is configured in Audit mode. The exploit ran. • **Allowed**: The anti-exploit protection is configured in Audit mode. The exploit ran. Not applicable if the exploit technique is **Vulnerable driver**. • **Blocked**: The exploit was blocked before it could run. • **Allowed by the user**: The computer user was asked for permission to end the compromised process, but decided to let the exploit run. • **Process ended**: The exploit was deleted, but managed to partially run. Not applicable if the exploit technique is **Vulnerable driver**. • **Pending restart**: The user was informed of the need to restart the computer to completely remove the exploit. In the meantime, the exploit continues to run. Not applicable if the exploit technique is **Vulnerable driver**.	Enumeration
Date	Date when the exploit attempt was detected on the computer.	Date

Table 20.29: Fields in the Exploit Activity list

Fields displayed in the exported file

The context menu of the Exploit Activity list shows two options: Export and Export List and Details. This section describes the content of the file generated when you select Export. For more information about the Export List and Details option, see ***Exported Excel files*** *on page* ***844****.*

Field	Comment	Values
Computer	Name of the computer where the threat was detected.	Character string
Compromised program or driver	Program affected by the exploit attack, or vulnerable driver loaded.	Character string
Exploit technique	Identifier of the technique used to exploit the program vulnerability.	Enumeration
User	User account under which the program that received the exploit attack was run.	Character string
Action	• **Allowed**: The anti-exploit protection is configured in Audit mode. The exploit ran. Not applicable if the exploit technique is **Vulnerable driver**. • **Blocked**: The exploit was blocked before it could run. • **Allowed by the user**: The computer user was asked for permission to end the compromised process, but decided to let the exploit run. • **Process ended**: The exploit was deleted, but managed to partially run. Not applicable if the exploit technique is **Vulnerable driver**. • **Pending restart**: The user was informed of the need to restart the computer to completely remove the exploit. In the meantime, the exploit continues to run. Not applicable if the exploit technique **Vulnerable driver**. • **Allowed (Audit mode)**: The user is informed that	Enumeration

Field	Comment	Values
	the exploit carried out its programmed actions. Because Audit mode is enabled, threats are detected, but they are not blocked or removed. See **Audit mode** on page **359**.	
Exploit run	Indicates whether the exploit managed to run or was blocked before it could affect the vulnerable program.	Binary value
Date	Date when the exploit attempt was detected on the computer.	Date

Table 20.30: Fields in the Exploit Activity exported file

Filter tool

Field	Comment	Values
Search	• **Computer**: Device on which the threat was detected. • **Hash**: String that identifies the compromised program. • **Compromised program:** Name or path of the compromised file.	Enumeration
Dates	Set a time period, from the current moment back.	• Last 24 hours • Last 7 days • Last month
Exploit run	Indicates whether the exploit managed to run or was blocked before it could affect the vulnerable program.	Binary value
Action	• **Allowed (Audit mode)**: The user is informed that the exploit carried out its programmed actions. Because Audit mode is enabled, threats are detected, but they are not blocked or removed. See **Audit mode** on page **359**. • **Allowed**: The anti-exploit protection is configured in Audit mode. The exploit ran. Not applicable if the exploit technique is **Vulnerable driver**.	Enumeration

Field	Comment	Values
	• **Blocked**: The exploit was blocked before it could run. • **Allowed by the user**: The computer user was asked for permission to end the compromised process, but decided to let the exploit run. • **Process ended**: The exploit was deleted, but managed to partially run. Not applicable if the exploit technique is **Vulnerable driver**. • **Pending restart**: The user was informed of the need to restart the computer to completely remove the exploit. In the meantime, the exploit continues to run. Not applicable if the exploit technique is **Vulnerable driver**.	

Table 20.31: Filters available in the Exploit Activity list

Details page

This page shows detailed information about the program classified as an exploit. See **Exploit detection** on page **823**.

If the exploit technique is **Vulnerable driver**, see **Vulnerable driver** on page **826**

Blocks by advanced security policies

This list shows all programs blocked by advanced security policies. These policies prevent the execution of scripts and unknown programs that use advanced infection techniques.

Field	Comment	Values
Computer	Name of the computer where the threat was detected.	Character string
User	User account under which the threat tried to run.	Character string
Path	Full path to the blocked file.	Character string
Action	Action taken on the file.	• Detected • Blocked • Allowed (audit mode)
Policy	For more information, see **Advanced**	• PowerShell with suspicious

Field	Comment	Values
	security policies on page **336**.	parameters • PowerShell run by the user • Unknown script • Locally compiled program • Document with macros • Registry modification to run when Windows starts • Program blocking by MD5 value • Program blocking by name
Date	Date when the threat was detected on the computer.	Date

Table 20.32: Fields in the Blocks by Advanced Security Policies list

Fields displayed in the exported file

*The context menu of the Blocks by Advanced Security Policies list shows two options: Export and Export List and Details. This section describes the content of the file generated when you select Export. For more information about the Export List and Details option, see **Exported Excel files** on page **844**.*

Field	Comment	Values
Computer	Name of the computer where the threat was detected.	Character string
Policy	For more information, see **Advanced security policies** on page **336**.	• PowerShell with suspicious parameters • PowerShell run by the user • Unknown script • Locally compiled program • Document with macros

Field	Comment	Values
		• Registry modification to run when Windows starts • Program blocking by MD5 value • Program blocking by name
Path	Full path to the file.	Character string
Action	Action taken on the file.	• Detected • Blocked • Allowed (audit mode)
Date	Date when the threat was detected on the computer.	Date
User	User account under which the threat tried to run.	Character string
MD5	MD5 hash of the blocked program.	Character string
SHA-256	SHA-256 hash of the blocked program.	Character string

Table 20.33: Fields in the Blocks by Advanced Security Policies exported file

Filter tool

Field	Comment	Values
Search	• **Computer**: Name of the device where the detection was made. • **Compromised program**: Name of the program blocked by the security policy. • **User**: Searches by the name of the user that was logged in to the computer at the time the detection was made.	Character string
Dates	Set a time period, from the current moment back.	• Last 24 hours • Last 7 days

Field	Comment	Values
		• Last month • Last year
Action	Action taken on the threat.	• Blocked • Detected
Policy applied	For more information, see **Advanced security policies** on page **336**.	• PowerShell with suspicious parameters • PowerShell run by the user • Unknown script • Locally compiled program • Document with macros • Registry modification to run when Windows starts • Program blocking by MD5 value • Program blocking by name

Table 20.34: Filters available in the Blocks by Advanced Security Policies list

Details page

This page shows detailed information about the program blocked by the advanced security policies. See **Block by advanced security policy** on page **828**.

Threats detected by the antivirus

This list provides complete, consolidated information about all detections made on all supported platforms and for all infection vectors used by hackers to infect computers on the network.

Field	Description	Values
Computer	Name of the computer where the threat was detected.	Character string
IP address	The computer primary IP address.	Character string
Group	Group within the Advanced EPDR group tree that the computer belongs to.	Character string • 'All' group • Native group • Active Directory group
Threat type	Type of detected threat.	• Viruses and ransomware • Spyware • Hacking tools and PUPs • Phishing • Suspicious items • Dangerous actions blocked • Tracking cookies • Malware URLs • Other
Path	Location of the threat on the file system.	Character string
Action	Action taken by Advanced EPDR.	• Deleted • Disinfected • Quarantined • Blocked • Process ended • Allowed (audit mode)

Field	Description	Values
Date	Date when the attack was detected.	Date

Table 20.35: Fields in the Threats Detected by the Antivirus list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Computer	Name of the computer where the threat was detected.	Character string
Malware name	Name of the detected threat.	Character string
Threat type	Type of detected threat.	• Viruses and ransomware • Spyware • Hacking tools and PUPs • Phishing • Suspicious items • Dangerous actions blocked • Tracking cookies • Malware URLs • Other
Malware type	Threat subclass.	Character string
Action	Action taken by Advanced EPDR.	• Quarantined

Field	Description	Values
		• Deleted • Blocked • Process ended • Allowed (audit mode)
Detected by	Engine that detected the threat.	• Device control • File protection • Firewall • Mail protection • On-demand scan • Web access control • Web protection
Detection path	Location of the threat on the file system.	Character string
Excluded	The threat was excluded from the scans by the administrator to allow it to run.	Binary value
Date	Date when the attack was detected.	Date
Group	Group within the Advanced EPDR group tree that the computer belongs to.	Character string
IP address	Primary IP address of the computer where the detection was made.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by the network administrator.	Character string

Table 20.36: Fields in the Threats Detected by the Antivirus exported file

Filter tool

Field	Description	Values
Computer	Name of the computer where the threat was detected.	Character string
Dates	**Range**: Set a time period, from the current moment back. **Custom range**: Choose specific dates from a calendar.	• Last 24 hours • Last 7 days • Last month • Last year
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Threat type	Type of threat.	• Viruses and ransomware • Spyware • Hacking tools and PUPs • Phishing • Suspicious items • Dangerous actions blocked • Tracking cookies • Malware URLs • Other

Table 20.37: Filters available in the Threats Detected by the Antivirus list

Details page

This page shows detailed information about the detected virus.

Field	Description	Values
Threat	Threat name.	Character string

Field	Description	Values
Action	Action taken by Advanced EPDR. See **Restoring files from quarantine** on page **816**.	• Quarantined • Deleted • Blocked • Process ended • Allowed (audit mode)
Computer	Name of the computer where the threat was detected. It includes a link to the Computer Details page.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
IP address	The computer primary IP address.	Character string
Logged-in user	Operating system user under which the threat was loaded and run.	Character string
Detection path	Location of the threat on the file system.	Character string
Name	Threat name.	Character string
Threat type	Type of threat.	Character string
Malware type	Type of malware.	• Viruses and ransomware • Spyware • Hacking tools and PUPs • Phishing • Suspicious items

Field	Description	Values
		• Dangerous actions blocked • Tracking cookies • Malware URLs • Other
Detected by	Module that detected the item.	
Date	Date when the attack was detected.	Date

Table 20.38: Details accessible from the Threats Detected by the Antivirus list

Blocked devices

This list provides details of the network computers that have restricted access to peripherals.

Field	Description	Values
Computer	Computer name.	Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	• Character string •  'All' group •  Native group •  Active Directory group
Name	Name assigned manually to the device by you to make identification easier.	Character string
Type	Type of device affected by the security settings.	• Removable storage drives • Imaging devices • CD/DVD drives • Bluetooth devices

Field	Description	Values
		• Modems • Mobile devices
Action	Action taken on the device.	• Block • Allow read access • Allow read and write access
Date	Date and time when the action was taken.	Date

Table 20.39: Fields in the Blocked Devices list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Computer	Computer name.	Character string
Original name	Name of the blocked device.	Character string
Name	Name assigned to the device by you.	Character string
Type	Type of device.	• Removable storage drives • Imaging devices • CD/DVD drives • Bluetooth devices • Modems

Field	Description	Values
		• Mobile devices
Instance ID	ID of the affected device.	Character string
Number of detections	Number of times the disallowed operation was detected on the device.	Numeric value
Action	Action taken on the device.	• Block • Allow read access • Allow read and write access
Detected by	Module that detected the disallowed operation.	Device control
Date	Date when the disallowed operation was detected.	Date
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
IP address	The computer primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by you.	Character string

Table 20.40: Fields in the Blocked Devices exported file

Filter tool

Field	Description	Values
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Search	Computer name.	Character string

Field	Description	Values
computer		
Dates	• **Range**: Set a time period, from the current moment back. • **Custom range**: Choose specific dates from a calendar.	• Last 24 hours • Last 7 days • Last month
Device type	Type of device affected by the security settings.	• Removable storage drives • Imaging devices • CD/DVD drives • Bluetooth devices • Modems • Mobile devices
Name	Device name.	Character string

Table 20.41: Filters available in the Blocked Devices list

Details page

This page shows detailed information about the blocked device.

Field	Description	Values
Device	Name of the blocked device.	Character string
Action	Action taken by Advanced EPDR.	• Quarantined • Deleted • Blocked • Process ended
Computer	Name of the computer where the device was blocked.	Character string
Computer type	Type of computer.	• Workstation • Laptop

Field	Description	Values
		• Server • Mobile device
IP address	The computer primary IP address.	Character string
Original name	Name of the blocked device.	Character string
Name	Name assigned to the device by you. To edit it, click the icon.	Character string
Device type	Type of device.	• Removable storage drives • Imaging devices • CD/DVD drives • Bluetooth devices • Modems • Mobile devices
Instance ID	ID of the affected device.	Character string
Blocked by	Module that detected the item.	Device control
Number of detections	Number of detected blocks.	Numeric value
Date	Date when the attack was detected.	Date

Table 20.42: Details accessible from the Blocked Devices list

Intrusion attempts blocked

This list shows the network attacks received by the computers on the network and blocked by the firewall.

Field	Description	Values
Computer	Name of the computer that received the network	Character string

Field	Description	Values
	attack.	
IP address	IP address of the primary network interface of the computer that received the network attack.	Character string
Group	Group within the Advanced EPDR group tree that the computer belongs to.	Character string
Intrusion type	Indicates the type of intrusion detected. For more information about each type of network attack, see **Block intrusions** on page **351**.	• All intrusion attempts • ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood • TCP Flags Check • Smart WINS • IP Explicit Path Land Attack • Smart DNS • ICMP Filter Echo Request • OS Detection • Smart DHCP • SYN Flood • Smart ARP • TCP Port Scan
Date	Date and time Advanced EPDR logged the attack on the computer.	Date

Table 20.43: Fields in the Intrusion Attempts Blocked list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	Character string
Computer	Name of the computer that received the network attack.	Character string
Intrusion type	Indicates the type of intrusion detected. For more information about each type of network attack, see **Block intrusions** on page **351**.	• ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood • TCP Flags Check • Smart WINS • IP Explicit Path • Land Attack • Smart DNS • ICM Filter Echo Request • OS Detection • Smart DHCP • SYN Flood • Smart ARP • TCP Port Scan
Local IP address	IP address of the computer that received the network attack.	Character string
Remote IP address	IP address of the computer that launched the network attack.	Character string
Remote MAC address	Physical address of the computer that launched the network attack, provided it is on the same subnet as the computer that received the	Character string

Field	Description	Values
	attack.	
Local port	In TCP and UDP attacks, this section indicates the port where the intrusion attempt was received.	Numeric value
Remote port	In TCP and UDP attacks, this section indicates the port from which the intrusion attempt was launched.	Numeric value
Number of detections	Number of intrusion attempts of the same type received.	Numeric value
Action	Action taken by the firewall according to its settings. For more information, see **Firewall (Windows computers)** on page **344**.	Block
Detected by	Detection engine that detected the network attack.	Firewall
Date	Date the network attack was logged.	Date
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
IP address	IP address of the primary network interface of the computer that received the network attack.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by you.	Character string

Table 20.44: Fields in the Intrusion Attempts Blocked exported file

Filter tool

Field	Description	Values
Dates	• **Range**: Set a time period, from the current moment back. • **Custom range**: Choose specific dates from a calendar.	• Last 24 hours • Last 7 days • Last month
Intrusion type	Indicates the type of intrusion detected. For more information about each type of network attack, see **Block intrusions** on page **351**.	• All intrusion attempts • ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood • TCP Flags Check • Smart WINS • IP Explicit Path Land Attack • Smart DNS • ICMP Filter Echo Request • OS Detection • Smart DHCP • SYN Flood • Smart ARP • TCP Port Scan
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server

Table 20.45: Filters available in the Intrusion Attempts Blocked list

Details page

This page shows detailed information about the network attack detected.

Field	Description	Values
Intrusion type	Indicates the type of intrusion detected. For more information about each type of network attack, see **Block intrusions** on page **351**.	• ICMP Attack • UDP Port Scan • Header Lengths • UDP Flood • TCP Flags Check • Smart WINS • IP Explicit Path • Land Attack • Smart DNS • ICM Filter Echo Request • OS Detection • Smart DHCP • SYN Flood • Smart ARP • TCP Port Scan
Action	Action taken by Advanced EPDR.	Blocked
Computer	Name of the computer where the threat was detected.	Character string
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
IP address	The computer primary IP address.	Character string
Local IP address	IP address of the computer that received the network attack.	Character string

Field	Description	Values
Remote IP address	IP address of the computer that launched the network attack.	Character string
Remote MAC address	Physical address of the computer that launched the network attack, provided it is on the same subnet as the computer that received the attack.	Character string
Local port	In TCP and UDP attacks, this section indicates the port where the intrusion attempt was received.	Numeric value
Remote port	In TCP and UDP attacks, this section indicates the port from which the intrusion attempt was launched.	Numeric value
Detected by	Module that detected the item.	Firewall
Number of detections	Number of successive times the same type of attack occurred between the same source and target computers.	Numeric value
Date	Date when the attack was detected.	Date

Table 20.46: Details accessible from the Intrusion Attempts Blocked list

Web access by category

Field	Description	Values
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.
Allowed access attempts	Number of accesses allowed to pages belonging to the category specified in the Category field.	Numeric value
Allowed devices	Number of computers allowed to access pages belonging to the category specified in the Category field.	Numeric value
Denied	Number of access attempts denied to pages	Numeric value

Field	Description	Values
access attempts	belonging to the category specified in the Category field.	
Denied computers	Number of computers denied to access pages belonging to the category specified in the Category field.	Numeric value

Table 20.47: Fields in the Web Access by Category list

Fields displayed in the exported file

Field	Description	Values
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.
Allowed access attempts	Number of accesses allowed to pages belonging to the category specified in the Category field.	Numeric value
Allowed devices	Number of computers allowed to access pages belonging to the category specified in the Category field.	Numeric value
Denied access attempts	Number of access attempts denied to pages belonging to the category specified in the Category field.	Numeric value
Denied computers	Number of computers denied to access pages belonging to the category specified in the Category field.	Numeric value

Table 20.48: Fields in the Web Access by Category exported file

Filter tool

Field	Description	Values
Dates	• **Range**: Set a time period, from the current moment back.	• Last 24 hours • Last 7 days

Field	Description	Values
	• **Custom range**: Choose specific dates from a calendar.	• Last month • Last year
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.

Table 20.49: Filters available in the Web Access by Category list

Web access by computer

This list shows all computers on the network and web page visits allowed or denied (sorted by category).

Field	Description	Values
Computer	Computer name.	Character string
IP address	The computer primary IP address.	Character string
Group	Group within the Advanced EPDR group tree that the computer belongs to.	• Character string • 'All' group • Native group • Active Directory group
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.
Allowed access attempts	Number of accesses allowed to pages belonging to the category specified in the Category field.	Numeric value
Denied access attempts	Number of access attempts denied to pages belonging to the category specified in the Category field.	Numeric value

Table 20.50: Fields in the Web Access by Computer list

Fields displayed in the exported file

Field	Description	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Computer	Computer name.	Character string
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.
Allowed access attempts	Number of accesses allowed to pages belonging to the category specified in the Category field.	Numeric value
Denied access attempts	Number of access attempts denied to pages belonging to the category specified in the Category field.	Numeric value
Group	Group within the Advanced EPDR group tree that the computer belongs to.	Character string
IP address	The computer primary IP address.	Character string
Domain	Windows domain the computer belongs to.	Character string
Description	Description assigned to the computer by you.	Character string

Table 20.51: Fields in the Web Access by Category exported file

Filter tool

Field	Description	Values
Dates	• **Range**: Set a time period, from the current moment back.	• Last 24 hours • Last 7 days

Field	Description	Values
	• **Custom range**: Choose specific dates from a calendar.	• Last month
Category	Category that the accessed web page belongs to.	Enumeration of all supported categories.
Computer type	Type of device.	• Workstation • Laptop • Mobile device • Server
Computer	Computer name.	Character string

Table 20.52: Filters available in the Web Access by Category list

Network attack activity

This list shows all network attacks detected and blocked by the Network Attack Protection module.

Field	Description	Values
Computer	Computer name.	Character string
Network attack	Name of the network attack. For more information, see **https://www.pandasecurity.com/en/support/card?id=700145**	Character string.
Local IP address	The computer local IP address.	IP address
Action	Action taken.	• Detected • Blocked
Remote IP address	IP address from which the attack originated.	IP address

Field	Description	Values
Date	Date the attack was detected or blocked.	Date

Table 20.53: Fields in the Network Attack Activity list

Fields displayed in the exported file

Field	Description	Values
Computer	Computer name.	Character string
Network attack	Type of network attack.	Character string
Action	Action taken on the attack.	• Detected • Block
Local IP address	The computer local IP address.	IP address
Remote IP address	Remote IP address of the attack.	IP address
Local port	Local port on which the attack was detected or blocked.	Character string
Remote port	Remote port from which the attack was detected or blocked.	Character string
Date	Date the attack was detected.	Date
Number of occurrences	Number of detections of the same type of attack with the same source IP address in the space of an hour.	Character string

Table 20.54: Fields in the Network Attack Activity exported file

Filter tool

Field	Description	Values
Computer	Computer name.	Character string
Network attack	Type of network attack.	Character string
Dates	Date range.	• Last 24 hours • Last 7 days • Last month
Action	Action taken on the threat.	• Detected • Blocked

Table 20.55: Filters available in the Network Attack Activity list

Details page

Field	Description	Values
Network attack	Type of network attack. For more details, click the icon.	Character string
Action	Action taken on the detection. For more information about how to manage detected threats blocked, see **Stopping detecting a network attack** on page **788**.	• Detected • Blocked
Computer	Name of the computer where the threat was detected, IP address, and folder it belongs to in the group tree.	• **Name**: Name of the computer. • **IP address**: IP address of the computer where the attack was detected. • **Group:** Folder within the Advanced EPDR group tree that the computer belongs to.

Field	Description	Values
Local IP address	The computer local IP address.	IP address
Remote IP address	Remote IP address of the network attack.	IP address
Local port	Local port on which the attack was detected or blocked.	Character string
Remote port	Remote port from which the attack was detected or blocked.	Character string
Detection date	Date the network attack was detected.	Date
Number of occurrences	Number of detections of the same type of attack with the same source IP address in the space of an hour.	Character string

Table 20.56: Fields on the Network Attack Detection page

Chapter 21

Risk assessment

The risk assessment feature enables you to monitor the overall status of the security risk for the computers you manage.

Advanced EPDR Individually monitors and assesses each configuration and each security module installed on the computers on the network. Each assessed feature is compared to an ideal configuration or status defined by Cytomic. When the ideal configuration and the configuration found on a user computer differ, a risk level is assigned to that specific feature.

When you configure the risk assessment feature, you can choose which security aspects you want to monitor on computers. If the assessed feature and the ideal configuration differ, Cytomic sets a specific risk level (Medium, High, or Critical). You can change this level afterward according to your needs.

Not all features you can assess are applicable to all operating systems installed across the network. Cytomic will add new checks with each new version of the product to gradually improve risk assessment.

For more information about the risk assessment feature, see: **Accessing, controlling, and monitoring the management console** on page **61**: Information about how to manage user accounts and assign permissions. **Managing lists** on page **48**: Information about how to manage lists.

Chapter contents

Chapter contents

Risk assessment settings

Required permissions

The risk assessment feature is visible to all users of the web console. However, you must have the Full Control role to configure it. For more information, see **Managing roles and permissions** on page **69**.

The risk assessment settings apply equally to all computers on the IT network.

Accessing the settings

From the top menu, select **Settings**. From the side menu, select **Risks**. The **Risks** page opens. This page is divided into two main areas: a list of risks and a series of drop-down menus to assign risk levels.

Risk list

Most risks have to do with the various types of settings implemented in Advanced EPDR. Other risks are related to the security software status information sent by computers to the Cytomic servers.

The risks you can assess vary based on the operating system installed on the computer.

Risk	Description
No protection	The computer has protection installation errors or does not have a license. See **Protection status** on page **662**.
Out-of-date protection	The version of the protection engine installed on the computer is out of date. The computer is vulnerable to threats. See **Details section (3)** on page **266**.
Out-of-date knowledge (more than 30 days)	The version of the signature file installed on the computer is out of date. The computer is vulnerable to threats. See **Outdated protection** on page **666**.
No connectivity to knowledge servers	Communications between the computer and the Cytomic servers have failed. The computer is not completely protected. To verify the computer meets the connection requirements, see **Product features and requirements** on page **932**.
No uninstallation protection	The computer is not password protected to prevent unauthorized protection uninstallation or tampering. See **Configuring security against**

Risk	Description
	protection tampering on page **321**.
Anti-tamper protection disabled	The protection can be modified and tampered with. See **Configuring security against protection tampering** on page **321**.
File antivirus disabled	The antivirus is disabled. See **Antivirus** on page **342** and **Antivirus for web browsers** on page **366** (Android).
Advanced protection for Windows disabled or in Audit mode	Advanced protection is not active or reports threats but does not block or disinfect malware. See **Advanced protection** on page **333**.
Advanced protection for Windows in Hardening mode	The advanced protection settings allow execution of unknown programs already installed on user computers but block programs that originate from an external source. See **Advanced protection** on page **333**.
Advanced protection for Linux disabled or in Do not detect or Audit mode	Advanced protection is not active or reports threats but does not block them. See **Detect malicious activity (Linux computers only)** on page **335**.
Anti-exploit protection disabled or in Audit mode	Anti-exploit protection is not active or reports detections but does not take action against them. See **Anti-exploit protection settings** on page **339**.
Anti-phishing disabled	The computer is not protected against fraudulent emails and websites. See **Threats to detect** on page **343**.
Web browsing antivirus disabled	The computer is not protected against threats hosted on certain web pages and URLs. See **Antivirus** on page **342** and **Antivirus for web browsers** on page **366**.
Folder, file, and	There are files, folders, or extensions that are not scanned for malware.

Risk	Description
extension exclusions	• For more information about how to configure items you do not want to be blocked, deleted, or disinfected, see **Files and paths excluded from scans** on page **331** • For more information about how to prevent certain programs from being blocked, see **Authorized software and exclusions** on page **582**. • For more information about how to add folder-level, file, or file extension exclusions without impacting a computer risk level, see **Managing exclusion impact**.
Recent indicators of attack	The computer reported the detection of indicators of attack (IOAs) in the last 30 days. Only IOA detections in Pending status are considered. See **Managing indicators of attack detections** on page **614**.
Critical patches pending installation	The computer has Cytomic Patch installed and has reported the existence of critical patches that are pending installation. You can receive notification of this risk immediately or a specified number of days after the patches are published. By default, the number of days is 30, although you can edit this parameter when you enable this risk for evaluation. See **Configuring the discovery of missing patches** on page **456**.
Audit mode enabled	The security software detects and reports threats, but it does not block or delete them. When you enable Audit mode in a settings profile, the overall status of the protection applied to the computers that receive the settings does not change. Audit mode does not change the configuration in the web console. See **Audit mode** on page **359**.
Network attack protection disabled or in "Audit" mode	Real-time scanning of network traffic does not detect or stop lateral movements by fileless threats and advanced attacks that use exploits. See **Network attack protection** on page **341**.

Table 21.1: Risk list

How risk assessment works

Cytomic sets a default risk level for each risk. This is the risk level when you first open the **Settings** > **Risks** page. You can change the default risk level to another risk level, based on your needs.

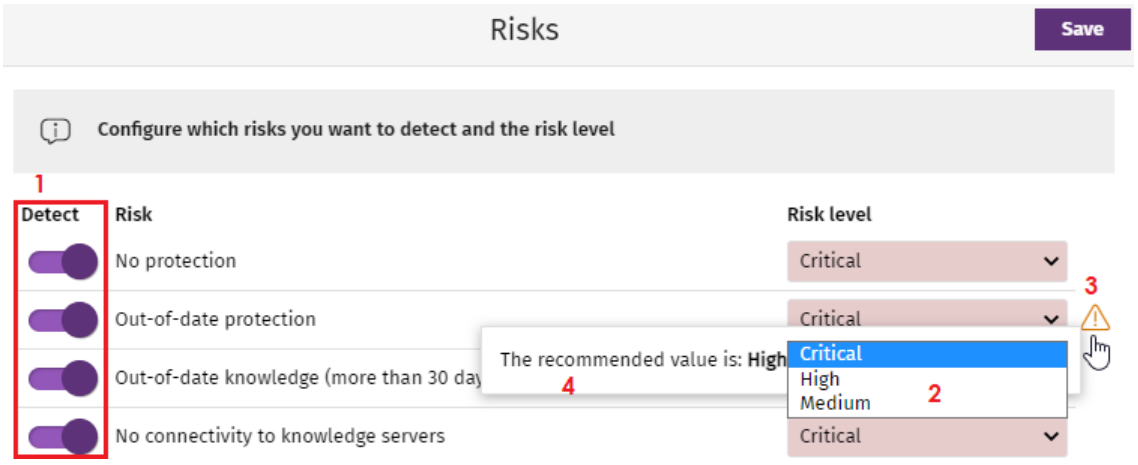


Figure 21.1: Configuring risk assessment

To configure risk assessment:

- From the list of risks **(1)**, enable the toggles for the risks you want to detect.
- From the **Risk level** drop-down menu **(2)**, select a level for each risk: **Critical**, **High**, **Medium**.

  If the recommended risk level is different from the level you select, the  icon **(3)** appears.

  Point to the icon. A message appears **(4)** that shows the risk level recommended by Cytomic.
- Click **Save**.

> *Risk update is asynchronous. There could be a delay between when you configure risks and when data shows in lists and widgets.*

Setting a risk level for recent IOAs

When you enable the **Recent indicators of attack** risk, the risk is detected when the security software detects an indicator of attack (IOA) on a computer.

To set the risk level:

- From the **Risk level** drop-down menu **(2)**, select a risk level (**Critical**, **High**, or **Medium**).
- From the **Risk level** drop-down menu **(2)**, select the **Risk of indicators of attack** option. If you select this option as the risk level, then the overall risk level becomes equal to the highest risk level for any IOA detected on the computer.

The security software only detects IOAs that have not been previously archived or were detected less than 30 days ago.

Example:

25 IOAs detected — 12 Low Risk, 12 Medium Risk, 1 High Risk. The overall risk level for **Recent indicators of attack** is **High**.

If you archive the high risk IOA or if there are unarchived IOAs after 30 days, the risk level is calculated again. The risk level is **Medium**.

Example:

25 IOAs detected — 2 Medium Risk, 23 Low Risk. The overall risk level for **Recent indicators of attack** is **Medium**.

If you archive one of the medium risk IOAs, the risk level stays the same because there is another medium risk IOA. When you archive the remaining medium risk IOAs, the risk level changes to **Low** because the remaining, unarchived IOAs have a low risk level.

Monitoring risk assessment

Risk assessment results appear in the relevant widgets and lists. For more information, see **Risk assessment module lists** and **Risk assessment module panels/widgets**.

Modification and recalculation of recommended values

When Cytomic releases a new version of Advanced EPDR, we might change the default risk level for risks. When you upgrade to a new version of Advanced EPDR:

- Risks that you did not modify the default risk level for automatically update to the new default value recommended by Cytomic.
- Advanced EPDR recalculates the overall risk level for all computers. The default configuration shows the new recommended risk levels.

Calculation of the overall risk level for a specific computer

The security software calculates the overall risk level for a specific computer when:

- You upgrade to a new version of Advanced EPDR.
- The computer settings change, the computer or device moves from one group to another, a new computer or device registers, or the license assigned to the computer changes, in some cases.

  The overall risk level assigned to a computer matches the highest risk level of the risks detected on it.

  For example:

  - A computer has five risks. All of the them are active, one of which has a **High** risk level and the other four have a **Medium** risk level. The computer overall risk level is **High**.
  - A computer has five risks. Four risks are active (One has a **High** risk level and three have a **Medium** risk level) and one is inactive (with a **Critical** risk level). The computer overall risk level is **High**.

Managing exclusion impact

The security software assigns a specific risk level to each risk detected on computers. On the **Manage exclusion impact** page, you can control whether folder-level, file, or file extension exclusions impact the overall security risk status for a computer.

Configure risk settings for exclusions

- From the top menu, select **Settings**. From the side menu, select **Risks**. The **Risks** page opens.
- From the list of risks **(1)**, enable the **Folder, file, and extension exclusions** toggle.
- Click **Manage exclusion impact**.

The **Manage exclusion impact** dialog box opens. This dialog box is divided into two areas:

- The left side shows all of the folder-level, file, or file extension exclusions added to all of the Workstations and Servers settings profiles created in the management console. These exclusions impact the security risk and are taken into account to calculate the risk level for your computers. See **How risk assessment works** and **Calculation of the overall risk level for a specific computer**.
- The right side shows the exclusions you have selected to not impact security risk status. These exclusions are not taken into account to calculate the overall risk level for your computers.

Click  to move the exclusions you do NOT want to impact security risk status to the right side of the dialog box. Click  to move exclusions back to the left side of the dialog box.

- Use the Control key to select multiple items at the same time. To select all items, click **Select all**.
- Click **Save**.

Viewing exclusions

The number of exclusions you have selected to not impact the risk level for your computers appears on the **Status** > **Risks** page. See **Risk assessment module panels/widgets**.

Risk assessment module lists

Accessing the lists

You can access the risk assessment lists in two ways:

- Select the **Status** menu at the top of the console.
- Select **Risks** from the side menu. Click the relevant widget.

  Or

- Select the **Status** menu at the top of the console.

- From the side panel, in the **My lists** section, click **Add**. The **Add list** window opens. This window shows all available lists.
- In the **General** section, select the risk list you want to use: **Risks by computer** or **Risks**. The list template opens. Edit and save it. The list is added to the **My lists** section in the side menu.

Risks by computer list

This list shows information about the risks detected on each computer or device as well as their risk level.

Field	Comment	Values
Computer	Computer name.	Character string
Group	Group to which the computer belongs.	Character string
Last connection	Date/time when the computer status was last sent to the Cytomic cloud.	Date/time
Risk level	Risk level for the computer or device. It is equal to the highest risk level for any risk detected on the computer.	• **No risk**: No risk was detected that had a critical, high, or medium risk level. • **Critical**: One or more risk detected have a critical risk level. • **High**: The highest risk level for any risk detected on the computer was high. • **Medium**: The highest risk level for any risk detected on the computer was medium.
Computer risks	Graph showing the risks detected on the computer or device during risk assessment.	• **Red**: Number of critical risks. • **Orange**: Number of high risks. • **Yellow**: Number of medium risks. • **Green**: Number of risks with no impact on security. • **Light gray**: Number of risks not

Field	Comment	Values
		compatible with the operating system installed on the computer or device. • **Dark gray**: Number of risks that were not evaluated because you did not enable them.

Table 21.2: Fields in the Risks by computer list

Click a row in the list to open the computer details page. See **Computer details** on page **252** and **Details section (3)** on page **266**.

Fields displayed in the exported file

You can export the information in the list to a CSV file. Click the  icon. The exported file contains the following data:

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server • Mobile device
Computer	Computer name.	Character string
Group	Folder in the Advanced EPDR group tree that the computer belongs to.	Character string
Last connection	Date when the computer status was last sent to the Cytomic cloud.	Date
Platform	Operating system installed on the computer.	• Windows • Linux • macOS • Android

Field	Comment	Values
		• iOS
Risk level	Overall risk level for the computer or device.	• No risk • Medium • High • Critical
Critical risks	Number of critical risks detected on the computer.	Numeric value
High risks	Number of high risks detected on the computer.	Numeric value
Medium risks	Number of medium risks detected on the computer.	Numeric value
No risk	Number of risks that have no impact on security.	Numeric value
Not applicable risks	Number of risks that do not apply to the computer based on the operating systems installed.	Numeric value
Not evaluated risks	Number of risks that you did not enable for evaluation.	Numeric value

Table 21.3: Fields in the Risks by computer exported file

Filter tool

To open the filter tool, click the **Filters** link next to the search box on the **Risks by computer** page. The filtering options are these:

Field	Comment	Values
Search computer	Filters computers by name.	Character string
Computer type	Filters computers according to type.	• Workstation • Laptop • Mobile device • Server

Field	Comment	Values
Last connection	Date when the computer risks were last sent to the Cytomic cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS • Android • iOS
Detected risk	The risk you enabled for evaluation.	• All • No protection • Out-of-date protection • Out-of-date knowledge (more than 30 days) • No connectivity to knowledge servers • No uninstallation protection • Anti-tamper protection disabled • File antivirus disabled • Advanced protection for Windows disabled or in Audit mode • Advanced protection for Windows in Hardening mode • Advanced protection for Linux disabled or in Do not detect or

Field	Comment	Values
		Audit mode • Anti-exploit protection disabled or in Audit mode • Anti-phishing protection disabled • Web browsing antivirus disabled • Folder, file, and extension exclusions • Recent indicators of attack • Critical patches pending installation • Audit mode enabled • Network attack protection disabled or in "Audit" mode
Risk level	Risk level assigned.	• Critical • High • Medium • No risk

Table 21.4: Filters available in the Risks by computer list

Risks list

The **Risks** list shows the risks you enabled for evaluation and the number of affected computers based on the risk level assigned to each risk. Click a row in the list to open the **Risks by computer** list.

The **Risks** list shows the following data:

Field	Comment	Values
Risk	Risk name.	Character string
Computers	Number of computers where the risk was detected.	Numeric value
Risk level	Risk level assigned.	• Critical • High

Field	Comment	Values
		• Medium • Risk of indicators of attack (see **Risk assessment settings**).
Risk by computers	Distribution graph that shows the number of computers where the risk was detected and the risk level assigned (Critical, High, Medium), and computers where there is no risk (the risk was selected for detection but was not detected).	• **Red**: Number of computers where the risk was detected and the risk level assigned is Critical. • **Orange**: Number of computers where the risk was detected and the risk level assigned is High. • **Yellow**: Number of computers where the risk was detected and the risk level assigned is Medium. • **Light gray**: Number of computers where the risk was not evaluated because it is not compatible with the operating system installed. • **Dark gray**: Number of computers where the risk was not evaluated because you did not enable it for detection.

Table 21.5: Fields in the Risks list

Fields in the exported file

You can export the information in the list to a CSV file. Click the  icon. The exported file contains the following data:

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Risk	Name of the risk you enabled for evaluation.	Character string
Risk level	Risk level assigned.	• Critical • High • Medium
Computers where the risk was detected	Number of computers where the risk was detected.	Numeric value
Critical	Number of computers in the account that have a Critical risk level.	Numeric value
High	Number of computers in the account that have a High risk level.	Numeric value
Medium	Number of computers in the account that have a Medium risk level.	Numeric value
Computers with no risk	Number of computers where the risk was not detected.	Numeric value
Computers the risk does not apply to	Number of computers where the risk was not evaluated because it is not compatible with the operating system installed.	Numeric value
Computers where the risk was not evaluated	Number of computers for which the risk was not enabled for detection.	Numeric value

Table 21.6: Fields in the Risks exported file

Filter tool

To open the filter tool, click the **Filters** link next to the search box on the **Risks** page. The filtering options are these:

Field	Comment	Values
Computer type	Filters computers according to type.	• Workstation • Laptop • Server • Mobile device
Platform	Operating system installed on the computer.	• Windows • Linux • macOS • Android • iOS

Table 21.7: Filters available in the Risks list

To schedule risk lists to be sent periodically, see ***Scheduled sending of reports and lists*** *on page* ***865****.*

Risk assessment module panels/widgets

Accessing the dashboard

From the top menu, select **Status**. From the side menu, select **Risks**.

Company risk

This widget shows the number and percentage of computers on the network with an assigned risk level. The status of computers is indicated by a circle with various colors and associated counters.

At the bottom of the widget, a message appears that shows the number of exclusions that are not considered a risk, if any, based on the exclusion impact settings. When you click the message, the **Manage exclusion impact** dialog box opens. See **Managing exclusion impact**

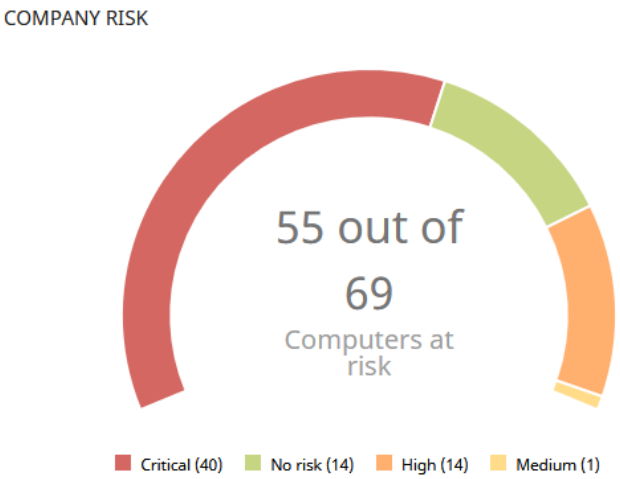


Figure 21.2: Company Risk panel

Meaning of the data displayed

Data	Description
Critical	Number of computers with a critical risk level.
High	Number of computers with a high risk level.
Medium	Number of computers with a medium risk level.
No risk	Number of computers that are not at risk.
Central area	Sum of all computers with an assigned risk level.

Table 21.8: Description of the data displayed in the Company Risk panel

Lists accessible from the panel

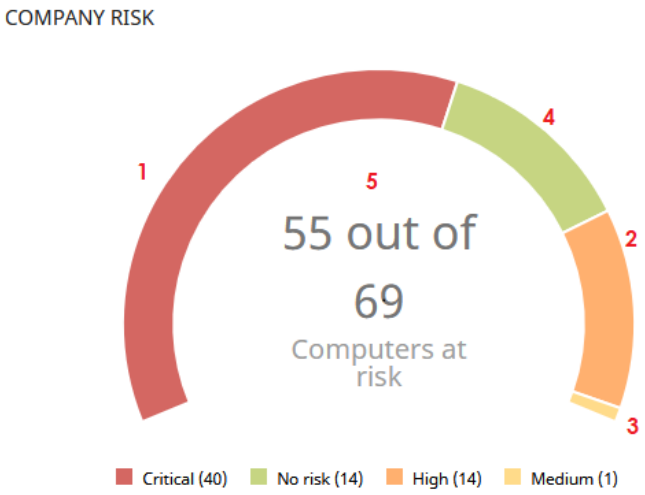


Figure 21.3: Hotspots in the Company Risk panel

Click the hotspots shown in **Hotspots in the Company Risk panel** to open the **Risks by computer** list with these predefined filters:

Hotspot	Filter
(1)	Risk = High
(2)	Risk = Critical
(3)	Risk = No risk
(4)	Risk = Medium
(5)	No filters

Table 21.9: Filters accessible from the Company Risk panel

Risks trend

This widget shows the number and types of risks that are detected over time.

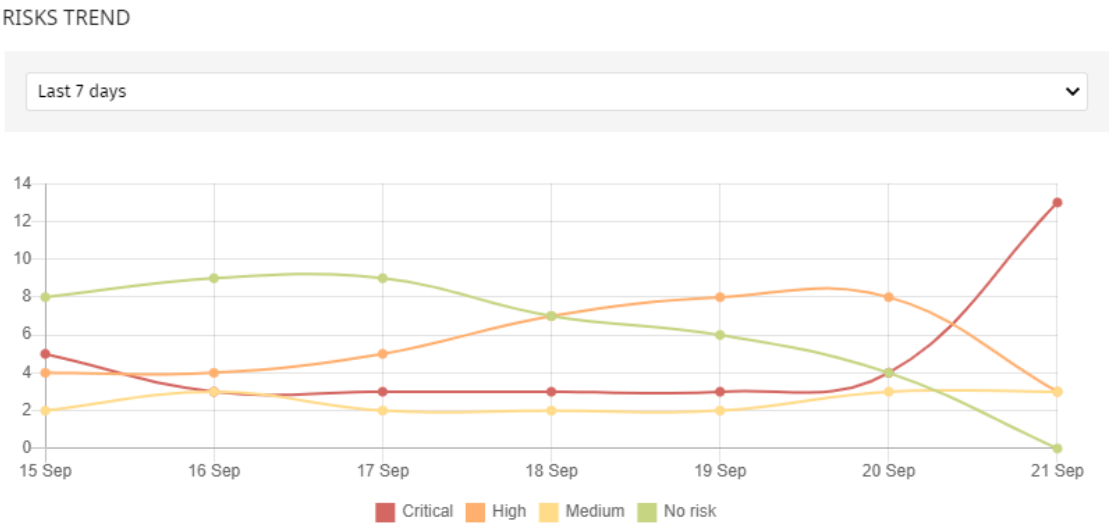


Figure 21.4: Risks Trend graph

Meaning of the data displayed

Data	Description
Critical risk	Trend of the number of computers with a critical risk level.
High risk	Trend of the number of computers with a high risk level.
Medium risk	Trend of the number of computers with a medium risk level.
No risk	Trend of the number of computers that have no risks.

Table 21.10: Description of the data displayed in the Risks Trend panel

Point the mouse to a node on the graph to show a label with this information:

- Date
- Risk level
- Number of affected computers

Lists accessible from the panel

Click the legend items under the graph to open the **Risks by computer** list filtered to show the selected item. To open the **Risks by computer** full list with no filters applied, click an empty space on the graph.

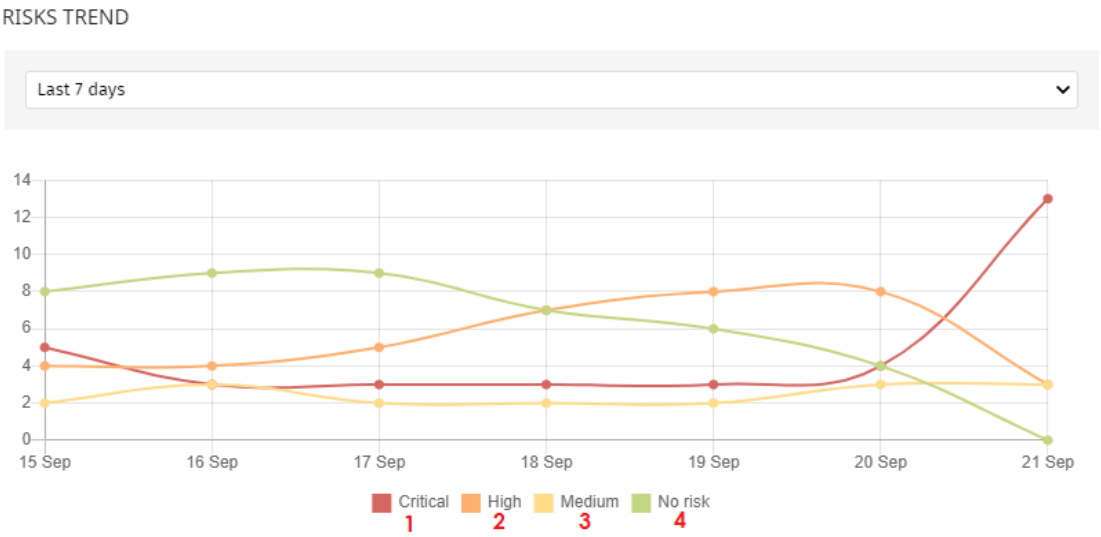


Figure 21.5: Hotspots in the Risks Trend graph

Hotspot	Filter
(1)	Risk = Critical
(2)	Risk = High
(3)	Risk = Medium
(4)	No risks

Table 21.11: Filters accessible from the Risks Trend panel

Detected risks

This widget shows the most commonly found risks on computers.

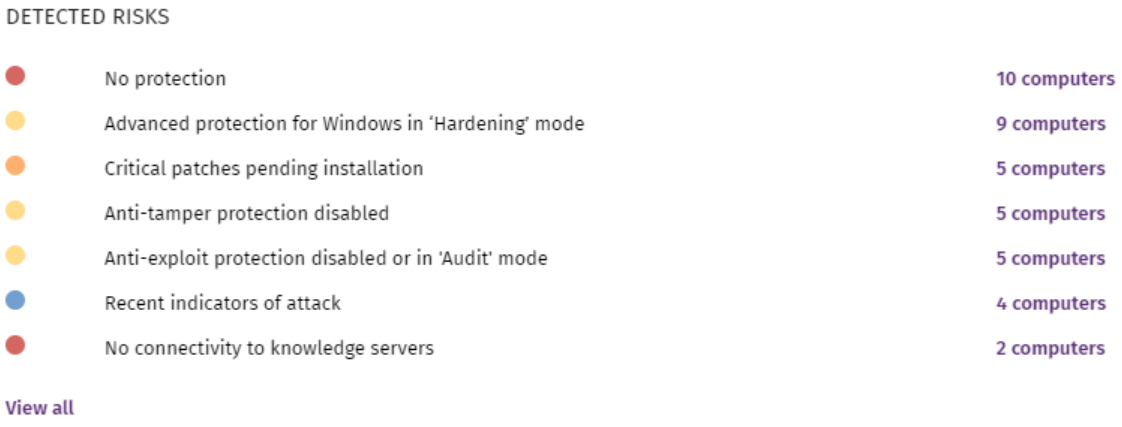


Figure 21.6: Detected Risks panel

Meaning of the data displayed

Data	Description
Icon	Risk level defined by you. • **Red**: Critical • **Orange**: High • **Yellow**: Medium • **Blue**: Custom
Name	Risk name.
Number	Number of computers where the risk was detected.
View all	Link to the full list of all of the risks detected.

Table 21.12: Description of the data displayed in the Detected Risks panel

Lists accessible from the panel

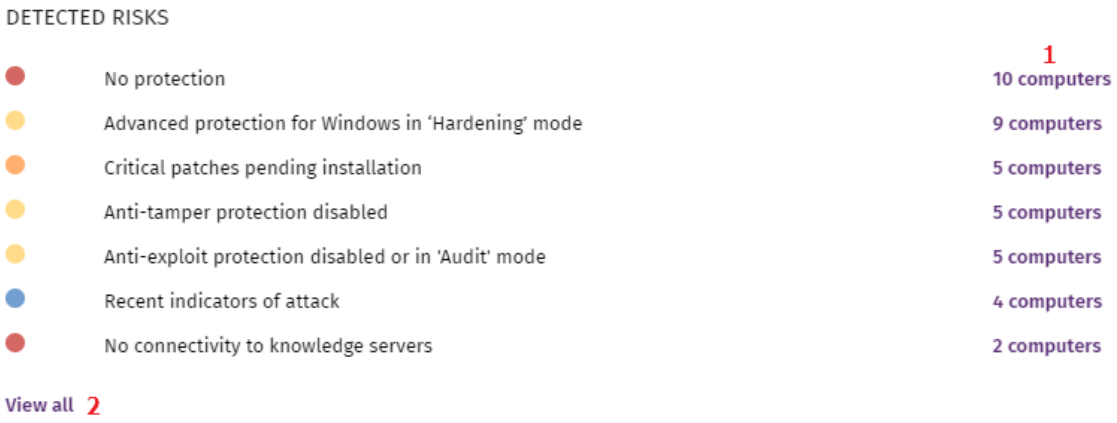


Figure 21.7: Hotspots in the Detected Risks panel

Click the hotspots shown in the figure to open these lists with these predefined filters:

Hotspot	List	Filter
(3)	Risks by computer	Detected risk = Risk selected on the widget
(4)	Risks	No filters

Table 21.13: Lists and filters accessible from the Detected Risks panel

Top 10 computers at risk

This widget shows the ten computers with the highest overall risk level.

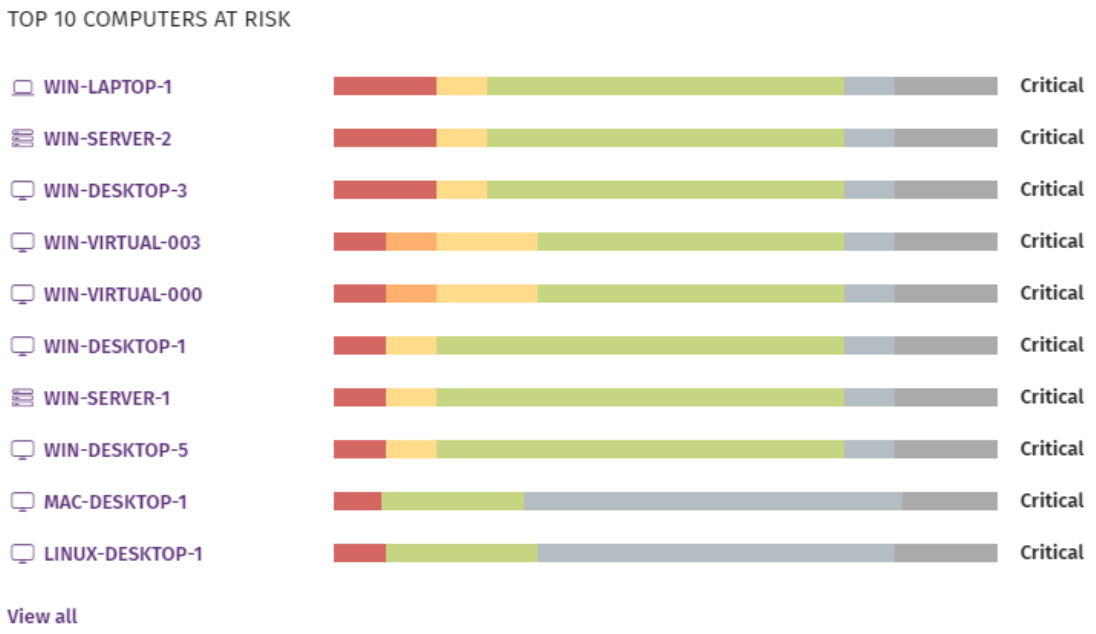


Figure 21.8: Top 10 Computers at Risk panel

A computer overall risk level is the highest risk level of the risk factors detected on the computer. For more information, see ***Calculation of the overall risk level for a specific computer****.*

Meaning of the data displayed

Data	Description
Name	Computer or device name and type.
Color bar	Type of risks found and the total number of risks.
Risk level	Overall risk level assigned to the computer.
View all link	Access to the Risks by Computer full list.

Table 21.14: Description of the data displayed in the Top 10 Computers at Risk panel

Lists accessible from the panel

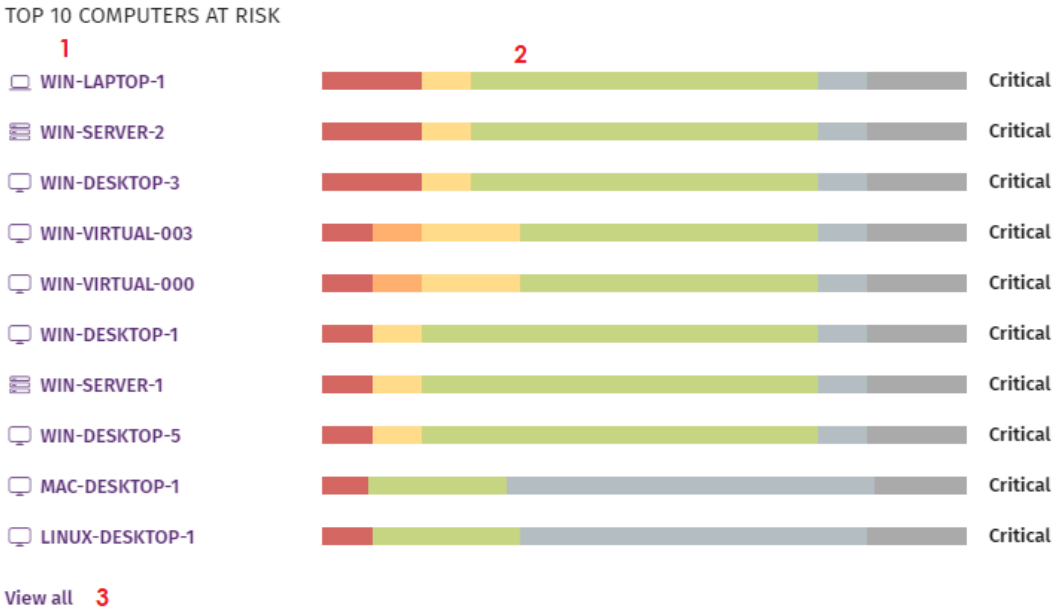


Figure 21.9: Hotspots in the Top 10 Computers at Risk panel

Click the hotspots shown in the figure to open these lists with these predefined filters:

Hotspot	List	Filter
(1)	Computer details	
(2)	Risks	Computer selected on the widget.
(3)	Risks by computer	No filters

Table 21.15: Lists and filters accessible from the Top 10 Computers at Risk panel

You can also review information on the status of the risks detected on a computer on the **Computer details** page. For more information, see **Computer details** on page **252**.

Chapter 22

Vulnerability assessment

The vulnerability assessment module built on Cytomic platform finds computers on the network with known software vulnerabilities and reports on the availability of patches to mitigate vulnerability impact on computers.

Vulnerability assessment supports Windows, macOS, and Linux operating systems. It identifies third-party applications that have missing patches or have reached end of life (EOL), as well as the patches and updates released by Microsoft for all of its products (operating systems, databases, Office applications, etc.).

Vulnerability assessment does not install the identified patches on managed computers. You can install the required patches on your own or purchase the Cytomic Patch module to install the patches centrally from the Advanced EPDR console.

For more information about the vulnerability assessment module, see:

***Creating and managing settings profiles** on page **294**: Information about how to create, edit, delete, or assign settings profiles to the computers on your network.*

***Accessing, controlling, and monitoring the management console** on page **61**: Managing user accounts and assigning permissions.*

***Managing lists** on page **48**: Information about how to manage lists.*

Chapter contents

Vulnerability assessment requirements

From 30 September 2024, you will not be able to add devices to the management console or install the protection software on new computers that run these operating system versions: Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008 (Windows 2008 R2 will continue to be supported). Existing computers in the management console will continue to be protected. See ***https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.***

Supported Windows operating systems

Workstations

- Windows 7 (32 and 64-bit)
- Windows 8 (32 and 64-bit)
- Windows 8.1 (32 and 64-bit)
- Windows 10 (32 and 64-bit)
- Windows 11 (64-bit)

Servers

- Windows 2008 (32 and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2, and 2016
- Windows Server 2022

Unsupported Windows computers

- The module does not install.
- Computers keep the vulnerability assessment settings profiles assigned to them, but they are not applied.
- The **Available patches by computers** list does not show information about these computers.

Supported macOS operating systems

- macOS Catalina 10.15
- macOS Big Sur 11

- macOS Monterey 12
- macOS Ventura
- macOS Sonoma

Supported Linux operating systems

Supported 64-bit distributions:

- **Red Hat**: 7.0, 8.0
- **CentOS**: 7.0
- **SUSE Linux Enterprise**: 12, 15

Vulnerability assessment settings

Accessing the settings

- Select **Settings** from the top menu. Select **Vulnerability assessment** from the side menu.
- Click the **Add** button. The settings page opens.

Required permissions

Permission	Access type
Configure vulnerability assessment	Create, edit, delete, copy, or assign vulnerability assessment settings profiles.
View available patches	View vulnerability assessment settings profiles.

Table 22.1: Permissions required to access the vulnerability assessment settings

General options

To enable the solution to automatically search for available patches, enable **Automatically search for patches**. If this option is not enabled, the solution lists do not show missing patches, although you can use patch installation tasks to install missing patches on computers.

Network administrators can choose between installing patches manually or using a third-party tool. However, by purchasing the Cytomic Patch module, you can install patches centrally and automatically from the Advanced EPDR console.

Search frequency

Search for patches with the following frequency specifies how often vulnerability assessment searches the cloud-based patch databases to check for missing patches for your computers.

Patch criticality

Specifies the importance (or criticality) of the security patches that vulnerability assessment searches for.

Windows Service Packs are not applied to macOS or Linux computers or devices.

Software vendors define the importance of the security patches they make available to address vulnerabilities. Patch classifications are not universal and vary by vendor. To determine whether you want to install a patch, we recommend that you review its description, especially for patches that a vendor does not classify as Critical.

*Patches containing bug fixes and feature enhancements for macOS and Linux are included in the **Other patches (non-security related)** category.*

Vulnerability assessment module panels/widgets

Discover Cytomic Patch

Cytomic Patch is a built-in module on Cytomic platform that finds computers on the network with known software vulnerabilities and updates them centrally and automatically.

For more information about Cytomic Patch, click the **Watch video** or **More information** links.

To close the informational message or not see it again, click the  icon.

Accessing the dashboard

To access the dashboard, select **Status** from the top menu. Select **Vulnerability assessment** from the side menu.

Required permissions

Permissions	Access to widgets
No permissions	• Vulnerability assessment status • Time since last check
View available patches	• End-of-Life programs

Permissions	Access to widgets
	• Available patches • Available patches trend • Most available patches for computers • Programs with most available patches

Table 22.2: Permissions required to access the vulnerability assessment widgets

Vulnerability assessment status

Shows computers where vulnerability assessment is working correctly and computers where there have been errors or problems installing or running the module. The status of the module is represented with a circle with different colors and associated counters. The panel shows the number and percentage of computers with the same status.

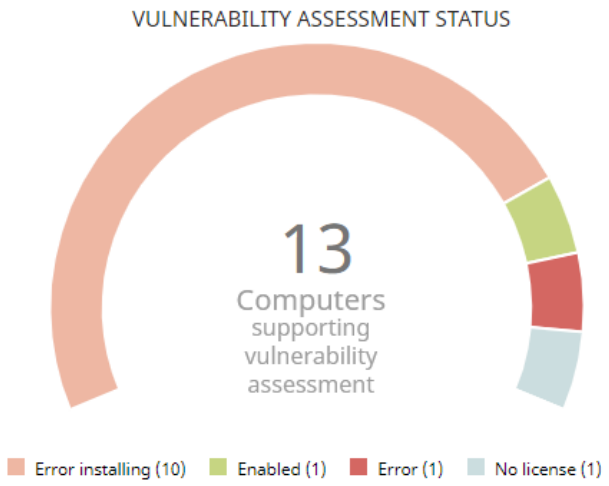


Figure 22.1: Vulnerability assessment status panel

Meaning of the data displayed

Data	Description
Enabled	Shows the percentage of computers where the vulnerability assessment module installed successfully, runs with no issues, and the assigned settings enable the module to search for patches automatically.
Disabled	Shows the percentage of computers where the vulnerability assessment module installed successfully, runs with no issues, but the assigned settings do not enable the module to search for patches automatically.
No license	Computers where the vulnerability assessment service does not work

Data	Description
	because no Advanced EPDR license is assigned to the computer or there are insufficient licenses.
Error installing	Computers where the module could not install.
No information	The computer has a license, but has not yet reported status to the server, or has an outdated agent installed.
Error	The vulnerability assessment module does not respond to requests sent from the server, or has settings that are different from those configured in the web console.
Central area	Shows the total number of computers compatible with the vulnerability assessment module.

Table 22.3: Description of the data displayed in the Vulnerability assessment status panel

Lists accessible from the panel

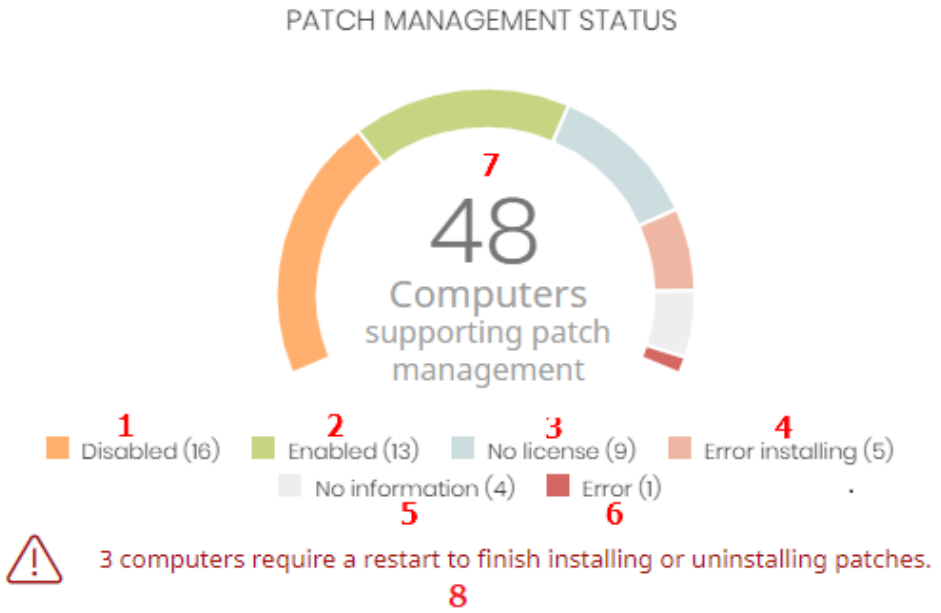


Figure 22.2: Hotspots in the Vulnerability assessment status panel

Click the hotspots shown in **Hotspots in the Vulnerability assessment status panel** to open the **Vulnerability assessment status** list with the following predefined filters:

Hotspot	Filter
(1)	Vulnerability assessment status = Disabled.
(2)	Vulnerability assessment status = Enabled.
(3)	Vulnerability assessment status = No license.
(4)	Vulnerability assessment status = Error installing.
(5)	Vulnerability assessment status = No information.
(6)	Vulnerability assessment status = Error.
(7)	No filters.

Table 22.4: Filters available for the Vulnerability assessment status list

Time since last check

Shows the number of computers that have not connected to the Cytomic cloud and reported patch status for more than 3, 7, and 30 days. Use this panel to identify computers that might be at risk and require your attention.

Figure 22.3: Time since last check panel

Meaning of the data displayed

Data	Description
72 hours	Number of computers that have not reported patch status in the last 72 hours.
7 days	Number of computers that have not reported patch status in the last 7 days.

Data	Description
30 days	Number of computers that have not reported patch status in the last 30 days.

Table 22.5: Description of the data displayed in the Time since last check panel

Lists accessible from the panel

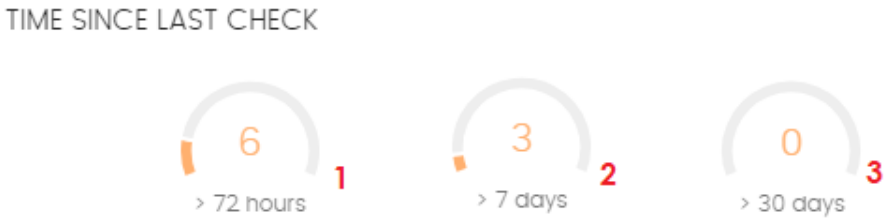


Figure 22.4: Hotspots in the Time since last check panel

Click the hotspots shown in **Figure 22.4:** to open the **Vulnerability assessment status** list with the following predefined filters:

Hotspot	Filter
(1)	Last connection = More than 3 days ago and Vulnerability assessment status = Enabled or Disabled or No information or Error.
(2)	Last connection = More than 7 days ago and Vulnerability assessment status = Enabled or Disabled or No information or Error.
(3)	Last connection = More than 30 days ago and Vulnerability assessment status = Enabled or Disabled or No information or Error.

Table 22.6: Filters available for the Vulnerability assessment status list

End-of-Life programs

Shows information about programs that have reached or are close to end of life, grouped by end-of-life date.

Figure 22.5: End-of-Life programs panel

Meaning of the data displayed

Data	Description
Currently in EOL	Programs that have reached end of life.
In EOL (currently or in 1 year)	Programs that have reached end of life or will in the next year.
With known EOL date	Programs that have a known end-of-life date more than one year in the future.

Table 22.7: Description of the data displayed in the End-of-Life programs panel

Lists accessible from the panel

Figure 22.6: Hotspots in the End-of-Life programs panel

Click the hotspots shown in Figure 22.6: to open the **End-of-Life programs** list with the following predefined filters:

Hotspot	Filter
(1)	End-of-Life date = Currently in EOL.
(2)	End-of-Life date = In EOL (currently or in 1 year).

Hotspot	Filter
(3)	End-of-Life date = All.

Table 22.8: Filters available for the End-of-Life programs list

Available patches

Shows the number of patches of different types that are available for computers on the network. Numbers in this panel count the same patch multiple times if multiple computers do not have the patch installed.

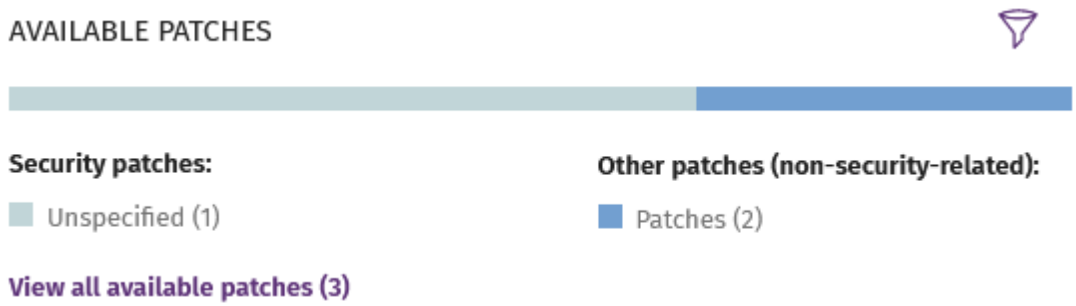


Figure 22.7: Available patches panel

Meaning of the data displayed

Data	Description
Security patches - Critical	Number of security patches classified as Critical that are missing from computers.
Security patches - Important	Number of security patches classified as Important that are missing from computers..
Security patches - Low	Number of security patches classified as Low that are missing from computers.
Security patches – Unspecified	Number of security patches that do not have a severity classification and are missing from computers.
Other patches (non-security related)	Number of patches not related to security that are missing from computers.

Data	Description
Service Packs	Number of patch and hotfix bundles that are missing from computers. Not applicable for Linux or macOS computers.

Table 22.9: Description of the data displayed in the Available patches panel

Lists accessible from the panel

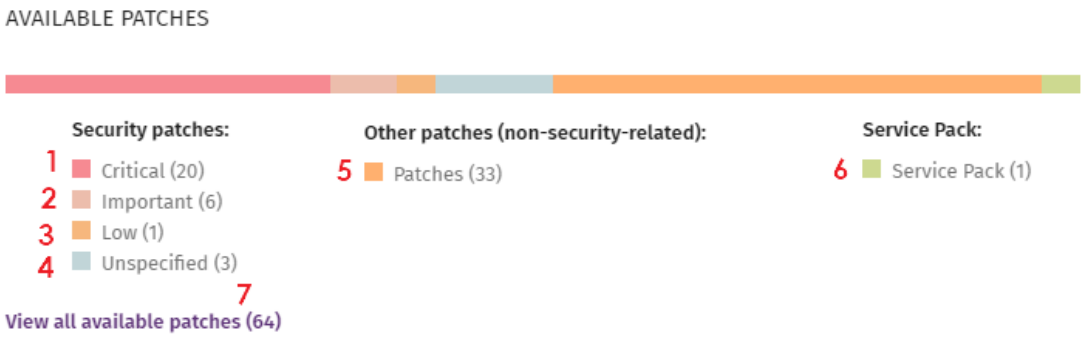


Figure 22.8: Hotspots in the Available patches panel

Click the hotspots shown in Figure 22.8: to open the **Available patches by computers** list with the following predefined filters:

Hotspot	Filter
(1)	Criticality = Critical (security-related).
(2)	Criticality = Important (security-related).
(3)	Criticality = Low (security-related).
(4)	Criticality = Unspecified (security-related).
(5)	Criticality = Other patches (non-security-related).
(6)	Criticality = Service Pack.
(7)	No filters.

Table 22.10: Filters available for the Available patches by computers list

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Definition
Computer type	• Workstation • Laptop • Server
Platform	• All • Windows • Linux • macOS
Patch type	• Operating system patches: Patches available for Windows, Linux, and macOS operating systems. • App patches: Patches available for apps.

Table 22.11: Filters available in the Available patches widget

Available patches trend

Shows the trend of the number of patches that are pending installation on the computers on the network, grouped by severity.

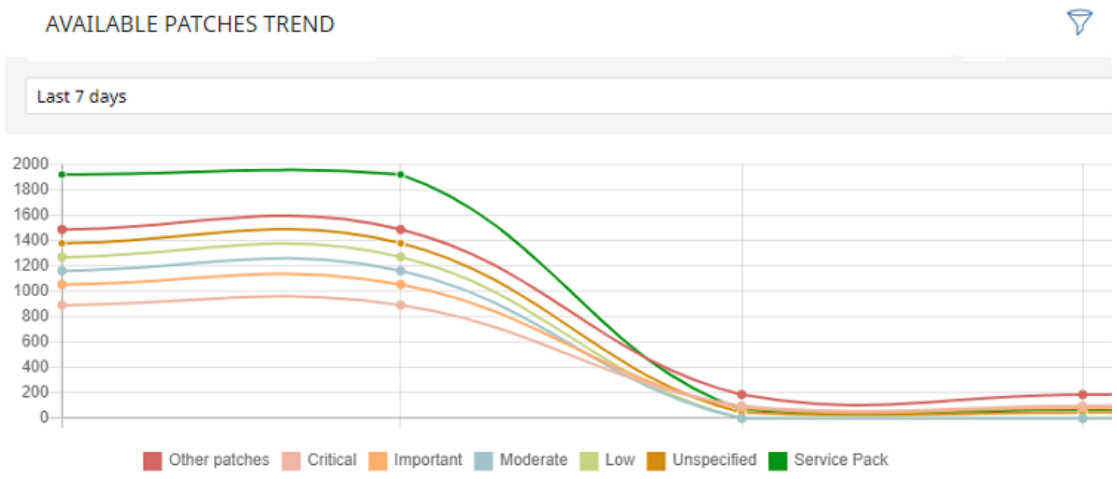


Figure 22.9: Available patches trend graph

Meaning of the data displayed

Data	Description
Security patches - Critical	Number of security patches classified as Critical that are missing from computers.

Data	Description
Security patches - Important	Number of security patches classified as Important that are missing from computers..
Security patches - Low	Number of security patches classified as Low that are missing from computers.
Security patches – Unspecified	Number of security patches that do not have a severity classification and are missing from computers.
Other patches (non-security related)	Number of patches not related to security that are missing from computers.
Service Packs	Number of patch and hotfix bundles that are missing from computers. Not applicable for Linux or macOS computers.

Table 22.12: Description of the data displayed in the Available patches trend panel

Point to a node on the graph to show a tooltip with this information:

- Date
- Type
- Number of patches

Lists accessible from the panel

Click the legend items below the graph to open the **Available patches by computers** list filtered by the selected item. Click the graph to open the full **Available patches by computers** list with no filters applied.

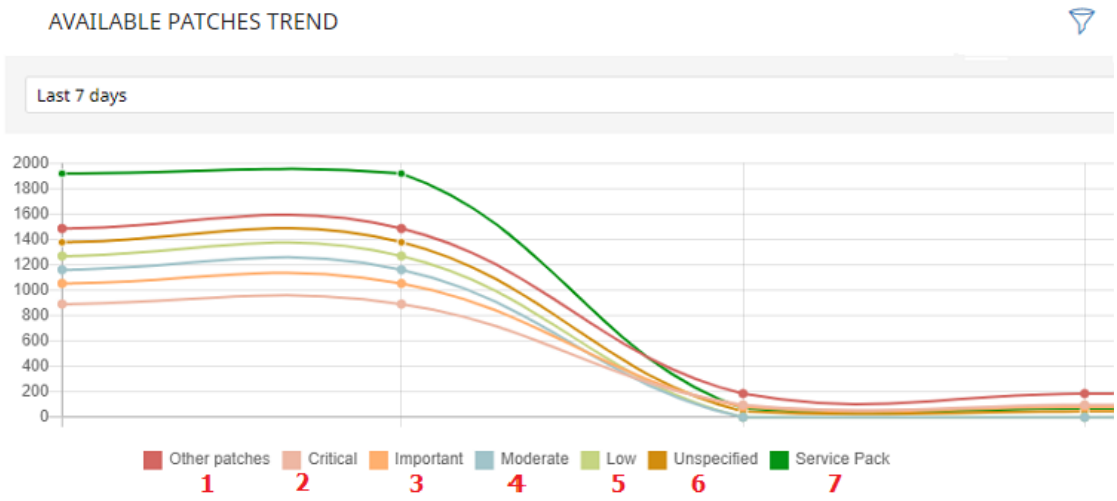


Figure 22.10: Data displayed in the Available patches trend graph

Hotspot	Filter
(1)	Criticality = Other patches (non-security-related).
(2)	Criticality = Critical (security-related).
(3)	Criticality = Important (security-related).
(4)	Criticality = Moderate (security-related).
(5)	Criticality = Low (security-related).
(6)	Criticality = Unspecified (security-related).
(9)	Criticality = Service Pack.

Table 22.13: Filters available for the Available patches by computers list

Filters available in the widget

Click the  icon to see filters you can apply to the information in the widget:

Filter	Definition
Computer type	• Workstation • Laptop • Server
Platform	• All • Windows • Linux • macOS
Patch type	• Operating system patches: Patches available for Windows, Linux, and macOS operating systems. • App patches: Patches available for apps.

Table 22.14: Filters available in the Available patches trend widget

Most available patches for computers

Lists available patches (in **Pending** status) and the number of devices the patch is available for, in descending order from left to right.

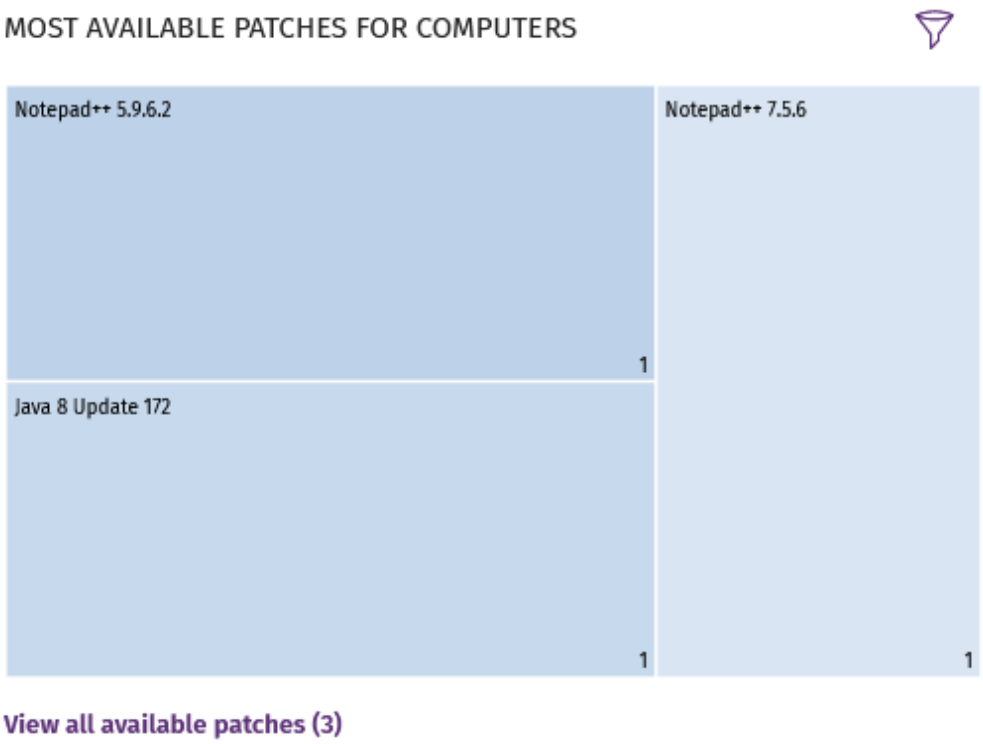


Figure 22.11: Most available patches for computers panel

Meaning of the data displayed

Data	Description
Name	Name of the available patch.
Number	Number of computers the patch is available for (the patch is in **Pending** status).
View all available patches link	Access to the Available patches by computers full list

Table 22.15: Description of the data displayed in the Most available patches for computers panel

Point to a box in the panel to see a summary of the patch, including:

- Patch name.
- Number of affected computers.
- Program (or operating system family).
- Criticality.

- Release date
- CVE (Common Vulnerabilities and Exposures) ID.

Lists accessible from the panel

Click a box in the panel to open the **Available patches by computers** list filtered to the selected patch.

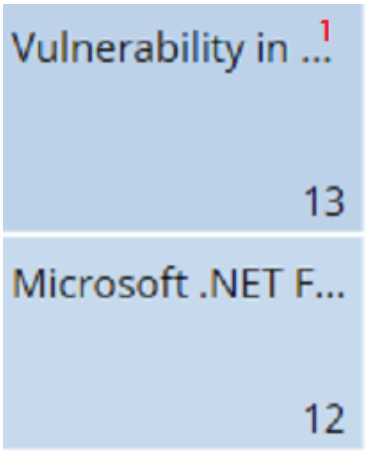


Figure 22.12: Hotspots in the Most available patches for computers panel

Hotspot	Filter
(1)	Patch = Name of the selected patch.

Table 22.16: Lists available from the Most available patches for computers panel

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Description	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack

Filter	Description	Values
Computer type	Type of device affected by the patch.	• Workstation • Laptop • Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Patch type	Type of software affected by the patch.	• App patches • Operating system patches

Table 22.17: Filters available in the Most available patches for computers panel

Programs with most available patches

Lists the programs that are missing patches, as well as the number of patches the program is missing, in descending order from left to right.

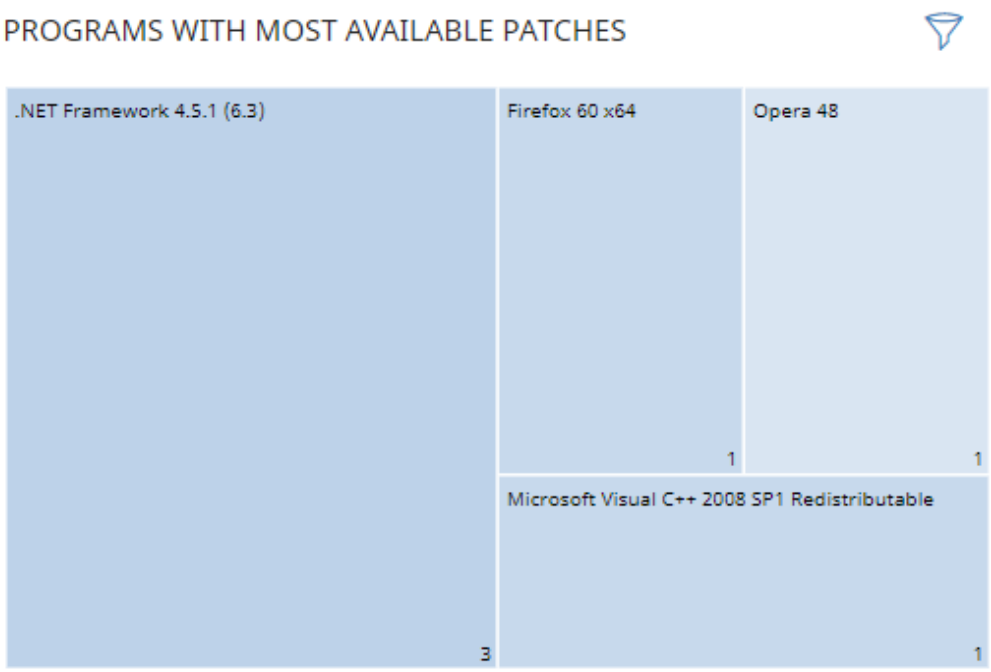


Figure 22.13: Programs with most available patches panel

Meaning of the data displayed

Data	Description
Name	Name of the program that is missing patches.
Number	Number of patches the program is missing.

Table 22.18: Description of the data displayed in the Programs with most available patches panel

Point to a box in the panel to see this information:

- Program name.
- Number of patches the program is missing.

Lists accessible from the panel

Click a box in the panel to open the **Available patches by computers** list filtered to the selected program.

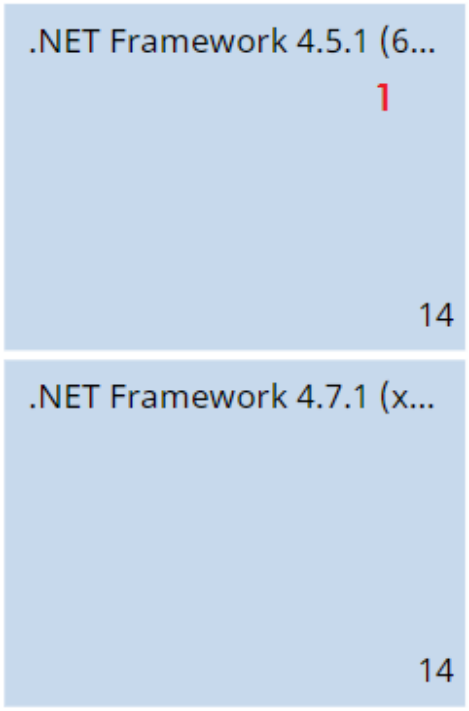


Figure 22.14: Hotspots in the Programs with most available patches panel

Hotspot	Filter
(1)	Program = Name of the selected program.

Table 22.19: Lists available from the Programs with most available patches panel

Filters available in the widget

Click the icon to see filters you can apply to the information in the widget:

Filter	Description	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computer type	Type of device affected by the patch.	• Workstation • Laptop • Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Patch type	Type of software affected by the patch.	• App patches • Operating system patches

Table 22.20: Filters available in the Programs with most available patches panel

Vulnerability assessment module lists

Accessing the lists

There are two methods to access the lists:

- Select **Status** from the top menu. Select **Vulnerability assessment** from the side menu. Click the relevant widget.

  Or,

- Select **Status** from the top menu. Click the **Add** link from the side menu. A window opens with the available lists.
- Select a list from the **Vulnerability assessment** section to view the associated template. Edit the template and click **Save**. The list is added to the side menu.

Required permissions

Permissions	Access to lists
No permissions	• Vulnerability assessment status
View available patches	Read-only access to these lists: • Vulnerability assessment status • Available patches by computers • End-of-Life programs

Table 22.21: Permissions required to access the vulnerability assessment lists

Vulnerability assessment status

Shows all computers on the network that are compatible with vulnerability assessment (with filters that enable you to identify workstations and servers that are not using the service due to any of the reasons shown in the associated panel).

Field	Comment	Values
Computer	Name of the computer with out-of-date software.	Character string
Computer status	Agent reinstallation: •  Reinstalling the agent. •  Error reinstalling the agent. Protection reinstallation: •  Reinstalling the protection. •  Error reinstalling the protection. •  Pending restart. Computer isolation status: •  Computer in the process of being isolated.	Icon

Field	Comment	Values
	• Isolated computer. • Computer in the process of stopping being isolated. "RDP attack containment" mode: • Computer in "RDP attack containment" mode. • Ending "RDP attack containment" mode.	
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Vulnerability assessment	Module status.	• Enabled • Disabled • Installation error (error reason) • No license • — No information • Error
Last checked	Date when vulnerability assessment last queried the cloud to check whether new patches had been published.	Date
Last connection	Date when the vulnerability assessment status was last sent to the Cytomic cloud.	Date

Table 22.22: Fields in the Vulnerability assessment status list

*To view a graphical representation of the list data, access the **Vulnerability assessment status** widget.*

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Name of the computer with out-of-date software.	Character string
IP address	The computer's primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Agent version		Character string
Installation date	Date when the module was successfully installed on the computer.	Date
Last connection date	Date when the agent last connected to the Cytomic cloud.	Date
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
Operating system	Operating system installed on the computer, internal version, and patch status.	Character string

Field	Comment	Values
Updated protection	Indicates whether the protection module installed on the computer is updated to the latest version or not.	Boolean
Protection version	Internal version of the protection module.	Character string
Last update on	Date the signature file was last updated.	Date
Vulnerability assessment status	Module status.	• Enabled • Disabled • Install error • No license • No information • Error
Last checked	Date when vulnerability assessment last queried the cloud to check whether new patches had been published.	Date
Isolation status	Indicates whether the computer has been isolated or can communicate normally with other computers on the network.	• Isolated • Not isolated
Installation error date	Date of the unsuccessful attempt to install the module.	Date
Installation error	Reason for the installation error.	• Download error • Execution error
Vulnerability assessment error	Error searching for available patches	Numeric value

Table 22.23: Fields in the Vulnerability assessment status exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Computer type	Type of device.	• Workstation • Laptop • Server
Last checked	Date when vulnerability assessment last queried the cloud to check whether new patches had been published.	• All • More than 3 days ago • More than 7 days ago • More than 30 days ago
Last connection	Date when the agent last connected to the Cytomic cloud.	Date
Vulnerability assessment status	Module status.	• Enabled • Disabled • Install error • No license • No information • Error

Table 22.24: Filters available in the Vulnerability assessment status list

Computer details page

Click any of the rows in the list to open the computer details page. See **Computer details** on page **252** for more information.

Available patches by computers

Shows all patches that are available for computers and information about patches in the process of installation.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Version	Version number of the out-of-date program.	Numeric value
Release date	Date when the patch was released for download and application.	Date
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Computers	Number of computers the patch is available for.	Numeric value

Table 22.25: Fields in the Available patches by computers list

To view a graphical representation of the list data, access the ***Available patches*** *on page* ***467*** *widget.*

Fields displayed in the exported file

Use the context menu to export the data. The export file can include all data in the list of available patches or a smaller version that shows information about the available patches in the last 7 days, the last month, or the last year.

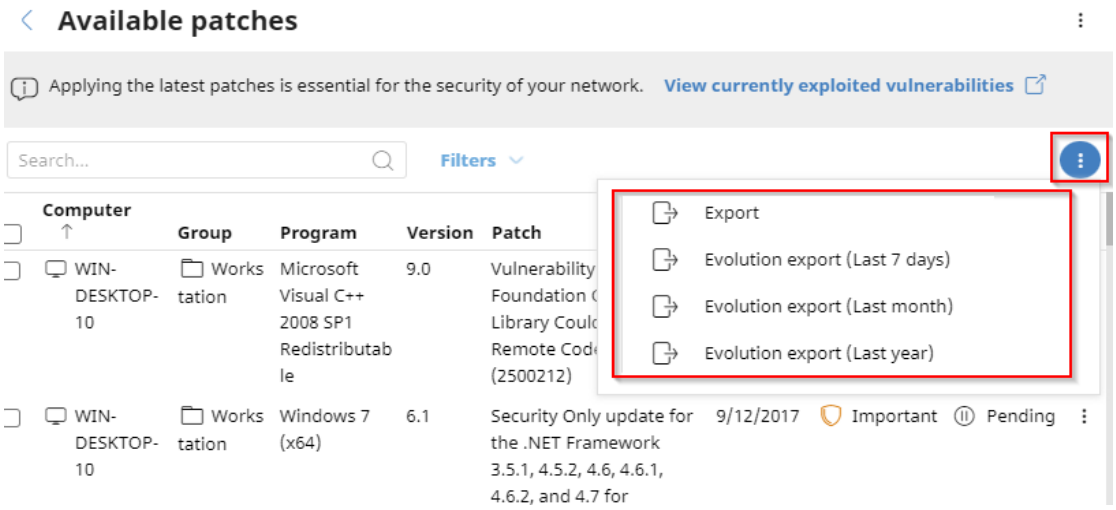


Figure 22.15: Context menu for data export

Field	Comment	Values
Vendor	The company that created the out-of-date program.	Character string
Product family	Name of the product with patches pending installation or a reboot.	Character string
Program version	Version number of the out-of-date program.	Numeric value
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Version	Version number of the out-of-date program.	Numeric value
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string

Field	Comment	Values
Criticality	Update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and the patch requirements (if any).	Character string
Release date	Date when the patch was released for download and application.	Date
Computers	Number of computers the patch is available for.	Numeric value
Platform	Operating system installed on the computer.	• Windows • Linux • macOS

Table 22.26: Fields in the Available patches by computers exported file

Filter tool

Field	Comment	Values
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
Computer type	Type of device.	• Workstation • Laptop • Server
Patch type	Type of available patch.	• App patches • Operating system patches
Search computer	Computer name.	Character string
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
CVE	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Select a program version, family, or vendor	The search applies to the selected program, product family, or company.	Character string
Criticality	Indicates the update severity classification and type.	• Other patches (non-security related) • Critical (security-related)

Field	Comment	Values
		• Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Show non-downloadable patches	Shows patches that cannot be downloaded directly because there are additional requirements set by the vendor (EULA acceptance, login credentials, captcha, etc.)	Boolean

Table 22.27: Filters available in the Available patches by computers list

Detected patch page

Click a row in the list. The **Detectedpatch** page opens and shows details of the patch. This data might vary depending on the operating system installed on the computer.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the out-of-date program or operating system version with missing patches.	Character string
Program version	Version number of the out-of-date program. Not available for macOS or Linux patches.	Character string
Family	Name of the product with patches pending installation or a reboot. Not available for macOS or	Character string

Field	Comment	Values
	Linux patches.	
Vendor	The company that created the out-of-date program. Not available for macOS or Linux patches.	Character string
Criticality	Indicates the update severity classification and type.	• Other patches (non-security related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID describing the vulnerability associated with the patch.	Character string
Release date	Date when the patch was released for download and application.	Date
KB ID	ID of the Microsoft Knowledge Base article describing the vulnerability fixed by the patch and the patch requirements (if any). Not available for macOS or Linux patches.	Character string

Field	Comment	Values
Description	Information about the impact the vulnerability could have on computers. Not available for macOS or Linux patches.	Character string

Table 22.28: Fields on the Detected patch page

End-of-Life programs

Shows information about programs that have reached or are close to end of life. These programs are no longer supported by the software vendor and are particularly vulnerable to malware and cyberthreats.

Field	Comment	Values
Computer	Name of the computer with software that has reached end of life.	Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Program	Name of the program that has reached end of life.	Character string
Version	Version of the program that has reached end of life.	Character string
EOL	Date when the program reached end of life.	Date (in red if the program has reached end of life)

Table 22.29: Fields in the End-of-Life programs list

To view a graphical representation of the list data, access the ***End-of-Life programs*** *on page* ***462****.*

Fields displayed in the exported file

Field	Comment	Values
Client	Customer account the service belongs to.	Character string

Field	Comment	Values
Computer type	Type of device.	• Workstation • Laptop • Server
Computer	Computer name.	Character string
Platform	Operating system installed on the computer.	• Windows • Linux • macOS
IP address	The computer's primary IP address.	Character string
Domain	Domain the computer belongs to.	Character string
Description		Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Program	Name of the program that has reached end of life.	Character string
Version	Version of the program that has reached end of life.	Character string
EOL	Date when the program reached end of life.	Date
Last seen	Date when the computer was last discovered.	Date

Table 22.30: Fields in the End-of-Life programs exported file

Filter tool

Field	Comment	Values
Search computer	Computer name.	Character string
Computer type	Type of device.	• Workstation • Laptop

Field	Comment	Values
		• Server
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS
End-of-Life date	Date when the program will reach end of life.	• All • Currently in End of Life • In End of Life (currently or in 1 year)

Table 22.31: Filters available in the End-of-Life programs list

Program details page

Click a row in the list. The **Program details** page opens.

Field	Comment	Values
Program	Name of the program or Windows operating system version that received the patch.	Character string
Family	Bundle, suite, or program group the software belongs to.	Character string
Publisher/Company	Company that designed or published the program.	Character string
Version	Program version.	Character string
EOL	Date when the program reached end of life.	Date

Table 22.32: Fields on the Program details page

Chapter 23

Managing threats, items in the process of classification, and quarantine

Advanced EPDR provides a balance between the effectiveness of the security service and the impact on the daily activities of protected users. This is achieved through tools that enable you to manage the way detected items are blocked from executing:

- Programs classified as malware.
- Programs classified as PUPs.
- Programs classified as exploits.
- Programs classified as viruses.
- Unknown programs in the process of classification.
- Network attacks.

For more information about how to allow the execution of unknown programs in the process of classification, see ***Authorized software settings*** *on page* ***581****.*
For more information about the Hardening and Lock modes of the advanced protection, see ***Advanced protection*** *on page* ***333****.*

Chapter contents

Introduction to threat management tools

You can change the behavior of Advanced EPDR with regard to found threats and unknown files in the process of classification using these tools:

- Unblock unknown processes.
- Allow the execution of programs classified as malware, PUP, or exploit.
- Do not detect a network attack again.
- Change the Advanced EPDR reclassification policy.
- Manage the backup/quarantine area.

Unblock unknown processes

Advanced EPDR automatically analyzes and classifies all unknown processes in the first 24 hours after detection on a workstation or server. This process classifies the process as goodware or malware and shares the classification with all Cytomic customers.

To strengthen the security of the computers on the network, Advanced EPDR provides **Hardening** and **Lock** modes in the advanced protection settings. In both modes, the security software blocks processes during the classification process to prevent potential risks. Classification is performed in two ways:

- **Automated analysis**: Primary method of classification. Machine learning processes analyze samples in real time.
- **Manual analysis**: If the automated analysis cannot return a classification of the unknown process with 99.999% certainty, then a malware expert manually analyzes a sample of the process. This analysis can take a short period of time to complete.

In circumstances where classification is not immediate, you can allow a blocked item after the security software detects and blocks it. Advanced EPDR provides several strategies to do this:

- **Reactive unblocking**: You allow the execution of an unknown program in the process of classification after a user tries to use it and Advanced EPDR detects and blocks it. For more information, see **Allowing blocked items to run**.

- **Proactive unblocking**: You make sure that unknown programs are never blocked, preventing any negative impact on user performance. For more information, see Authorized software settings.

Allow the execution of programs classified as malware, PUP, or exploit

Administrators can allow software that Advanced EPDR classified as a threat. For example, a toolbar with extra search capabilities classified as a PUP. For more information, see **Allowing blocked items to run**.

Do not detect a network attack again

When Advanced EPDR detects traffic behavior that it suspects to be a network attack, Network Attack Protection prevents this traffic from reaching user computers. If you do not consider the traffic behavior a threat, you can create an exclusion for the source IP address and the type of attack.

Change the reclassification policy

If you unblock an unknown item that was previously blocked Advanced EPDR, the classification process, after some time, catalogs the item as malware or goodware. If it is classified as goodware, then there are no additional steps to continue to allow the item to run. If it is classified as malware, then the reclassification policy is applied. The reclassification policy enables you to define the behavior of Advanced EPDR for this item. For more information, see **Reclassification policy**.

Manage the backup/quarantine area

You have tools to restore items considered to be threats deleted from user computers.

Security software behavior

Known files

If a known file is classified as malware, PUP, or exploit and the advanced protection operating mode is **Hardening** or **Lock**, then Advanced EPDR blocks the file, unless the administrator allows it to run.

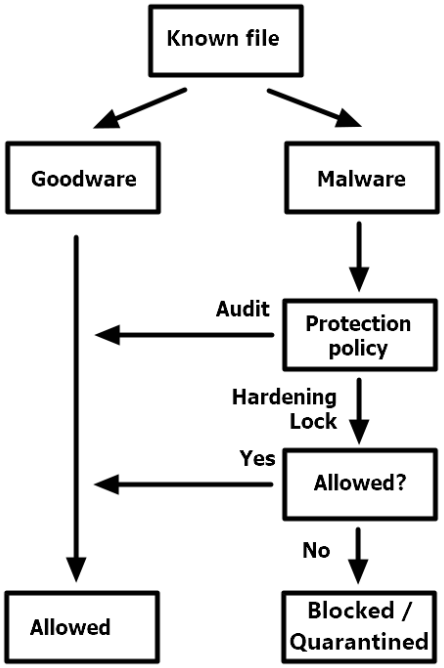


Figure 23.1: Action diagram for known, classified processes

Unknown files

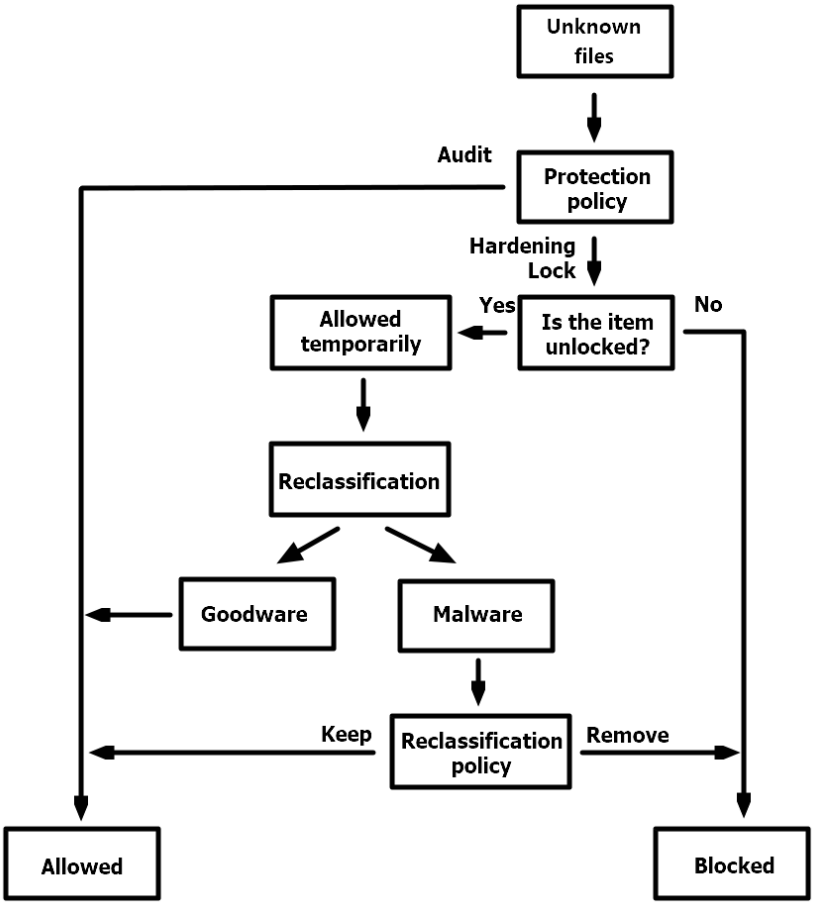


Figure 23.2: Action diagram for unknown files

When an unknown file is in the process of classification and the advanced protection operating mode is **Hardening** or **Lock**, then:

- If you have not configured the unblocking of files:
  - The security software blocks the file.
  - Advanced EPDR allows the file to run if, after classification, the file is determined to be goodware.
  - Advanced EPDR prevents the file from running if, after classification, the file is determined to be malware.
- If you have configured the unblocking of files:
  - Advanced EPDR allows the file to run while the classification process completes.
  - If the file is goodware, Advanced EPDR continues to allow the file to run.
  - If the file is malware, Advanced EPDR allows or does not allow the file to run based on the reclassification policy. For more information, see **Reclassification policy**.

Allowing blocked items to run

Use these panels according to the type of blocked item you want to allow to run:

- **Currently blocked programs being classified**: Unblock items in the process of classification.
- **Malware activity:** Allow the execution of programs classified as malware.
- **PUP activity**: Allow the execution of programs classified as PUPs.
- **Exploit activity**: Allow the execution of exploit techniques.
- **Threats detected by the antivirus**: Restore, from quarantine, items that Advanced EPDR deleted that matched a signature in the signature file.
- **Network attacks**: Allow traffic classified as dangerous by the Network Attack Protection.

Unblocking items pending classification

In general, it is not recommended to allow the execution of unclassified items as this could pose a risk to the integrity of the company data and IT systems.

If users cannot wait for classification of an item, the administrator can unblock it manually.

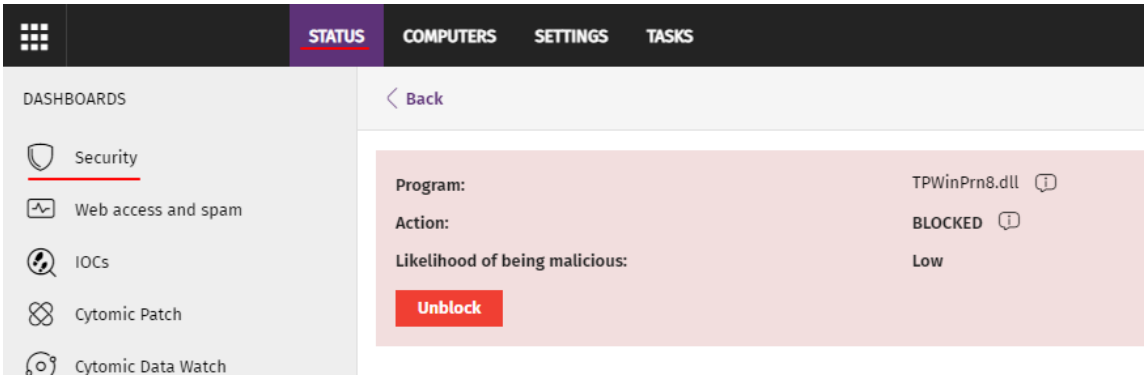


Figure 23.3: Unblocking an item in the process of classification

To allow the execution of an unknown item in the process of classification:

- From the top menu, select **Status**. From the side panel, select **Security**.
- Click the **Currently blocked programs being classified** panel and select the item you want to unblock from the list.
- Click **Unblock**. A page opens to inform you of the risk of unblocking the unknown item and the assessment of its risk level.
- Click **Unblock**. Advanced EPDR performs these actions:
    - Allows the item to run on all managed computers on the IT network.
    - Allows all libraries and binary files used by the program to run, except those already known and classified as threats
    - Removes the item from the **Currently blocked programs being classified** list.
    - Adds the item to the **Programs allowed by the administrator** list.
    - Adds the item to the **History of programs allowed by the administrator** list..
    - Continues to analyze the item until it is classified.

Allowing the execution of items classified as malware, PUP, or exploit

> ⚠ *In general, it is not recommended to allow the execution of items classified as a threat, because this poses a clear risk to the integrity of the company data and IT systems.*

If users need to use certain features provided by a program classified as a threat and the administrator considers that the danger posed to the integrity of the managed IT network is low, the administrator can allow the program.

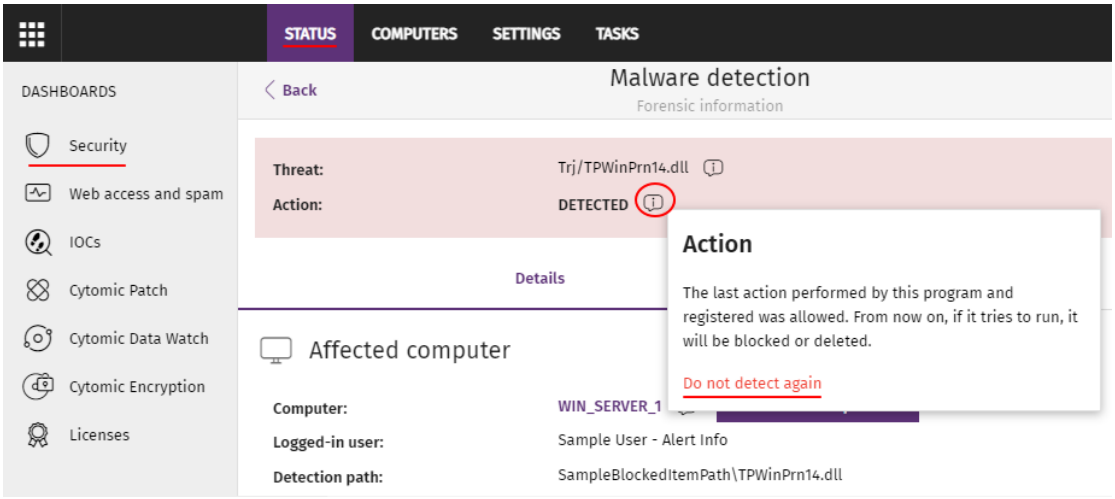


Figure 23.4: Allowing a threat to run

To allow execution of a program classified as malware, PUP, or exploit:

- From the top menu, select **Status**. From the side panel, select **Security**.
- Click the **Malware activity**, **PUP activity**, or **Exploit activity** panel and select the threat that you want to allow to run.
- On the details page, click the  icon next to the action. A pop-up dialog box describes the action taken by Advanced EPDR.
- Click **Do not detect again**. Advanced EPDR performs these actions:
    - Allows the item to run on all computers managed by the administrator. With exploits, you allow the execution of the specific exploit technique that was used on the specific vulnerable program.
    - Allows all libraries and binary files used by the program to run, except those already known and classified as threats.
    - Adds the item to the **Programs allowed by the administrator** list.
    - Stops generating incidents for the item in the **Malware**, **PUP**, and **Exploit** panels.

Restoring or stopping detecting programs classified as viruses

If users have to use certain features provided by a program whose signature file was classified as a threat, and you determine that the danger posed to the integrity of the managed IT network is low, you can allow the program to run.

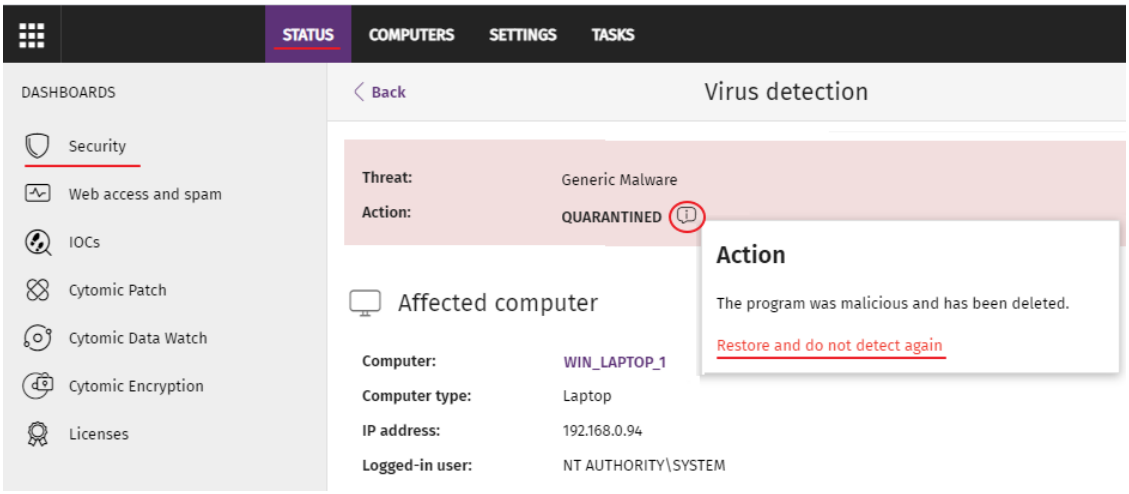


Figure 23.5: Restore and do not detect a threat again

To restore deleted programs from the quarantine or backup area and not detect them again:

- From the top menu, select **Status**. From the side panel, select **Security**.
- Click the **Threats detected by the antivirus** panel and select the item that you want to allow to run.
- On the details page, click the icon next to the action. A pop-up dialog box describes the action taken by Advanced EPDR.
- Click **Restore and do not detect again**. Advanced EPDR performs these actions:
  - Copies the item from quarantine or the backup area to its original location on the computers in the network.
  - Allows the item to run and does not generate any detections.
  - Adds the item to the **Programs allowed by the administrator** list.

Stopping detecting a network attack

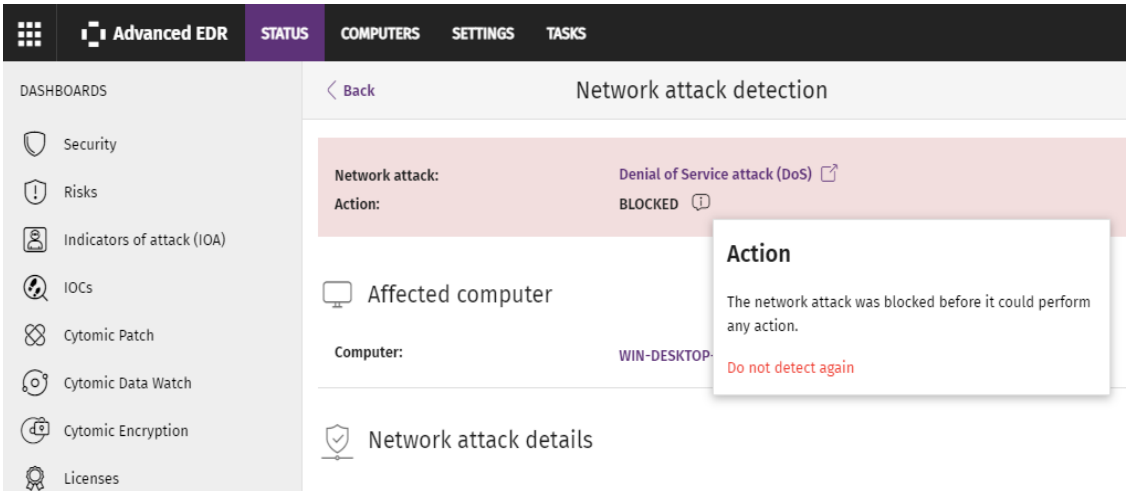


Figure 23.6: Do not detect a network attack again

If you do not consider the traffic blocked a threat, you can create an exclusion for the source IP address and the type of attack.

The exclusion applies to all computers managed by Advanced EPDR.

To stop blocking an item and create an exclusion for Network Attack activity:

- From the top menu, select **Status**. From the side panel, select **Security**.
- Click the **Network Attack Activity** panel. Select the type of network attack you want to allow.
- On the details page, click the  icon next to the action. A pop-up dialog box describes the action taken by Advanced EPDR.
- Click **Do not detect again**. The **Do not detect again** box opens. It shows the type of attack and the source IP address.
- In **Allow this type of network attack only from the following IPs** text box, enter the source IP addresses from which you want to allow inbound traffic for the attack type. You can enter individual IP addresses separated by commas or IP address ranges separated by a dash. If you want to allow any IP address to send traffic of the specified attack type, leave the text box empty.
- Click **Do not detect again**. Advanced EPDR performs these actions:
    - Allows inbound traffic corresponding to the attack type to enter the network if the source IP address is on the list.
    - Stops generating detections for this traffic.
    - Includes the attack type in the **Detected items allowed by the administrator list** list.

Stopping allowing the execution of previously allowed items

To block a previously allowed item again:

- From the top menu, select **Status**. From the side panel, select **Security**.
- In the **Detected items allowed by the administrator** list, click the  icon to the right of the item that you want to stop allowing to run.

Advanced EPDR performs these actions:

- Removes the item from the **Detected items allowed by the administrator** list.
- Adds an entry to the **History of items allowed by the administrator** list. The **Action** column shows **Exclusion removed by the user**.
- Adds the item back to the corresponding list:

- **Malware activity**
- **PUP activity**
- **Exploit activity**
- **Threats detected by the antivirus**
- **Network attack activity**

- If it is virus, the item reappears in the **Threats detected by the antivirus** list.
- Resumes generating incidents for the item.
- If the item is an unknown item in the process of classification, it reappears in the **Currently blocked programs being classified** list.

Unblocking an item in the process of classification

You have multiple panels and lists available to get information about blocked programs in the process of classification:

- The **Currently blocked programs being classified** panel.
- The **Currently blocked programs being classified** list.
- The **History of blocked programs** list.

Additionally, you can perform maintenance actions from the **Currently blocked programs being classified** list, removing programs that Advanced EPDR cannot analyze for a number or reasons. See **Removing unknown processes from lists**.

Currently Blocked Programs Being Classified panel

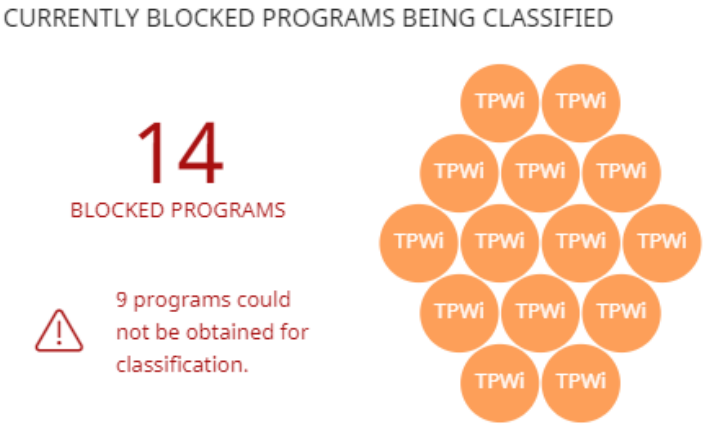


Figure 23.7: Currently Blocked Programs Being Classified panel

Advanced EPDR reports incidents in the **Currently blocked programs being classified** panel when it detects the execution of a program that has not yet been classified. This panel shows all blocked

items that have not yet been classified from the time the protection service was activated until the present time.

The threats copied from computers on the network show the IP address of the computer from which an infection originated, as well as the number of times that IP address was the source of a detection (in parentheses). To open the **Malware activity** list, click the IP address. See **Malware/PUP activity** on page **691**.

To prevent too many detections of the same program in the console, Advanced EPDR reports a maximum of one incident every 24 hours for each hash found on each computer.

*This widget is not affected by the time period you select in the top menu **Status**, side option **Security**.*

Each blocked program in the process of classification is represented by a circle with these characteristics:

- Each circle corresponds to an item with a different hash.
- The color of the circle represents the risk level temporarily assigned to the item.
- The size of the circle represents the number of different computers where the blocked unknown program tried to run. The size **does** not represent the number of execution attempts on the computers on the network.

Additionally, the number of programs that could not be sent to the Cytomic cloud for analysis is specified.

Meaning of the data displayed

Blocked applications have one of these colors:

Data	Description
Orange	Applications with a medium probability of being malware.
Dark orange	Applications with a high probability of being malware.
Red	Applications with a very high probability of being malware.
Blocked programs	Total number of different applications blocked.
Programs that could not be obtained for classification	Total number of blocked programs where an error occurred when the solution tried to classify them.

Data	Description
Threats copied from computers on the network	IP address of the computer from which an infection originated, and number of times that IP address was the source of a detection.

Table 23.1: Description of the data displayed in the Currently Blocked Programs Being Classified panel

When you point the mouse to a circle, it expands, showing the full name of the item and a series of icons that represent key actions:

- **Folder**: The program read data from the user hard disk.
- **Globe**: The program connected to another computer.

Figure 23.8: Graphical representation of a program in the process of classification

Lists accessible from the panel

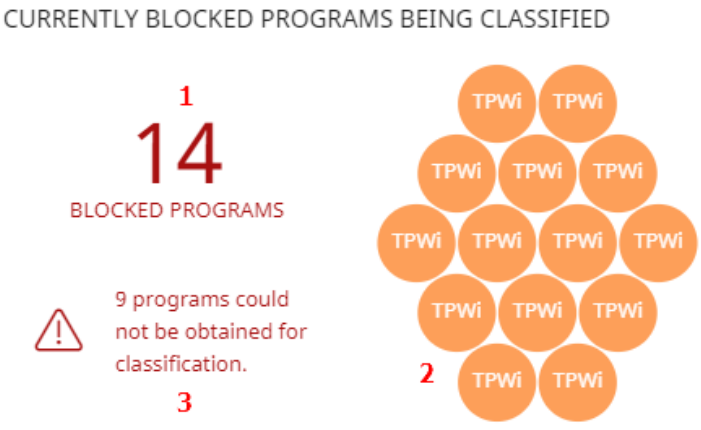


Figure 23.9: Hotspots in the Currently Blocked Programs Being Classified panel

Click the hotspots shown in **Figure 23.9:** to open the **Currently blocked programs being classified** list with these predefined filters:

Hotspot	Filter
(1)	No filter.
(2)	Search = Hash.
(3)	Status = Couldn't get the file

Table 23.2: Filters available in the Currently Blocked Programs Being Classified list

Currently Blocked Programs Being Classified list

This list shows all blocked files that have not yet been classified.

Field	Comment	Values
Computer	Name of the computer where the unknown file was found.	Character string
Path	Name and location of the unknown file on the user computer.	Character string
Accessed data 	The unknown file accessed data on the user computer.	Boolean
Made external connections 	The unknown file communicated with remote computers to send or receive data.	Boolean
Protection mode	Advanced protection operating mode when the unknown file was detected.	• Audit • Hardening • Lock
Likelihood of being malicious	Likelihood that the unknown item is actually malware.	• Medium • High • Very high
Status	Classification process status:	Enumeration

Field	Comment	Values
	• **Getting the program**: The program is being sent to the Cytomic cloud for analysis. • **Classifying**: The program was sent successfully to the Cytomic cloud and is being analyzed. • **Couldn't get the file**: An error occurred and the program did not reach the Cytomic cloud.	
Date	Date the unknown file was first seen.	Date

Table 23.3: Fields in the Currently Blocked Programs list

Fields displayed in the exported file

*The context menu of the **Currently blocked programs being classified** list shows a drop-down menu with two options: **Export** and **Export list and details**. This section describes the content of the file generated when you select **Export**. For more information about the **Export list and details** option, see* ***Exported Excel files** on page **844**.*

Field	Comment	Values
Computer	Name of the computer where the unknown file was found.	Character string
Threat	Name of the unknown file.	Character string
Path	Name and location of the unknown file on the user computer.	Character string
Protection mode	Protection operating mode when the unknown file was detected.	• Audit • Hardening • Lock
Accessed data	The unknown file accessed files on the user computer.	Boolean
External connections	The unknown file communicated with remote computers to send or receive data.	Boolean

Field	Comment	Values
Likelihood of being malicious	Likelihood that the unknown item is actually a threat when the classification process is completed.	• Medium • High • Very high
Date	Date the unknown file was first seen.	Date
Dwell time	Period of time during which the threat was on the customer network without being classified.	Date
User	User account under which the program was run.	Character string
MD5	MD5 hash of the file.	Character string
SHA-256	SHA-256 hash of the file.	Character string
Threat source computer	Name of the computer, if the blocked program came from another computer on the customer network.	Character string
Threat source IP address	IP address of the computer, if the blocked program came from another computer on the customer network.	Character string
Threat source user	The user who was logged in on the computer that the blocked program came from, if applicable.	Character string
Status	Classification process status: • **Getting the program**: The program is being sent to the Cytomic cloud for analysis. • **Classifying**: The program was sent successfully to the Cytomic cloud and is being analyzed. • **Couldn't get the file**: An error occurred and the program did not reach the Cytomic cloud.	Enumeration

Table 23.4: Fields in the Currently Blocked Programs exported file

Filter tool

Field	Comment	Values
Dates	Set a time period, from the present time back.	• Last 24 hours • Last 7 days • Last month
Search	• **Computer**: Device where the unknown item resides. • **Threat**: File name. • **Hash**: String that identifies the file. • **Threat source**: Search by the user, IP address, or name of the computer the blocked item came from.	Enumeration
Protection modes	Advanced protection operating mode when the unknown file was detected.	• Hardening • Lock
Accessed data	The unknown file accessed data on the user computer.	Boolean
External connections	The unknown file communicated with remote computers to send or receive data.	Boolean
Status	Classification process status: • **All** • **Getting the program**: The program is being sent to the Cytomic cloud for analysis. • **Classifying**: The program was sent successfully to the Cytomic cloud and is being analyzed. • **Couldn't get the file**: An error occurred and the program did not reach the Cytomic cloud.	Enumeration

Table 23.5: Filters available in the Currently Blocked Programs list

Details page

This page shows detailed information about the blocked program. See **Block of unknown programs in the process of classification and history of blocked programs** on page **830**.

History of Blocked Programs list

This list shows a history of all events that have occurred over time regarding unknown processes blocked.

This list does not have an associated panel on the dashboard. To access it, click the **View history of blocked items** link in the upper-right corner of the **Currently blocked programs being classified** list page.

Field	Comment	Values
Computer	Name of the computer where the unknown file was found.	Character string
Path	Name and location of the unknown file on the user computer.	Character string
Action	Action taken by Advanced EPDR.	• Blocked • Reclassified as goodware • Reclassified as malware • Reclassified as PUP
Reclassification time	Time it took Advanced EPDR to classify the item. See **Reclassification time calculation for unknown files**	Date
Accessed data	The unknown file accessed data on the user computer.	Boolean
Made external connections	The unknown file communicated with remote computers to send or receive data.	Boolean
Protection mode	Advanced protection operating mode when the unknown file was detected.	• Audit • Hardening • Lock
Excluded	The unknown file was unblocked/excluded by you. It is allowed to run.	Boolean

Field	Comment	Values
Likelihood of being malicious	Likelihood that the unknown item is actually a threat when the classification process is completed.	• Medium • High • Very high
Date	Date the unknown file was first seen.	Date

Table 23.6: Fields in the History of Blocked Programs list

Fields displayed in the exported file

*The context menu of the **History of blocked programs** list shows a drop-down menu with two options: **Export** and **Export list and details**. This section describes the content of the file generated when you select **Export**. For more information about the **Export list and details** option, see* **Exported Excel files** *on page* **844**

Field	Comment	Values
Computer	Name of the computer where the unknown file was found.	Character string
Threat	Name of the unknown file.	Character string
Path	Location of the unknown file on the user computer.	Character string
Protection mode	Advanced protection operating mode when the unknown file was detected.	• Audit • Hardening • Lock
Action	Action taken by Advanced EPDR.	• Blocked • Reclassified as goodware • Reclassified as malware • Reclassified as

Field	Comment	Values
		PUP
Accessed data	The unknown file accessed data on the user computer.	Boolean
External connections	The unknown file communicated with remote computers to send or receive data.	Boolean
Excluded	The unknown file was unblocked by you. It is allowed to run.	Boolean
Likelihood of being malicious	Likelihood that the unknown item is actually a threat when the classification process is completed.	• Medium • High • Very high
Date	Date the unknown file was first seen.	Date
Reclassification start date	Date the Cytomic cloud received the item.	Date
Reclassification completed	Date the item was classified.	Date
Reclassification time	Time it took Advanced EPDR to classify the item. See **Reclassification time calculation for unknown files**	Date
Classification technique	• **Classified by WatchGuard lab technicians**: The item was classified manually by Cytomic technicians. • **Classified automatically by WatchGuard Collective Intelligence**: The item was classified by Cytomic automatic machine learning processes.	Enumeration
Dwell time	Period of time during which the threat was on the customer network without being classified.	Date

Field	Comment	Values
User	User account under which the program was run.	Character string
MD5	MD5 hash of the file.	Character string
SHA-256	SHA-256 hash of the file.	Character string
Threat source computer	Name of the computer the blocked program came from, if applicable.	Character string
Threat source IP address	IP address of the computer the blocked program came from, if applicable.	Character string
Threat source user	The user that was logged in on the computer the blocked program came from, if applicable.	Character string

Table 23.7: Fields in the History of Blocked Programs exported file

Filter tool

Field	Comment	Values
Search	• **Computer**: Device where the unknown file resides. • **Threat**: Name of the threat. • **Hash**: String that identifies the file. • **Threat source**: Search by the user, IP address, or name of the computer the threat came from.	Enumeration
Dates	Set a time period, from the present time back.	• Last 24 hours • Last 7 days • Last month
Action	Action taken by Advanced EPDR.	• Blocked • Reclassified as goodware • Reclassified as malware

Field	Comment	Values
		• Reclassified as PUP • PUP blocked due to connectivity failure • Malware blocked due to connectivity failure • Goodware blocked due to connectivity failure • Deleted from list
Excluded	The unknown file was unblocked by you. It is allowed to run.	Boolean
Protection modes	Advanced protection operating mode when the unknown file was detected.	• Hardening • Lock
Accessed data	The unknown file accessed data on the user computer.	Boolean
External connections	The unknown file communicated with remote computers to send or receive data.	Boolean

Table 23.8: Fields in the History of Blocked Programs exported file

Details page

This page shows detailed information about the blocked program. For more information, see **Block by advanced security policy** on page **828**.

Removing unknown processes from lists

Unknown processes show in the **Currently Blocked Programs Being Classified panel** widget until Advanced EPDR has analyzed them. Sometimes it is not possible to complete the analysis because the file is too large (larger than 50 MB) or no longer available on the user computer. When this happens, unknown files continue to display in the **Currently blocked programs being classified** widget.

To remove unknown files from the blocked file widget and list:

- From the top menu, select **Status**. From the side menu, select **Security**. Click the **Currently blocked programs being classified** widget. The **Currently blocked programs being classified** list opens.

Or

- From the top menu, select **Status**. From the **My lists** side menu, click **Add**. A dialog box opens and shows the available lists.
- Select the **Currently blocked programs being classified** list.
- Select the checkboxes for the files you want to remove from the list. In the toolbar, click **Delete**. A confirmation dialog box opens.
- Click **Delete**. The deleted items appear in the **History of blocked programs** list with the **Action** field updated to show **Deleted from list**. These files cannot be unblocked.

*You can delete a blocked program that is in the process of classification to simplify the list. Internally, Advanced EPDR continues to consider these items as unknown. If an attempt is made to run them again, they reappear in the **Currently blocked programs being classified** widget and list*

Reclassification time calculation for unknown files

When Advanced EPDR blocks the execution of an unknown file, it calculates the time taken to assign a category and unblock it. Many unknown files are analyzed almost immediately, and the vast majority of more complex files require an analysis time of less than four hours.

The Advanced EPDR console shows the classification time for unknown items in these fields:

- **Reclassification completed**: The date and time when reclassification finished.
- **Reclassification time**: The time it took Advanced EPDR to classify the file. See **Classification time start**.
- **Reclassification start date**: The date and time the Cytomic cloud received the file for analysis.

Classification time start

To mark the start of the classification process, Advanced EPDR uses the earlier of these two dates:

- The date when the item was received on the Cytomic servers.
- The date when the item was blocked on the user device.

In most cases, the classification time starts from when the blocked file is received by the Cytomic cloud, as indicated in the **Reclassification start date** field. However, there are several exceptions to this rule:

- If the user device cannot send the blocked file (because of a a temporary network failure, the file no longer exists in the file system, or the file size requirements are not met) but the file is classified by other means, the **Reclassification time** is the time elapsed between when Advanced EPDR blocked the file on the user device and when it classified it. In this case, the **Reclassification start date** field is empty.
- If the blocked file was sent to the Cytomic cloud previously by another user, but Advanced EPDR blocks it on the user device because the classification is not yet available when the user tries to run it, the **Reclassification time** is the time elapsed between when Advanced EPDR blocked the file on the user device and when it finally classified it.

List of allowed threats and unknown programs

You have multiple panels and lists available to get information about programs that you allow which Advanced EPDR initially prevented from running:

- The **Detected items allowed by the administrator** panel.
- The **Detected items allowed by the administrator** list.
- The **History of items allowed by the administrator** list.

Detected items allowed by the administrator

This panel shows the number of items the administrator allows which Advanced EPDR initially prevented from running. These items were considered a threat or are unknown files under classification.

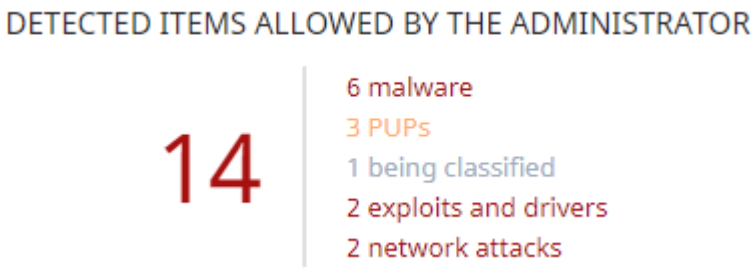


Figure 23.10: Panel Elementos detectados permitidos por el administrador

Meaning of the data displayed

The panel shows the total number of items excluded from blocking, broken down by type:

- Malware
- PUPs
- Being classified

- Exploits and drivers
- Network attacks

Lists accessible from the panel

Figure 23.11: Zonas activas del panel Elementos detectados permitidos por el administrador

Click the hotspots in **Figure 23.11:** to open the **Detected items allowed by the administrator list** list with these predefined filters:

Hotspot	Filter
(1)	No filters.
(2)	Classification = Malware.
(3)	Classification = PUP.
(4)	Classification = Being classified (blocked and suspicious items).
(5)	Classification = Exploits and drivers
(6)	Classification = Network attack.

Table 23.9: Filters available in the Programs Allowed by the Administrator list

Detected items allowed by the administrator list

This list shows all items the administrator allows which Advanced EPDR considered a threat.

Field	Description	Values
Classification	Type of threat that is allowed to run.	• Malware • PUP • Goodware

Field	Description	Values
		• Exploits and drivers • Being classified • Network attack
Threat	Name of the item that is allowed to run. • If it is an unknown item, the field is empty. • If it is an exploit, the exploit technique used appears. • If it is a network attack, the type appears.	Character string
Details	Name of the file that contains the threat. • If it is an unknown item, the column shows the name of the file under classification. • If it is an exploit, the column shows the exploited file name. • In the case of a network attack, you can see the source IP addresses from which the type of attack is allowed.	Character string
Hash	String that identifies the file. This is empty if it is an exploit or network attack.	Character string
User name	Console user account that added the item exclusion.	Character string
Date allowed	Date the event took place.	Date
Delete	Removes the item exclusion.	

Table 23.10: Fields in the Detected Items Allowed by the Administrator list

Fields displayed in the exported file

Field	Description	Values
Details	Name of the file that contains the threat. • If it is an unknown item, the column shows the name of the file under classification. • If it is an exploit, the column shows the exploited file name. • In the case of a network attack, you can see the source IP addresses from which the type of attack is allowed.	Character string
Current type	Current classification of the threat that is allowed to run.	• Malware • PUP • Goodware • Exploits and drivers • Being classified • Network attack
Original type	Classification of the threat that is allowed to run when it was initially detected.	• Malware • PUP • Goodware • Exploit • Being classified • Network attack
Threat	Name of the item that is allowed to run. • If it is an unknown item, the field is empty. • If it is an exploit, the exploit technique used appears. • If it is a network attack, the type appears.	Character string
Hash	String that identifies the file.	Character string

Field	Description	Values
	This is empty if it is an exploit or network attack.	
User name	User account which triggered the change to the allowed file.	Character string
Date allowed	Date the event was logged.	Date

Table 23.11: Fields in the Programs Allowed by the Administrator exported file

Filter tool

Field	Description	Values
Search	• **Details**: Details of the threat. • **Threat**: Name of the threat detected. • **User name**: Console user account that added the item exclusion. • **Hash**: String that identifies the file.	Enumeration
Classification	File type the last time it was classified.	• All • Malware • PUP • Goodware • Exploit • Network attack • Being classified (blocked and suspicious items)
Original classification	Original classification of the file when it was allowed to run.	• All • Malware • PUP • Being classified (blocked item) • Being classified (suspicious item)

Field	Description	Values
		• Exploit • Network attack

Table 23.12: Filters available in the Programs Allowed by the Administrator list

History of items allowed by the administrator list

This list shows a history of all events related to threats and unknown files in the process of classification that the administrator allowed to run. This list shows all classifications that an item has gone through, from the time it entered the **Detected items allowed by the administrator** list until it left it, as well as all other classifications caused by Advanced EPDR or by you.

This list does not have a corresponding panel. You must access it through the **History** button in the upper-right corner of the **Detected items allowed by the administrator** page.

Field	Description	Values
Classification	Type of threat that is allowed to run.	• Malware • PUP • Goodware • Exploit • Being classified • Network attack
Threat	Name of the item that is allowed to run. • If it is an unknown item, the field is empty. • If it is an exploit, the exploit technique used appears. • If it is a network attack, the type appears.	Character string
Details	Name of the file that contains the threat. • If it is an unknown item, the column shows the name of the file under classification. • If it is an exploit, the column shows the exploited file name.	Character string

Field	Description	Values
	• In the case of a network attack, you can see the source IP addresses from which the type of attack is allowed.	
Hash	String that identifies the file. This is empty if it is an exploit or network attack.	Character string
Action	Action taken on the allowed item. • **Exclusion removed by the user**: You allowed the item to be blocked again. • **Exclusion removed after reclassification**: Advanced EPDR applied the action associated with the category after reclassification. • **Exclusion added by the user**: You allowed the item to be run. • **Exclusion kept after reclassification**: Advanced EPDR did not block the item after reclassification.	Enumeration
User name	User account which triggered the change to the allowed file.	Character string
Date allowed	Date the event was logged.	Date

Table 23.13: Fields in the History of Programs Allowed by the Administrator list

Fields displayed in the exported file

Field	Description	Values
Details	Name of the file that contains the threat. • If it is an unknown item, the column shows the name of the file under classification. • If it is an exploit, the column shows the exploited file name. • In the case of a network attack, you can see the source IP addresses from which the type of attack is allowed.	Character string

Field	Description	Values
Current type	Current classification of the threat that is allowed to run.	• Malware • PUP • Exploit • Blocked item • Suspicious item • Network attack
Original type	Classification of the threat that is allowed to run when it was initially detected.	• Malware • PUP • Exploit • Blocked item • Suspicious item • Network attack
Threat	Name of the malware or PUP that is allowed to run. If it is an unknown item, the column shows the file name. If it is an exploit or network attack, the exploit technique used appears.	Character string
Hash	String that identifies the file. If it is an exploit or network attack, this field is blank.	Character string
Action	Action taken on the allowed item. • **Exclusion removed by the user**: You allowed the item to be blocked again. • **Exclusion removed after reclassification**: Advanced EPDR applied the action associated with the category after reclassification. • **Exclusion added by the user**: You allowed the item to be run.	Enumeration

Field	Description	Values
	• **Exclusion kept after reclassification**: Advanced EPDR did not block the item after reclassification.	
User name	Console user account that added the item exclusion.	Character string
Date allowed	Date the event took place.	Date

Table 23.14: Fields in the History of Items Allowed by the Administrator exported file

Filter tool

Field	Description	Values
Search	• **Details**: Details of the threat. • **User name**: Console user account that added the item exclusion. • **Hash**: String that identifies the file.	Enumeration
Classification	File type the last time it was classified.	• All • Malware • PUP • Goodware • Exploit • Network attack • Being classified (blocked and suspicious items)
Original classification	Original classification of the file when it was allowed to run.	• All • Malware • PUP • Being classified (blocked item)

Field	Description	Values
		• Being classified (suspicious item) • Exploit • Network attack
Action	Action taken on the allowed item. • **Exclusion removed by the user**: You allowed the item to be blocked again. • **Exclusion removed after reclassification**: Advanced EPDR applied the action associated with the category after reclassification. • **Exclusion added by the user**: You allowed the item to be run. • **Exclusion kept after reclassification**: Advanced EPDR did not block the item after reclassification.	Enumeration

Table 23.15: Filters available in the History of Items Allowed by the Administrator list

Reclassification policy

The reclassification policy defines the actions Advanced EPDR takes when an item that was unblocked by the administrator is reclassified:

- Advanced EPDR classifies the item as goodware: Allows the item to run.
- Advanced EPDR classifies the item as malware: The reclassification policy is applied. The reclassification policy enables you to define the behavior of Advanced EPDR for this item.

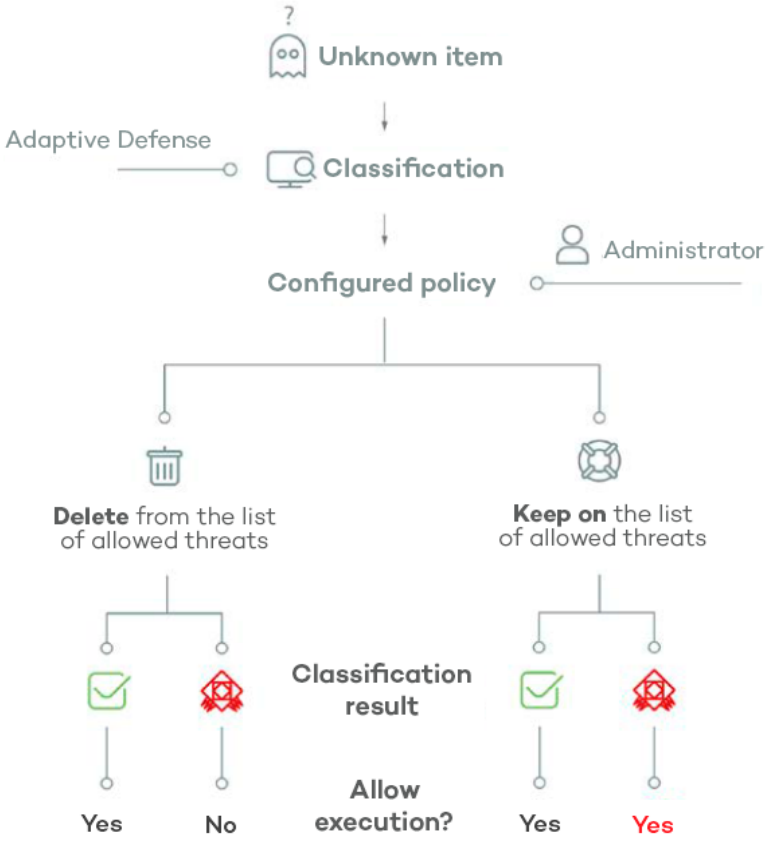


Figure 23.12: Advanced EPDR behavior based on the reclassification policy selected and the classification result

Changing the reclassification policy

The reclassification policy applies to all devices on the network. The assigned security settings profiles do not impact the reclassification policy.

To change the actions that Advanced EPDR takes when a file is reclassified:

- From the top menu, select **Status**. From the side menu, select, select **Security**.
- In the **Programs allowed by the administrator** pane, select the item type:
    - Malware
    - PUPs
    - Being classified
    - Exploits
- Click **Change behavior**. A dialog box opens. Select the action you want to apply.
    - **Remove it from the list of programs allowed by the administrator**: If the unknown file is goodware, then it continues to run normally. If it is malware, the exclusion is removed automatically and the file is blocked, unless the administrator creates an exclusion for the file.

- **Keep it on the list of programs allowed by the administrator**: A red warning in the **Programs allowed by the administrator** list indicates that this option could lead to potentially dangerous exposure. Whether the unknown file is classified as goodware or malware, the exclusion is maintained and the file continues to run.

*We recommend that you do not use the **Keep it on the list of programs allowed by the administrator** setting, as it could open a security hole that enables malware to run on network devices.*

Reclassification of unblocked files

If you selected **Keep it on the list of programs allowed by the administrator** for an item, you should enable alerts and review the history of allowed programs to know whether the security software reclassified it as malware and allowed it to run.

History of allowed programs

To view reclassification and other events for an unblocked file:

- From the top menu, select **Status**. From the side menu, select **Security**.
- Click the **Currently blocked programs being classified** panel.
- Click **View history of blocked items**. The **History of blocked programs** list opens.
- In the Search bar, enter the name of the threat. The **Action** column shows the types of events that occurred For more information, see **History of Blocked Programs list**.

Email alerts

*For more information about email alerts, see **Alerts** on page **855**.*

You can receive an email alert every time an unknown file gets blocked. It is recommend that you configure alerts when a previously unblocked file is reclassified.

To enable email notifications when an unknown file is blocked:

- From the top menu, select **Settings**. From the side menu, select **My alerts**.
- Enable the toggles for these alert types:
    - A program that is being classified gets blocked.
    - A file allowed by the administrator is finally classified.

File classification: Strategy for new software

If you monitor the installation of programs on network devices, you might want to allow unknown software to run without an increased security risk.

This topic describes a strategy for staged installation of new software:

- Configure a test computer.
- Install the new software.
- Reclassify blocked software.
- Send blocked software to Cytomic support

Configure a test computer

With a test computer, determine whether the new software is known malware or is unknown to Cytomic. Make sure that the test computer has the security software installed and advanced protection configured in **Hardening** mode.

Install the new software

Install the new software on the test computer and open it normally. If Advanced EPDR determines that the software contains an unknown module or program, it blocks the software. A dialog box opens to show that the software was blocked and a new item is added to the **Currently blocked programs being classified** list. Advanced EPDR sends the binary files to the cloud for analysis.

If no items are blocked in Hardening mode, change the advanced protection settings to Lock mode. Open the new software again. If additional items are blocked, they show in the **Currently blocked programs being classified** list.

Reclassify blocked software

When Advanced EPDR reclassifies blocked software, you can enable email alerts with information on whether it has unblocked the software or kept the software blocked. If all processes are classified as goodware, the installed software is valid for use across the network.

Send blocked software to Cytomic support

When a file is unknown, Advanced EPDR sends the binary files to the cloud for analysis. Cytomic is designed to prevent network performance issues and could delay when it sends the files to the cloud. To speed up the classification process, contact Cytomic Support.

Managing the backup/quarantine area

The Advanced EPDR quarantine is a backup area that stores items that were deleted after being classified as a threat.

Quarantined items are stored on the user computer, in a `Quarantine` folder in the software installation directory. This folder is encrypted and cannot be accessed by any other process. It is therefore impossible to directly access or run the programs there.

The quarantine feature is only available on Windows, macOS, and Linux endpoints.

The classification and type of threat determines the actions that Cytomic takes on the detected file:

- **Malicious files for which disinfection is not possible**: The file is moved to quarantine permanently.
- **Malicious files for which disinfection is possible**: The file is disinfected and restored to its original location. A copy of the file is stored in quarantine for 30 days.
- **Non- malicious items**: Files determined to be goodware and incorrectly classified as malware (false positive), are automatically restored from quarantine to their original location. A copy of the file is stored in quarantine for seven days
- **Suspicious items**: Files are stored in quarantine for 30 days. If they a determined to be goodware, they are restored to their original location.

Advanced EPDR does not permanently delete files from user computers. All deleted files are sent to a backup folder.

Reviewing quarantined files

To review a list of quarantined items:

- From the top menu, select **Status**. From the side panel, select **Security**.
- Click the panel for the type of threats you want to review:
    - Malware activity.
    - PUP activity.
    - Exploit activity.
    - Threats detected by the antivirus
- Click **Filters**. In the **Action** area, select the **Quarantined** and **Deleted** checkboxes. Click **Filter**.

Restoring files from quarantine

- From the top menu, select **Status**. From the side panel, select **Security**.
- Click the panel for the type of threats you want to restore:

- Malware activity
- PUP activity
- Exploit activity
- Threats detected by the antivirus

- Click **Filters**. In the **Action** area, select the **Quarantined** and **Disinfected** checkboxes.
- Next to the **Action**, click the icon. A pop-up describes why the item was moved to quarantine.
- Click **Restore and do not detect again**. The file is restored to its original location. The permissions, owner, and registry entries related to the file are also restored.

Chapter 24

Forensic analysis

Advanced EPDR detects and blocks the execution of unknown and specially crafted malware designed to go unnoticed by signature-based traditional antivirus solutions. This is achieved by monitoring the actions taken by processes on customers' computers, which are sent to the Cytomic cloud as part of the telemetry collected. Process monitoring enables us to classify every program run on users' computers and determine the extent to which a customer's network has been compromised. With this information about which actions were carried out by malicious processes, network administrators can take the containment and remediation measures appropriate to each case.

The web console makes all this information available to users through various resources, each of which provides different levels of detail:

- Extended detail pages.
- Action tables.
- Graphs.
- Excel files.

Chapter contents

Details of blocked programs

Advanced EPDR provides extended details of programs blocked by any of the advanced detection technologies it incorporates:

- **Malware and PUP detection**
- **Exploit detection**
- **Vulnerable driver**
- **Block by advanced security policy**
- **Block of unknown programs in the process of classification and history of blocked programs**

Malware and PUP detection

Accessing the Malware Details and PUP Details pages

- From the top menu, select **Status**. From the side menu, click the **Add** link. A dialog box opens that shows all available lists.
- Select the **Malware and PUP activity** list.
- Set the filters and click the **Launch query** button. A list opens that shows all items classified as malware or PUP.
- From the list, select an item. The **Malware detection** or **PUP detection** page opens.

Or:

- From the top menu, select **Status**. From the side panel, select **Security**. A page opens that shows all widgets associated with the security module.
- Click the **Malware activity** or **PUP activity** widget.
- Set the filters and click the **Launch query** button. A list opens that shows all items classified as malware or PUP.
- From the list, select an item. The **Malware detection** or **PUP detection** page opens.

The details page is divided into several sections:

- Overview.
- Affected computer.
- Threat impact on the computer.
- Infection source.
- Occurrences on other computers.

Overview

Field	Description	Values
Threat	Name of the threat and hash that identifies it.	• Threat name and type. • Hash (MD5 and/or SHA-256)
Action	Action taken by Advanced EPDR on the item. • **Quarantined**: The file was moved to quarantine. • **Blocked**: The process was blocked before it ran. • **Disinfected**: The file was disinfected. A copy of the original file was moved to quarantine. • **Deleted**: The file was deleted. • **Detected**: The process was detected but not blocked because the advanced protection is configured in Audit mode. • **Allowed (Audit mode)**: The user was informed that the malware performed suspicious actions. Because Audit mode is enabled, threats are detected, but they are not blocked or removed. See **Audit mode** on page **359**.	Enumeration For more information about how to manage detected threats blocked, see **Allowing blocked items to run** on page **785**. See **Restoring files from quarantine** on page **816**.

Table 24.1: Fields of the Overview section on the Malware Detection page

Affected computer

*For more information about the actions you can take on the items found, see **Managing threats, items in the process of classification, and quarantine** on page **781**.*

Field	Description
Computer	Name of the computer where the threat was detected, IP address, and folder in the group tree to which the computer belongs.
View available patches	If the Cytomic Patch module is enabled, this button shows all patches and updates that are missing from the computer.

Field	Description
Logged-in user	Operating system user under which the threat was loaded and run.
Detection path	Threat location on the file system.

Table 24.2: Fields of the Affected Computer section on the Malware Detection and PUP Detection pages

Threat impact on the computer

Field	Description
Threat	Name of the detected threat and file identification string (hash). Two buttons appear to search for additional information on Google and the VirusTotal website. If the threat is newly discovered, the text **New threat** appears.
Activity	Summary of the most important actions taken by the malware: • **Has run** • **Has accessed data files** • **Has exchanged data with other computers** • **View full activity details**: Click this button to open the **Activity** tab described in **Action tables**. • **View activity graph**: Click this button to view the **Activity** graph described in **Execution graphs**.
Detection date	Date when Advanced EPDR detected the threat on the customer network.
Dwell time	Time during which the threat was on the customer network without being classified.

Table 24.3: Fields of the Threat Impact on the Computer section on the Malware Detection and PUP Detection pages

Infection source

Field	Description
Threat source computer	Name of the computer, if the infection attempt originated from

Field	Description
	another computer on the customer network.
Threat source IP address	IP address of the computer, if the infection attempt originated from another computer on the customer network.
Threat source user	User that was logged in to the computer the infection originated from.

Table 24.4: Fields of the Infection Source section on the Malware Detection and PUP Detection pages

Occurrences on other computers 

This section shows all computers on the network where the malware was seen.

Fields	Description
Computer	Computer name.
File path	Name and path of the file that contains the malware.
First seen	Date when the threat was first detected on the relevant computer.

Table 24.5: Fields of the Occurrences on Other Computers section on the Malware Detection and PUP Detection pages

Exploit detection

Accessing the Exploit Details page

- From the top menu, select **Status**. From the side menu, click the **Add** link. A dialog box opens that shows all available lists.
- Select the **Exploit activity** list.
- Set the filters and click the **Launch query** button. A list opens that shows all items classified as exploits.
- From the list, select an item. The **Exploit detection** page opens.

Or:

- From the top menu, select **Status**. From the side panel, select **Security**. A page opens that shows all widgets associated with the security module.
- Click the **Exploit activity** widget.
- Set the filters and click the **Launch query** button. A list opens that shows all items classified as exploits.
- From the list, select an item. The **Exploit detection** page opens.

The details page is divided into several sections:

- Overview.
- Affected computer.
- Exploit impact on the computer.

Overview

Field	Description	Values
Compromised program	Name of the program affected by the vulnerability exploit attempt and hash that identifies it.	• **Path**: Path of the program affected by the exploit. • **Version**: Version of the program affected by the exploit. • **Hash**: Hash of the program affected by the exploit (MD5 and/or SHA-256).
Technique	Identifier of the technique used to exploit the program vulnerability.	Link to a description of the technique used by the exploit.
Action	Shows the action taken by Advanced EPDR on the program affected by the exploit. • **Allowed**: The anti-exploit protection is configured in **Audit** mode. The exploit ran. • **Blocked**: The exploit was blocked before it could run. • **Allowed by the user**: The computer user	Enumeration For more information about how to manage detected threats blocked, see **Allowing blocked items to run** on page **785**.

Field	Description	Values
	was asked for permission to end the compromised process, but decided to let the exploit run. • **Process ended**: The exploit was deleted but managed to partially run. • **Pending restart**: The user was informed of the need to restart their computer to completely remove the exploit. Meanwhile, the exploit continues to run. • **Allowed (Audit mode)**: The user was informed that the malware performed suspicious actions. Because Audit mode is enabled, threats are detected, but they are not blocked or removed. See **Audit mode** on page **359**.	

Table 24.6: Fields of the Overview section on the Exploit Detection page

Affected computer

Field	Description
Computer	Name of the computer where the threat was detected, IP address, and folder in the group tree to which the computer belongs.
Logged-in user	Operating system user under which the threat was loaded and run.
Path of the compromised program	Path of the program affected by the vulnerability exploit attempt.

Table 24.7: Fields of the Affected Computer section on the Exploit Detection page

Exploit impact on the computer

Field	Description
Compromised program	Path and name of the program file associated with the incident. If Advanced EPDR detects that the program is not updated to the latest

Field	Description
	available version, it shows a warning: ⚠**Vulnerable program**.
Activity	• **Has run**: The exploit managed to run before being detected by Advanced EPDR. • **View full activity details**: Click this button to open the **Activity** tab described in **Action tables**. • **View activity graph**: Click this button to view the **Activity** graph described in **Execution graphs**.
Detection date	Date when Advanced EPDR detected the exploit on the customer network.
Possible source of the exploit	Name and path of the program from which the exploit possibly originated.

Table 24.8: Fields of the Exploit Impact on the Computer section on the Exploit Detection page

Vulnerable driver

Accessing the Driver Details page

To access the Driver Details page, follow the steps described in **Exploit detection**. From the **Exploit activity** list, select an item whose exploit technique is vulnerable driver.

The details page is divided into several sections:

- Overview.
- Affected computer.
- Vulnerable driver.

Overview

Field	Description	Values
Vulnerable driver	Name of the driver that was prevented from loading.	• Name of the compromised program. • **Path**: Path of the driver the security software prevented from

Field	Description	Values
		loading. • **MD5**: MD5 hash of the driver. • **SHA-256**: SHA-256 hash of the driver.
Technique	Identifier of the technique used to exploit the program vulnerability.	Vulnerable driver
Action	Action taken by Advanced EPDR on the exploit. • **Blocked**: The exploit was blocked before it could run. • **Allowed by the user**: The computer user was asked for permission to end the compromised process, but decided to let the exploit run. • **Allowed (Audit mode)**: The user was informed that the malware performed suspicious actions. Because Audit mode is enabled, threats are detected, but they are not blocked or removed. See **Audit mode** on page **359**.	Enumeration For more information about how to manage detected threats blocked, see **Allowing blocked items to run** on page **785**.

Table 24.9: Fields of the Overview section on the Driver Details page

Affected computer

Field	Description
Computer	Name of the computer where the threat was detected, IP address, and folder in the group tree to which the computer belongs.
Logged-in user	Operating system user under which the threat was loaded and run.
Driver path	Path of the driver the security software prevented from loading.

Table 24.10: Fields of the Affected Computer section on the Driver Details page

Vulnerable driver

Field	Description
Name	Name of the driver the security software prevented from loading.
Activity	• **Has run**: The exploit managed to run before being detected by Advanced EPDR. • **View full activity details**: Click this button to open the **Activity** tab described in **Action tables**. • **View activity graph**: Click this button to view the **Activity** graph described in **Execution graphs**.
Detection date	Date when Advanced EPDR detected the exploit on the customer network.
MD5	MD5 hash of the blocked driver.
SHA-256	SHA-256 hash of the blocked driver.

Table 24.11: Fields of the Vulnerable Driver section

Block by advanced security policy

Accessing the Block by Advanced Security Policy page

- From the top menu, select **Status**. From the side menu, click the **Add** link. A dialog box opens that shows all available lists.
- Select the **Blocks by advanced security policies** list.
- Set the filters and click the **Launch query** button. A list opens that shows all items blocked by advanced security policies.
- From the list, select an item. The **Block by advanced security policy** page opens.

Or:

- From the top menu, select **Status**. From the side panel, select **Security**. A page opens that shows all widgets associated with the security module.
- Click the **Detections by advanced security policies** widget.

- Set the filters and click the **Launch query** button. A list opens that shows all items blocked by advanced security policies.
- From the list, select an item. The **Block by advanced security policy** page opens.

The details page is divided into several sections:

- Overview.
- Computer.
- Blocked program.

Overview

Field	Description
Blocked program	Name of the blocked program.
Policy applied	Name of the advanced security policy that blocked the program. See **Advanced security policies** on page **336**.
Action	• **Blocked**: The process was blocked before it ran. • **Detected**: The process was detected but not blocked because the security policy is configured in Audit mode. • **Allowed (Audit mode)**: The user was informed that the process performed suspicious actions. Because Audit mode is enabled, threats are detected, but they are not blocked or removed. See **Audit mode** on page **359**.

Table 24.12: Fields of the Overview section on the Block by Advanced Security Policy page

Computer 

Field	Description
Computer	Name of the computer where the threat was detected, IP address, and folder in the group tree to which the computer belongs. When you click the computer name, the computer details page opens. See **Computer details** on page **252**
Logged-in user	Operating system user under which the threat was loaded and run.

Table 24.13: Fields of the Computer section on the Block by Advanced Security Policy page

Blocked program 

Field	Description
Name	Name of the blocked program.
MD5	MD5 hash of the blocked file.
SHA-256	If included in the detection, SHA-256 hash of the blocked program.
Path	Folder where the blocked program is located on the user computer.
Activity	• **View full activity details**: Click this button to open the **Activity** tab described in **Action tables**. • **View activity graph**: Click this button to view the **Activity** graph described in **Execution graphs**.
Detection date	Date when Advanced EPDR blocked the program from running.

Table 24.14: Fields of the Blocked Program section on the Block by Advanced Security Policy page

Block of unknown programs in the process of classification and history of blocked programs

Accessing the Blocked Program Details page

- From the top menu, select **Status**. From the side menu, click the **Add** link. A dialog box opens that shows all available lists.
- Select the **Currently blocked programs being classified** list.
- Set the filters and click the **Launch query** button. A list opens that shows all unknown items in the process of classification.
- From the list, select an item. The **Blocked program details** page opens.
- To open the history of unknown programs blocked, click the **View history of blocked items** link.

Or:

- From the top menu, select **Status**. From the side panel, select **Security**. A page opens that shows all widgets associated with the security module.
- Click the **Currently blocked programs being classified** widget.
- Set the filters and click the **Launch query** button. A list opens that shows all unknown items in the process of classification.
- From the list, select an item. The **Blocked program details** page opens.

The details page is divided into several sections:

- Overview.
- Computer.
- Program activity on the computer.
- Source.

Overview

Field	Description
Program	Name of the blocked program. Point the mouse to the icon to view the MD5 hash and/or SHA-256 hash of the blocked program.
Action	• Blocked • Reclassified as goodware • Reclassified as malware • Reclassified as PUP • Deleted from list
Likelihood of being malicious	Appears only if the item has not yet been classified. • Low • Medium • High • Very high
Classification technique	• **Classified by WatchGuard lab technicians**: The item was classified manually by Cytomic technicians. • **Classified automatically by WatchGuard Collective Intelligence**: The item was classified by Cytomic automatic machine learning

Field	Description
	processes.
Reclassification completed	Date the item was classified.
Reclassification time	Time it took Advanced EPDR to classify the item. When you point the mouse to the icon, the **Reclassification start** field appears. See **Reclassification time calculation for unknown files** on page **802**
Status	Status of the classification process and source of the error if the investigation process could not be completed.
Unblock	Allows the program to run before it is classified. For more information about how to manage detected threats blocked, see **Allowing blocked items to run** on page **785**.

Table 24.15: Fields of the Overview section on the Blocked Program Details page

Computer

Field	Description
Computer	Name of the computer where the threat was detected, IP address, and folder in the group tree to which the computer belongs.
Logged-in user	Operating system user under which the threat was loaded and run.
Protection mode	Advanced protection operating mode when the file was blocked (Audit, Hardening, Lock).
Detection path	Path of the blocked program on the workstation or server.

Table 24.16: Fields of the Computer section on the Blocked Program Details page

Program activity on the computer

Field	Description
Program	Name of the blocked program.
Activity	Summary of the most important actions taken by the malware: • **Has run** • **Has accessed data files** • **Has exchanged data with other computers** • **View full activity details**: Click this button to open the **Activity** tab described in **Action tables**. • **View activity graph**: Click this button to view the **Activity** graph described in **Execution graphs**.
Detection date	Date when Advanced EPDR blocked the program from running.
Dwell time	Time during which the threat was on the customer network without being classified.

Table 24.17: Fields of the Program Activity on the Computer section on the Blocked Program Details page

Source

Field	Description
Source computer	If the file came from another computer on the customer network, this field shows the computer name.
Source IP address	If the file came from another computer on the customer network, this field shows the computer IP address.
Source user	The user who was logged in on the computer the file came from.

Table 24.18: Fields of the Source section on the Blocked Program Details page

Action tables

Advanced EPDR shows 15 days of telemetry associated with each detection made by advanced protection. This telemetry shows the actions taken by the programs involved in an attack.

To view the action table for a threat, access its details page (see **Details of blocked programs**) and select the **Activity** tab.

The action table only shows the most relevant events triggered by a threat.

Because the number of actions and events triggered by a process is very high, showing all of them would hinder the extraction of useful information to perform a forensic analysis.

The table content is initially sorted by date, making it easier to follow the progress of the threat.

This table shows the fields included in action tables:

Field	Comment	Values
Date	Action date.	Date
Times	Number of times the action was executed. A single action executed several times consecutively appears only once in the list.	Numeric value
Action	Action logged on the system and command-line parameters associated with it.	• Downloaded from • Communicates with • Accesses data • Accesses • Is accessed by • LSASS.EXE opens • LSASS.EXE is opened by • Is run by • Runs • Is created by

Field	Comment	Values
		• Creates • Is modified by • Modifies • Is loaded by • Loads • Is deleted by • Deletes • Is renamed by • Renames • Is killed by • Kills process • Process suspended • Creates remote thread • Thread injected by • Is opened by • Opens • Creates key pointing to EXE file • Modifies key to point to EXE file • Tries to stop • Ended by
Path/URL/Registry Key/IP:Port	• Action entity. It has different values depending on the action type. • **Registry Key**: For actions that involve modifying the Windows registry. • **IP:Port**: For actions that involve communicating with a local or remote computer. • **Path**: For actions that involve	

Field	Comment	Values
	accessing the computer hard disk. For more information, see **Path format**. • **URL**: For actions that involve accessing a URL.	
File Hash/Registry Value/Protocol-Direction/Description	This field complements the entity. • **File Hash**: For all actions that involve accessing a file. If the SHA-256 hash appears, it is separated from the MD5 hash by the "|" character. Example: d131dd02c5e6eec4 | 4d70210e28716ccaa7cd4ddb79 • **Registry Value**: For all actions that involve accessing the Windows registry. • **Protocol-Direction**: For all actions that involve communicating with a local or remote computer. Possible values are: • TCP • UDP • Bidirectional • Unknown • Description	
Trusted	The file is digitally signed.	Binary value

Table 24.19: Fields shown in the action table for a threat

Path format

We use numbers and the "|" character to indicate the storage drive and system folders respectively:

Code	Storage drive type
0	Unknown drive.
1	Invalid path. For example, a drive that does not have a mounted volume.
2	Removable drive. For example, a floppy disk, a USB memory device, or a card reader.
3	Internal drive. For example, a hard disk or an SSD disk.
4	Remote drive. For example, a network drive.
5	CD-ROM/DVD drive.
6	RAM disk drive.

Table 24.20: Codes used to indicate the drive type

This is an example of a path:

```
3|TEMP|\app\a_470.exe
```

- **3**: Internal drive. The file is located on the computer hard disk.
- **|TEMP|**: The file is located in the computer \windows\temp\ system folder.
- **\app**: Name of the folder where the file is located.
- **a_470.exe**: File name.

Subject and predicate in actions

To correctly understand the format used to present the information in the action list, a parallel needs to be drawn with natural language:

- All actions have as the subject the file classified as a threat. This subject is not specified in each line of the action table because it is common throughout the table.
- All actions have a verb which relates the subject (the classified threat) to an object, called entity. The entity appears in the **Path/URL/Registry Key/IP:Port** field of the table.
- The entity is complemented with a second field which adds information to the action: **File Hash/Registry Value/Protocol-Direction/Description**.

Table 24.21: illustrates two actions carried out by the same hypothetical malware:

Date	Times	Action	Path/URL/Registry Key/IP:Port	File Hash/Registry Value/Protocol-Direction/Description	Trus-ted
3/30/2015 4:38:40 PM	1	Communicates with	54.69.32.99/80	TCP-Bidirectional	NO
3/30/2015 4:38:45 PM	1	Loads	PROGRAM_ FILES | \ MOVIES TOOLBAR\SAFETYN	9994BF035813FE8EB6 BC98E CCBD5B0E1	NO

Table 24.21: Action list of a sample threat

The first action indicates that the malware (subject) connected to (**Communicates with** action) the IP address `54.69.32.99:80` (entity) through the TCP-bidirectional protocol.

The second action indicates that the malware (subject) loaded (**Loads** action) the library `PROGRAM_ FILES|\MOVIES TOOLBAR\SAFETYNUT\SAFETYCRT.DLL` with hash `9994BF035813FE8EB6BC98ECCBD5B0E1`.

As with natural language, two types of sentences are implemented in Advanced EPDR:

- **Active**: These are predicative actions (with a subject and predicate) connected by an active verb. In these actions, the verb connects the subject, which is always the process classified as a threat, to a direct object, the entity, which can vary based on the type of action. Examples of active actions are:
  - Communicates with
  - Loads
  - Creates
- **Passive**: These are actions where the subject (the process classified as a threat) becomes the passive subject (which receives, rather than executes, the action), and the verb is passive (to be + participle). In this case, the passive verb connects the passive subject (which receives the action) to the entity, which performs the action. Examples of passive actions are:
  - Is created by
  - Downloaded from

Table 24.22: shows an example of a passive action for a hypothetical malware:

Date	Time-s	Actio-n	Path/URL/Registry Key/IP:Port	File Hash/Registry Value/Protocol-Direction/Descriptio n	Trus-ted
3/30/2015 4:51:46 PM	1	Is run by	`WINDOWS|\explorer.exe`	`7522F548A84ABAD8FA516D E5AB3931EF`	NO

Table 24.22: Example of a passive action

In this action, the malware (passive subject) **is run by** (passive action) the `WINDOWS|\explorer.exe` program (entity) with hash `7522F548A84ABAD8FA516DE5AB3931EF`.

> *Active actions enable you to inspect, in detail, the steps taken by a threat. By contrast, passive actions usually reflect the infection vector used by the malware (which process ran it, which process copied it to the user computer, etc.).*

Execution graphs

Advanced EPDR shows a graph with the telemetry collected in the last 15 days for each detection made by the advanced protection. This graph provides a graphical representation of the actions taken by the programs involved in an attack.

To view the execution graph for a threat, access its details page (see **Details of blocked programs**). Select the **Activity** tab. Click the **View activity graph** button.

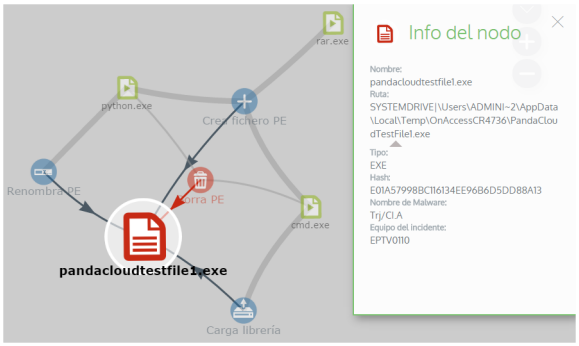


Figure 24.1: Graph representing a threat activities

- Select the **Malware and PUP activity** list to open the **Malware detection** page.
- Select the **Exploit activity** list to open the **Exploit detection** page.

- Select the **Currently blocked programs being classified** list to open the **Blocked program details** page.
- Select the **Blocks by advanced security policies** list to open the **Block by advanced security policy** page.

Select the **Activity** tab. Click **View activity graph** to view a threat execution graph.

Execution graphs offer a graphical representation of the information shown in the action tables, emphasizing the time aspect. They provide an at-a-glance idea of the actions triggered by a threat.

Diagrams

Execution graphs represent the actions taken by threats with two items:

- **Nodes**: They mostly represent actions or information items.
- **Arrows**: They connect the action and information nodes to establish a timeline, and assign each node the role of "subject" or "predicate".

Nodes

Nodes show information through their associated icon, color, and description panel on the right of the page when you select them.

The color code used is as follows:

- **Red**: Untrusted item, malware, threat.
- **Orange**: Unknown/unclassified item.
- **Green**: Trusted item, goodware.

Table 24.23: shows action-type nodes along with a brief description:

Symbol	Description	Symbol	Description
	File downloaded. Compressed file created.		Executable file deleted.
	Socket/communication used.		Library loaded.
	Monitoring initiated.		Service installed.

Symbol	Description	Symbol	Description
	Process created.		Executable file renamed.
	Executable file created. Library created. Registry key created.		Process stopped or closed.
	Executable file modified. Registry key modified.		Thread created remotely.
	Executable file mapped for write access.		Compressed file opened.

Table 24.23: Graphical representation of malware actions in an execution graph

Table 24.24: shows description-type nodes along with a brief description:

Symbol	Description
	File name and extension. • **Green**: Goodware. • **Orange**: Unclassified item. • **Red**: Malware/PUP.
	Internal computer (it is on the corporate network). • **Green**: Trusted. • **Orange**: Unknown. • **Red**: Untrusted.
	External computers. • **Green**: Trusted. • **Orange**: Unknown.

Symbol	Description
	• **Red**: Untrusted.
	Country associated with the IP address of an external computer.
	File and extension.
	Registry key.

Table 24.24: Graphical representation of description-type nodes in an execution graph

Arrows

The arrows of the graphs connect the different nodes and help establish the order in which the actions performed by a threat were executed.

The two attributes of an arrow are:

- **Thickness**: The thickness of the arrow represents the number of times the same type of action was executed between two nodes. The greater the number of actions, the thicker the arrow.
- **Direction**: The direction of the arrow indicates the direction of the action.

Timeline

The timeline helps control the display of the string of events carried out by a threat over time. The controls at the bottom of the timeline enable you to position the view at the precise moment when the threat carried out an action and retrieve extended information that can help you complete a forensic analysis.

To select a specific interval on the timeline, drag the gray interval selectors to the left or right.

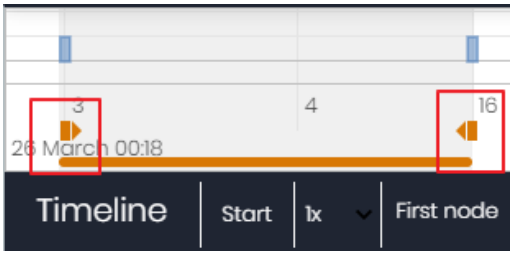


Figure 24.2: Time selectors

After selecting a timeframe, the graph shows the events and nodes that occurred within the interval. Other events and nodes are blurred.

The actions carried out by a threat are represented on the timeline as vertical bars accompanied by a timestamp, which indicates the hour and minute when they occurred.

To view the string of actions taken by a threat, use the following controls:

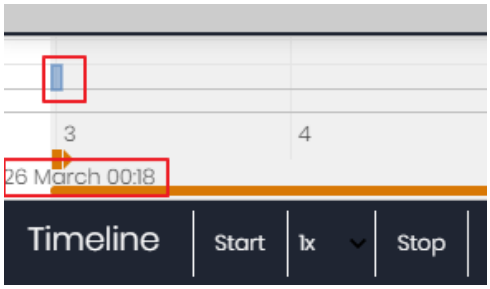


Figure 24.3: Timestamp, date, and actions carried out by the threat

- **Start**: Starts the timeline at a constant speed of 1x. The graphs and lines representing the actions appear while display as the timeline progresses.
- **1x**: Sets the speed of the timeline.
- **Stop**: Stops the progress of the timeline.
- **+** and **-**: Zooms in and zooms out of the timeline.
- **<** and **>**: Select the previous or subsequent node.
- **Initial zoom**: Restores the initial zoom level if you zoomed in or out with the + and – buttons.
- **Select all nodes**: Moves the time selectors to cover the whole timeline.
- **First node**: Sets the time interval to the start of the timeline.

To see the full path of the timeline, select "First node". Then, click "Start". To set the travel speed, click 1x and select a speed option.

Filters

The controls for filtering the information shown on an execution graph are at the top of the graph.

- **Action:** Use the drop-down menu to select an action type from all those executed by the threat. The graph shows only the nodes that match the action type selected and the adjacent nodes associated with this action.
- **Entity**: Use the drop- down menu to choose an entity (the content of the `Path/URL/Registry Key/IP:Port` field).

Node movement and general zoom

To move a graph in the four directions (up, down, left, right) and zoom in or zoom out, you can use the controls in the upper-right corner of the graph.

> *To zoom in and zoom out more easily, you can use the mouse wheel.*

- Click the symbol to leave the graph view.
- To hide the timeline button zone in order to leave more space on the page for a graph, click the icon located in the lower-right corner of the graph.
- Finally, you can configure the behavior of a graph through the panel shown when you click the button in the upper-left corner of the graph.

Exported Excel files

Advanced EPDR enables you to export the contextual telemetry associated with a process at the time an attack is detected by one of the security software advanced technologies. This telemetry is exported to an Excel file. For more information about this file, see section **Details of blocked programs** . To download it, click the icon in the upper-right corner of the **Blocks by advanced security policies** list page. Select the **Export list and details** option to download an Excel file with extended details of all threats on the list.

Field	Description	Values
Date	Action date.	Date
MD5	MD5 hash of the blocked file.	Character string
SHA-256	SHA-256 hash of the blocked file.	Character string
Policy	Name of the policy that blocked the file. Available in the **Detections by advanced**	Character string

Field	Description	Values
	security policies list.	
Threat	Threat name. Available in these lists: • Malware activity • PUP activity • Currently blocked programs being classified • History of blocked programs	Character string
User	User account under which the threat was run.	Character string
Computer	Name of the computer where the threat was detected.	Character string
Path	Threat name, device, and folder where the file is located on the user computer.	Character string
Accessed data	The threat accessed files located on the user computer. Available in these lists: • Malware activity • PUP activity • Currently blocked programs being classified • History of blocked programs	Binary value
Action	Action logged on the system.	• Downloaded from • Communicates with • Accesses data • Accesses • Is accessed by • LSASS.EXE opens

Field	Description	Values
		• LSASS.EXE is opened by • Is run by • Runs • Is created by • Creates • Is modified by • Modifies • Is loaded by • Loads • Is deleted by • Deletes • Is renamed by • Renames • Is killed by • Kills process • Process suspended • Creates remote thread • Thread injected by • Is opened by • Opens • Creates • Is created by • Creates key pointing to EXE file • Modifies key to point to EXE file • Tries to stop • Ended by
Command Line	Command-line parameters associated with the action.	Character string

Field	Description	Values
Event date	Date and time when the event was logged on the customer computer.	Character string
Times	Number of times the action was executed. A single action executed several times consecutively appears only once in the list.	Numeric value
Path/URL/Registry Key/IP:Port	Action entity. It can have different values depending on the action type.	• **Registry Key**: For actions that involve modifying the Windows registry. • **IP:Port**: For actions that involve communicating with a local or remote computer. • **Path**: For actions that involve accessing the computer hard disk. • **URL**: For actions that involve accessing a URL.

File Hash/Registry Value/Protocol-Direction/Description	This field complements the entity.	• **File Hash**: For actions that involve accessing a file.
		• **Registry Value**: For actions that involve accessing the Windows registry.
		• **Protocol-Direction**: For actions that involve communicating with a local or remote computer. Possible values are:
		  • TCP
		  • UDP
		  • Bidirectional

Field	Description	Values
		• Unknown • Description
Trusted	Indicates whether the blocked file is digitally signed.	Binary value

Table 24.25: Fields in the Detections by Advanced Security Policies_Details exported file

Interpreting the action tables and execution graphs

Action tables and execution graphs show 15 days of telemetry associated with each detection made by advanced protection. This telemetry shows the actions taken by the programs involved in an attack. A certain degree of technical knowledge is necessary to be able to extract activity patterns and key information in each situation.

The following section provides some basic guidelines to interpret the action tables with some real-life examples of threats.

The names of the threats indicated herein might vary across security vendors. We recommend that you use a hash to identify malware.

Example 1: Trj/OCJ.A malware activity

The **Details** tab provides key information about the malware found. In this case, the most important data is as follows:

- **Threat**: Trj/OCJ.A
- **Computer**: XP-BARCELONA1
- **Detection path**: `TEMP|\Rar$EXa0.946\appnee.com.patch.exe`

Activity

The **Activity** tab shows a number of actions because Advanced EPDR was configured in Hardening mode and the malware already resided on the computer when Advanced EPDR was installed. The malware was unknown at the time of running.

Hash

Use the hash string to obtain more information on sites such as VirusTotal and get a general idea of the threat and how it works.

Detection path

The path where the malware was detected for the first time on the computer belongs to a temporary directory and contains the 'RAR' string. Therefore, the threat comes from a RAR file temporarily uncompressed into the directory, and which resulted in the `appnee.com.patch.exe` executable.

Activity tab

Step	Date	Action	Path
1	3:17:00	Is created by	`PROGRAM_FILES|\WinRAR\WinRAR.exe`
2	3:17:01	Is run by	`PROGRAM_FILES|\WinRAR\WinRAR.exe`
3	3:17:13	Creates	`TEMP|\bassmod.dll`
4	3:17:34	Creates	`PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK`
5	3:17:40	Modifies	`PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\amtlib.dll`
6	3:17:40	Deletes	`PROGRAM_FILES|\ADOBE\ACROBAT 11.0\ACROBAT\AMTLIB.DLL.BAK`
7	3:17:41	Creates	`PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\ACROBAT.DLL.BAK`
8	3:17:42	Modifies	`PROGRAM_FILES|\Adobe\ACROBAT 11.0\Acrobat\amtlib.dll`
9	3:17:59	Runs	`PROGRAM_FILES|\Google\ Chrome\Application\chrome.exe`

Table 24.26: List of actions performed by Trj/OCJ.A

Steps 1 and 2 indicate that the malware was uncompressed by `WinRAR.exe` and run from that program. The user opened the compressed file and clicked its binary.

After being run, in step 3 the malware created a DLL file (bassmod.dll) in a temporary folder, and another one (step 4) in the installation directory of the Adobe Acrobat 11 program. In step 5, it modified an Adobe DLL file, to take advantage perhaps of a program vulnerability.

After modifying other DLL files, it launched an instance of Google Chrome which is when the timeline finishes. Advanced EPDR classified the program as a threat after that string of suspicious events and stopped its execution.

The timeline shows no actions on the Windows registry, so it is very likely that the malware is not persistent or was not able to modify the Windows registry to make sure it could survive a computer restart.

The Adobe Acrobat 11 software was compromised, so a reinstall is recommended. Thanks to the fact that Advanced EPDR monitors both goodware and malware executables, the execution of a compromised program is detected as soon as it triggers dangerous actions, and is blocked.

Example 2: Communication with external computers by BetterSurf

BetterSurf is a potentially unwanted program that modifies the web browser installed on user computers, injecting ads in the web pages they visit.

The **Details** tab provides key information about the malware found. In this case, it shows this data:

- **Name**: PUP/BetterSurf
- **Computer**: MARTA-CAL
- **Detection path**: `PROGRAM_FILES|\VER0BLOCKANDSURF\N4CD190.EXE`
- **Dwell time**: 11 days 22 hours 9 minutes 46 seconds

Dwell time

In this case, the dwell time is very long: The malware remained dormant on the customer network for almost 12 days. This is increasingly normal behavior and can be due to various reasons. For example, the malware did not carry out any suspicious actions until very late, or the user downloaded the file but did not run it at the time. In any case, the threat was unknown to the security service, so there was no malware signature to compare it to.

Activity tab

Step	Date	Action	Path
1	3/8/2015 11:16	Is created by	`TEMP|\08c3b650-e9e14f.exe`
2	3/18/2015 11:16	Is created by	`SYSTEM|\services.exe`
3	3/18/2015 11:16	Loads	`PROGRAM_ FILES|\VER0BLOF\N4Cd190.dll`
4	3/18/2015 11:16	Loads	`SYSTEM|\BDL.dll`

Step	Date	Action	Path
5	3/18/2015 11:16	Communicates with	127.0.0.1/13879
6	3/18/2015 11:16	Communicates with	37.58.101.205/80
7	3/18/2015 11:17	Communicates with	5.153.39.133/80
8	3/18/2015 11:17	Communicates with	50.97.62.154/80
9	3/18/2015 11:17	Communicates with	50.19.102.217/80

Table 24.27: List of actions performed by PUP/BetterSurf

In this case, you can see how the malware communicated with different IP addresses. The first address (step 5) is the infected computer itself, and the rest are external IP addresses to which it connected through port 80 and from which the advertising content was probably downloaded.

The main preventive measure in this case should be to block those IP addresses in the corporate firewall.

Before adding rules to block IP addresses in the corporate firewall, you should consult those IP addresses in the associated RIR (RIPE, ARIN, APNIC, etc.) to see the networks to which they belong. In many cases, the remote infrastructure used by malware is shared with legitimate services housed in providers such as Amazon and similar, so blocking certain IP addresses would be the same as blocking access to legitimate web pages.

Example 3: Access to the Windows registry by PasswordStealer.BT

PasswordStealer.BT is a Trojan that logs the user activity on the infected computer and sends the information obtained to an external server. Among other things, it captures screens, logs keystrokes, and sends files to a C&C (Command & Control) server.

The **Details** tab provides key information about the malware found. In this case, it shows this data:

Detection path: `APPDATA|\microsoftupdates\micupdate.exe`

The name and location of the executable file indicate that the malware poses as a Microsoft update. This particular malware cannot infect computers by itself; it requires the user to run it

manually.

Activity tab

Advanced EPDR was configured in Hardening mode and the malware already resided on the computer when Advanced EPDR was installed. The malware was unknown at the time of running.

Action table

Step	Date	Action	Path
1	03/31/2015 23:29	Is run by	`PROGRAM_FILESX86|\internet explorer\iexplore.exe`
2	03/31/2015 23:29	Is created by	`INTERNET_CACHE|\Content.IE5\ QGV8PV80\ index[1].php`
3	03/31/2015 23:30	Creates key pointing to EXE file	`\REGISTRY\USER\S-1-5[...]9-5659\Software\Microsoft\Windows\ CurrentVersion\Run?MicUpdate`
4	03/31/2015 23:30	Runs	`SYSTEMX86|\notepad.exe`
5	03/31/2015 23:30	Thread injected by	`SYSTEMX86|\notepad.exe`

Table 24.28: List of actions performed by PasswordStealer.BT

In this case, the malware was generated in step 2 by a web page and run by Internet Explorer.

The sequence of actions has a granularity of one microsecond. For this reason, the actions executed within the same microsecond might not appear in order on the timeline, as in step 1 and step 2.

After being run, the malware became persistent in step 3, adding a branch to the Windows registry to run every time the computer started up. It then started to execute typical malware actions such as opening the `notepad` and injecting code in one of its threads.

As a remediation action in this case and in the absence of a known disinfection method, you can minimize the impact of the malware by deleting the malicious Windows registry entry. However, it is quite possible that the malware might prevent you from modifying that entry on infected computers; in that case, you would have to either start the computer in safe mode or with a bootable CD to delete the entry.

Example 4: Access to confidential data by Trj/Chgt.F

Trj/Chgt.F was uncovered by WikiLeaks at the end of 2014 as a tool used by government agencies in some countries for selective espionage.

In this example, we go directly to the **Activity** tab to show you the behavior of this advanced threat.

Action table

Step	Date	Action	Path
1	4/21/2015 2:17:47	Is run by	SYSTEMDRIVE|\Python27\pythonw.exe
2	4/21/2015 2:18:01	Accesses data	#.XLS
3	4/21/2015 2:18:01	Accesses data	#.DOC
4	4/21/2015 2:18:03	Creates	TEMP|\doc.scr
5	4/21/2015 2:18:06	Runs	TEMP|\doc.scr
6	4/21/2015 2:18:37	Runs	PROGRAM_FILES|\Microsoft Office\Office12\WINWORD.EXE
7	4/21/2015 8:58:02	Communicates with	192.168.0.1/2042

Table 24.29: List of actions performed by Trj/Chgt.F

The malware was initially run by the Python interpreter (step 1), and later accessed an Excel file and a Word document (steps 2 and 3). In step 4, a file with an SCR extension was run, probably a screensaver with some type of flaw or error that could be exploited by the malware.

In step 7 the malware established a TCP connection. The IP address is private, so the malware connected to the customer own network.

In a case such as this, it is important to check the content of the files accessed by the threat to assess the loss of information. However, the timeline of this particular attack shows that no information was extracted from the customer network.

Advanced EPDR disinfected the threat and blocked any subsequent execution of the malware on this and other customers systems.

Chapter 25

Alerts

The alert system is a resource provided by Advanced EPDR to quickly notify administrators of situations that might affect the correct operation of the security service.

Namely, an alert is sent to the administrator every time one of these events occurs:

- The security software detects a malware specimen, PUP, or exploit.
- The security software detects a network attack.
- The security software detects indicators of attack.
- The security software detects network attack activity.
- There is an attempt to use an unauthorized external device.
- The security software reclassifies an unknown item (malware or PUP).
- Advanced EPDR detects and blocks an unknown process during classification.
- There is a license status change.
- There are installation errors or a computer is unprotected.

Chapter contents

Email alerts

Email alerts are messages generated and sent by Advanced EPDR to the configured recipients (typically the network administrator) when certain events occur.

Accessing the alert settings

From the top menu, select **Settings**. From the side menu, select **My alerts**. The **Email alerts** page opens, where you can configure the email alert settings.

Alert settings

The alert settings page is divided into three sections:

- **Send alerts in the following cases**: Select which events will trigger an alert. For more information, see **Alert types** .
- **Send the alerts to the following address**: Enter the email addresses of the alert recipients.
- **Send the alerts in the following language**: Choose the alert message language from those supported in the console:
    - German
    - Spanish
    - French
    - English
    - Italian
    - Japanese
    - Hungarian
    - Portuguese
    - Swedish

Alert export

If the console user has Total Control permissions, they can export the **My alerts** settings for all account users that have specified alert recipient email addresses. See **Alert settings**.

To export the settings, click the  icon in the upper-right corner of the **Email alerts** page.

Fields displayed in the exported file

Field	Description	Values
Customer	Customer account.	Character string
User	Advanced EPDR console user who configured **My alerts**.	Character string
Login email	Email address with which the user logs in to the Advanced EPDR console.	Character string
Blocked	Indicates whether the user can access the Advanced EPDR console. See **Removing or blocking user accounts**	• Yes • No

Field	Description	Values
	on page 65.	
Active cases to send	Indicates whether the user has configured alerts to send in the **My alerts** settings. See **Alert settings**.	• Yes • No
Destination address	Alert recipient email addresses specified by the user.	Character string

Table 25.1: Fields in the Alerts Destinations exported file

Access permissions and alerts

You define alerts for each web console user. The content of an alert email varies with the managed computers that are visible to the recipient.

Alert types

Type	Frequency	Condition	Information shown
Malware detections (real-time protection only)	The solution sends a maximum of two messages for each computer each day.	• Sends an alert for each malware detected in real time on a computer • Windows computers only.	• First or second message. • Name of the malicious program. • Computer name. • Group. • Date and time (UTC). • Path of the malicious program. • Hash. • Table with contextual telemetry associated with the attacking process at the time it is detected. • List of computers where the malware was previously seen.
Exploit detections	The solution sends a	• Sends an alert for each exploit	• Name, path, and hash of the program hit by the

Type	Frequency	Condition	Information shown
	maximum of 10 alerts for each computer-exploit each day.	attempt detected. • Windows computers only.	exploit attempt. • Computer name. • Group. • Date and time (UTC). • Action taken. • Computer risk level. • Assessment of the targeted program security level. • Table with contextual telemetry associated with the attacking process at the time it is detected. • Possible source of the exploit.
PUP detections	The solution sends a maximum of two alerts for each computer-PUP each day.	• Sends an alert for each PUP detected in real time on a computer. • Windows computers only.	• First or second message. • Name of the malicious program. • Computer name. • Group. • Date and time (UTC). • Path of the malicious program. • Hash. • Table with contextual telemetry associated with the attacking process at the time it is detected. • List of computers where the malware was previously seen.
Network attack detections	Every hour.	• Sends an alert for each type of	• Computer. • Group.

Type	Frequency	Condition	Information shown
		network attack and each source IP address. • Windows computers only.	• Network attack. • Local IP address. • Remote IP address. • Local port. • Remote port. • Number of occurrences.
Blocked program in the process of classification	The solution sends an alert for each unknown program detected in real time on the file system.	Windows computers only.	• Name of the unknown program. • Computer name. • Group. • Date and time (UTC). • Path of the unknown program. • Hash. • Table with contextual telemetry associated with the attacking process at the time it is detected. • List of computers where the unknown program was previously seen.

Programs blocked or detected by advanced security policies	• If the action is Block, the solution sends a single email message for each computer each day.
	• If the action is not Block, the solution sends the first 50
		Windows computers only.	• Detection details:
			  • Name of the applied policy.
			  • Computer name
			  • Group
			  • Logged-in user
			  • File name.
			  • File MD5 hash.
			  • Program name and path.
			  • Date and time (UTC).

Type	Frequency	Condition	Information shown

	messages generated for all computers each day.		• Lifecycle of the detected item:
			  • Date and time (UTC).
			  • Action.
			  • Path/URL/Registry/Key
			  • File/MD5/Registry Value
			  • Trusted
			• Occurrences on other computers:
			  • Computer name
			  • Date the item was first seen.
			  • Program name and path.

Programs blocked by the administrator	The solution sends an alert every time a program is blocked.	Windows computers only.	• Program name • Hash • Program path • Computer name • Group to which the computer belongs • User who launched the program • Date when the program was blocked
Classification of a file allowed by the administrator	Administrator-allowed files are files which the administrator allowed to run although Advanced EPDR blocked them. As soon as the solution completes the classification, it informs the administrator of the verdict so that the file can be allowed or blocked, based on the reclassification policy. For more information about reclassification policies, see **Reclassification policy** on page **812**.		
Indicators of attack (IOA)	The solution sends an alert	For each computer on the	• Affected computer • IP address

Type	Frequency	Condition	Information shown
	when it detects an indicator of attack.	network that has an Indicators of Attack (IOA) settings profile assigned to it.	• Group • Customer • Type of indicator of attack • Risk • Action
Malware URL blocked	The solution sends a message every 15 minutes with a summary of all detected threats.	• Sends an alert when a URL that points to malware is detected.	• Number of malware URLs detected within the time range. • Number of affected computers.
Phishing detections	The solution sends a message every 15 minutes with a summary of all detected threats.	• Sends an alert when a phishing attack is detected.	• Number of phishing attacks detected within the time range. • Number of affected computers.
Intrusion attempts blocked	The solution sends a message every 15 minutes with a summary of all detected threats.	• Sends an alert when the IDS module blocks an intrusion attempt. • Windows computers only.	• Number of intrusion attempts blocked within the time range. • Number of affected computers.
Blocked devices	The solution sends a message every 15 minutes with a summary of all detected threats.	• Sends an alert when a user tries to access a device or peripheral that the administrator blocked.	• Number of device access attempts blocked. • Number of affected computers.

Type	Frequency	Condition	Information shown
		• Compatible with Windows, Linux, macOS, and Android devices.	
Computers with protection errors	The solution sends an alert every time an error is found.	• Sends an alert when the solution finds an unprotected computer on the network. • Sends an alert when the solution finds a computer with a protection or installation error.	• Computer name. • Group. • Description. • Operating system. • IP address. • Active Directory path. • Domain. • Date and time (UTC). • **Failure reason**: Protection with errors or installation error.
Computers without a license	The solution sends an alert every time an error is found.	Sends an alert when the solution fails to assign a license to a computer when there is no free license.	• Computer name. • Description. • Operating system • IP address • Group • Active Directory path • Domain. • Date and time (UTC). • Failure reason: Computer without a license.
Install errors	The solution sends an alert every time an error is found.	• Sends an alert when an event occurs that causes computer status	• Computer name. • Protection status. • Reason for the status change.

Type	Frequency	Condition	Information shown
		to change **(1)** from protected to unprotected. • If the solution detects several events at the same time that could cause a computer status to change from protected to unprotected, it only generates one alert with a summary of all the events	
Unmanaged computers discovered	The solution sends an alert every time an error is found.	• Sends an alert when a discovery computer finishes a discovery task. • Sends an alert when a discovery task finds a never-seen-before computer on the network.	• Name of the discovery computer. • Number of discovered computers. • Link to the list of unmanaged computers discovered.

Table 25.2: Alert table

Status change alerts (1)

These computer statuses trigger an alert:

- **Protection with errors**: The status of the antivirus or advanced protection installed on a computer shows an error. This only applies to computers with an operating system that

supports antivirus or advanced protection.

- **Installation error**: An installation error occurs that requires user intervention, such as insufficient disk space. Transient errors that can be resolved autonomously after a number of retries do not generate alerts.
- **No license**: A computer does not receive a license after registration because there are no free licenses

These computer statuses do not trigger an alert:

- **No license**: The administrator manually removes a computer license, or Advanced EPDR automatically removes a computer license because the number of purchased licenses has been reduced.
- **Installing**: It does not make sense to generate an alert every time the protection is installed on a computer on the network.
- **Protection disabled**: This status is the consequence of a voluntary change of settings.
- **Protection out-of-date**: This status does not necessarily mean the computer is unprotected, despite its protection is out of date.
- **Pending restart:** This status does not necessarily mean the computer is unprotected.
- **Knowledge out-of-date**: This status does not necessarily mean the computer is unprotected.

Opting out of email alerts

If an email recipient wants to opt out of the notifications, but does not have access to the Advanced EPDR console or appropriate permissions, the recipient can unsubscribe from the email message. To opt out of email alerts:

- At the bottom of the email alert, click the link **If you don't want to receive any more messages of this kind, click here.** In the window that opens, type the email address that you do not want to receive email alerts. The link is valid for 15 days after the alert is sent.
- If the email address you enter currently receives email alerts, a confirmation email is sent to the address.
- In the confirmation email, click the opt-out link to confirm that you want no longer want to receive emails at the specified email address. The link is valid for 24 hours after the alert is sent.

Chapter 26

Scheduled sending of reports and lists

Advanced EPDR sends, by email, all the security information from the computers it protects. This makes it easy to share information across departments in a company and keep a history of all the events that occurred on the platform, beyond the capacity limits of the web console. This feature enables you to closely monitor the security status of the network without having to access the web console, thus saving management time.

With automated email reports, stakeholders can stay up to speed on all generated security events, thanks to a tamper-proof system that enables them to accurately assess the security status of the network.

Chapter contents

Report features

Report period

There are two types of reports based on the time period covered by the report:

- **Consolidated reports**: These include, in a single document, all the information generated over a given period of time.

- **Instant reports**: These reflect the security status of the network at a specific moment in time.

Method of sending

Advanced EPDR enables you to send reports automatically based on the settings established in the task scheduler or manually on demand.

The automated sending of reports provides recipients with network activity information without having to go to the web console.

Format

Depending on the type of report, Advanced EPDR can deliver reports in PDF and/or CSV format.

Content

The content of reports can be configured depending on the type of report: include data from any number of Advanced EPDR modules or set filters to restrict the information displayed to computers that meet certain criteria.

Report types

Advanced EPDR enables you to generate three types of reports, each with its own features:

- List views
- Executive reports
- Lists of devices

Next is a summary of the features of each type of report:

Type	Period	Sent	Contents	Format
List views	Instant	Automatically	Configurable using searches	CSV
Executive reports	Consolidated	Automatically and on demand	Configurable by categories and groups	PDF, CSV, Excel, Word
Lists of devices	Instant	Automatically	Configurable using filters	CSV

Table 26.1: Summary of report types and their features

Requirements for generating reports

Users with the read-only role can preview executive reports but cannot schedule the sending of new reports.

Next is a description of the tasks you must perform in order to use the feature for sending scheduled reports.

List views

First, create a view and configure the search tools so the list shows the information you consider relevant. After that, you can create the scheduled report task. See **Creating a custom list** on page **55** for more information about how to create list views with associated searches.

Executive reports

No prior tasks are required: The content of the report is determined at the time of configuring the schedule report task.

List of filtered devices

You must first create a filter or use one of the filters created in Advanced EPDR. See **Filter tree** on page **214** for more information about how to configure and use filters.

Accessing the sending of reports and lists

From the Scheduled reports section

To access the list of tasks for sending reports and lists, click **Status** in the top menu, then **Scheduled reports** from the side menu. A page opens with the tools required to search for previously created send tasks, edit them, delete them, or create new ones.

From a list view

List views are stored in the left panel of the **Status** page. You can schedule the sending of each of them following the steps below.

- **From the context menu**: Click the context menu of the list view. Click the option **Schedule report** . A window opens with the information required, which is explained in section **Report and list settings**.
- **From the list view**: Click the icon in the upper-right corner of the page. A window opens with the information required, which is explained in section **Report and list settings**.

After the scheduled report task has been created, a pop-up message appears in the upper-right corner of the page confirming the creation of the task.

From a filter

- Click the **Computers** menu at the top of the console. Click the tab to show the filter tree.
- When clicking a filter, the list of devices is refreshed to show the devices whose characteristics meet the conditions of the selected filter.
- Click the context menu icon ⋮ corresponding to the filter and click **Schedule report**. A window opens with the information required, which is explained in section **Report and list settings**.

After the scheduled report task has been created, a pop-up message appears in the upper-right or bottom-right corner of the page confirming the creation of the task. This message also includes a link to the list of scheduled report tasks. See **Report and list settings**.

Managing reports

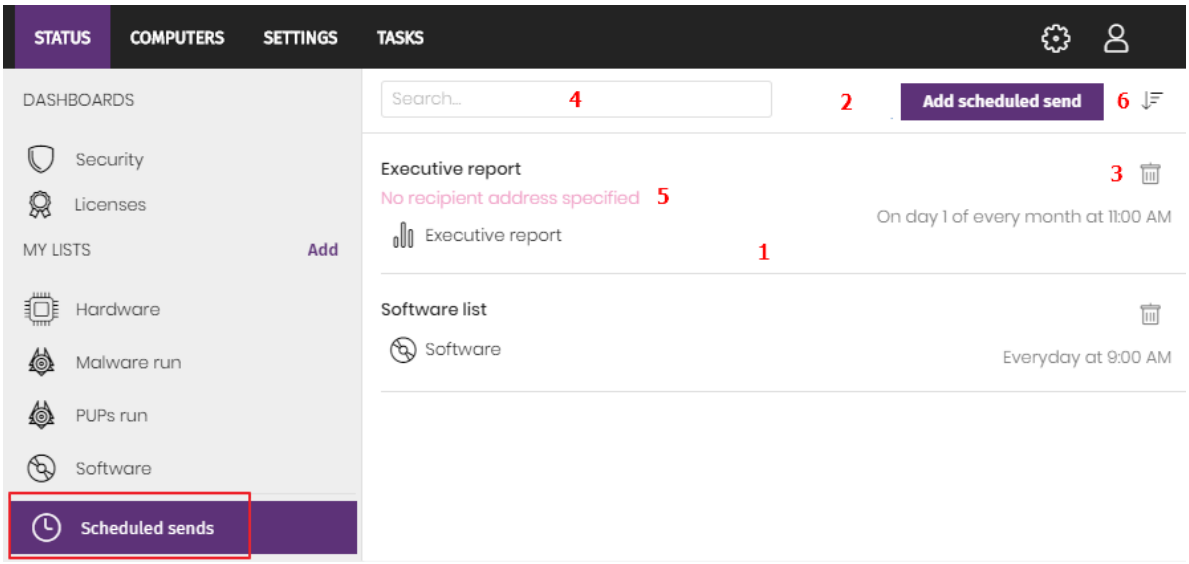


Figure 26.1: Page for managing scheduled sending of reports

To create, delete, edit, and list scheduled reports, click the **Status** menu at the top of the console. Then, click **Scheduled reports** from the side menu.

List of scheduled reports

The panel on the right shows the list of previously created scheduled report tasks.

All tasks include a name and below it a series of messages that indicate whether data is missing from the settings of the scheduled report task.

Creating scheduled reports

Click the **Add scheduled report** button **2** to show the settings window.

See **Report and list settings** for more information about the data administrators must provide to configure a scheduled report task.

Sorting scheduled reports

Click the icon **(6)** to expand a context menu with the sort options:

- Sort by creation date
- Sort by name
- Ascending
- Descending

Deleting and editing scheduled reports

To delete or edit a scheduled report task, follow the steps below:

- To delete a scheduled report task, use the icon **3**).
- To edit a scheduled report, click its name.

> *A list view or filtered list with a scheduled report task configured cannot be deleted until the corresponding task has been deleted.*
> *The lists sent by a scheduled report correspond to a specific list view or filtered list. If these are edited, the scheduled report will be updated accordingly.*

Report and list settings

Field	Description
Name	Name of the entry shown in the list of scheduled reports.
Send automatically	Frequency with which the report or list is sent: • **Every day**: It is sent every day at the scheduled time. • **Every week**: It is sent every week on the scheduled day and at the scheduled time • **Every month**: It is sent every month at the scheduled time on the scheduled date.
Report type	Type of report you want to send:

Field	Description
	• Executive report • List • Filter The report content varies depending on the type of report. For more information, see **Contents of reports and lists**.
Preview report	This option appears only when you select Executive Report. This link opens a new tab in your browser and enables you to see the contents of the report before you schedule it to be sent, download it, or print it. For lists and filters, the format is CSV and the preview option is not available.
Dates	Time period covered by the report. • Last month • Last 7 days • Last 24 hours In the case of lists and filters, the report is generated immediately. The information shown reflects the security status in the moment the report is generated. For more information, see **Report features**.
Computers	The computers from which data is extracted to generate the executive report: • **All computers**. • **Selected groups**: From the group tree, select individual groups using the checkboxes. This field appears only for executive reports.
To	Target email addresses separated by commas.
CC	Target email addresses (carbon copy recipients) separated by commas.
CCO	Target email addresses (blind copy recipients) separated by commas.
Subject	Summary description of the email message.

Field	Description
Format	• **For list views**: A CSV file is attached to the email message. • **For executive reports**: The report is attached to the email message in PDF, Excel, or Word format.
Language	Language of the report.
Content	Type of information included in the report: • **Table of contents**: List of the sections in the report. • **License status**: Information about the licenses contracted and used as well as their expiration dates. See **Licenses** on page **189**. • **Security status**: The status of the Advanced EPDR software on the network computers on which it is installed. • **Detections**: The threats detected on the network. • **Risks:** The security risk levels assigned to computers on the network. See **Risk assessment module panels/widgets** on page **739** • **Indicators of attack**: Information about the detected indicators of attack (IOA). See **Indicators of Attack module panels/widgets** on page **646**. • **Web access**: User Internet activities. For more information, see **Security module panels/widgets** on page **661**. • **Patch management**: The patch status of computers on your network. See **Cytomic Patch widgets/panels** on page **458**. • **Vulnerability assessment status**: Shows computers on the network with known software vulnerabilities and reports on the availability of patches to mitigate vulnerability impact on computers. This appears only if the customer does not have Cytomic Patch. For more information, see **Vulnerability assessment module panels/widgets** on page **750**. • **Data Control**: Information about the Cytomic Data Watch deployment status and computers on the network with most PII files found. See **Cytomic Data Watch panels/widgets** on page **396**. • **Encryption**: The encryption status of the computers on the network. See **Cytomic Encryption module panels/widgets** on page **556**. • **Endpoint Access Enforcement**: Inbound connections detected and blocked on the computers on the corporate network. For more information, see **Endpoint Access Enforcement panels/widgets** on

Field	Description
	page 526. See **Contents of reports and lists**.

Table 26.2: Information to generate on-demand reports

Contents of reports and lists

Lists

The content of the lists sent is similar to the content generated by the **Export** or **Detailed export** button of a list view. If the list view supports detailed exports, when you configure the send task two options appear:

- **Summary report**: Corresponds to the **Export** option in the list.
- **Full report**: Corresponds to the **Detailed export** option in the list.

The lists that support detailed exports are:

- Software
- Malware and PUPs
- Exploits
- Currently blocked programs being classified
- Blocks by advanced security policies
- Patch installation history

For more information about the types of lists available in Advanced EPDR and their content, see **Managing lists** on page **48**.

Lists include the computers visible to the user account that last edited the scheduled report. For this reason, a list edited by an account with less visibility than the account that initially created it contains information about a smaller number of computers than those shown when it was first created.

Lists of devices

The content of the report sent corresponds to the basic exported list of devices filtered by certain criteria. For more information about the content of the CSV file sent, see **Computers** on page **229**.

For more information about how to manage and configure filters, see **Filter tree** on page **214**.

Executive report

Depending on the settings defined in the **Contents** field, the executive report can include this data:

Overview

- **Created on**: Date when the report was created.
- **Period**: Time period covered by the report.
- **Included information**: Computers included in the report.

Table of contents

This section shows a list with links to the various sections of the executive report.

License status

- **Contracted licenses**: Number of licenses contracted by the customer.
- **Used licenses**: Number of licenses assigned to the network computers.
- **Expiration date**: Date when the license contract expires.

See **Licenses** on page **189**.

Security status

Operation of the protection module on the network computers on which it is installed.

- **Protection status**: See **Protection status** on page **662**.
- **Online computers**: See **Offline computers** on page **665**.
- **Up-to-date protection**: See **Outdated protection** on page **666**.
- **Up-to-date knowledge**: See **Outdated protection** on page **666**.

Detections

The threats detected on the network.

- **Classification of all programs run and scanned**: See **Classification of all programs run and scanned** on page **671**.
- **Top 10 computers with most detections**: The top 10 computers with most detections by the antivirus module during the specified period:
    - **Computer**: Name of the computer.
    - **Group**: Group to which the computer belongs.
    - **Detections**: Number of detections during the specified period.

    - **First detection**: Date of first detection.
    - **Last detection**: Date of last detection.
- **Malware activity**: See **Malware/PUP activity** on page **667**.
- **PUP activity**: See **Malware/PUP activity** on page **667**.
- **Exploit activity**: See **Exploit activity** on page **669**.
- **Network attack activity**: See **Network attack activity** on page **670**.
- **Latest malware detections**: See **Malware and PUP detection** on page **820**.
- **Latest PUP detections**: See **Malware and PUP detection** on page **820**.
- **Latest exploit detections**: See **Exploit detection** on page **823**.
- **Latest network attack detections**: See **Network attack activity** on page **721**.
- **Threats detected by the antivirus**: See **Threats detected by the antivirus** on page **675**.

Risks

Overall status of the security risks assigned to computers. See **Risk assessment module panels/widgets** on page **739**.

- **Company risk**: Number of computers on the network with an assigned risk level.
- **Risks trend**: Number and types of risks that are detected over time.
- **Detected risks**: The most commonly found risks and the number of computers where the risk was found.
- **Top 10 computers at risk**: Computers with the highest risk level.

Indicators of attack

Details of IOAs detected.

- **Threat hunting service**: See **Threat Hunting Service** on page **647**.
- **Detections trend**: See **Detections trend** on page **648**.
- **Top 10 indicators of attack (IOA) detected**: See **Indicators of attack (IOA)** on page **624**.
- **Top 10 indicators of attack (IOA) by computer**: See **Indicators of attack (IOA)** on page **624**.

Web access

Web activity of network users.

- **Web access**: See **Web access** on page **678**.
- **Top 10 most accessed categories**: See **Top 10 most accessed categories** on page **678**.
- **Top 10 most accessed categories by computer**: See **Top 10 most accessed categories by computer** on page **679**.

- **Top 10 most blocked categories**: See **Top 10 most blocked categories** on page **680**.
- **Top 10 most blocked categories by computer**: See **Top 10 most blocked categories by computer** on page **681**.

Patch management

Patch status of computers on your network.

- **Patch management status**: See **Patch management status** on page **459**.
- **Top 10 computers with most available patches**: List of the ten computers that are missing most patches, grouped by type: security patches, non-security patches, and Service Packs. See **Computers with most available patches** on page **472**.
- **Top 10 most critical patches**: List of the ten most critical patches sorted by the number of computers affected.
- **Available patches trend**: Shows the trend of the number of patches that are pending installation on the computers on the network, grouped by severity. See **Available patches trend** on page **464**.

Vulnerability assessment

- **Vulnerability assessment status**: Shows the status of the vulnerability assessment module on computers on your network: computers where vulnerability assessment did not install correctly, computers with no vulnerability assessment license, and other issues. See **Vulnerability assessment status** on page **751**.

  Time since last check: Shows the number of computers that have not connected to the Cytomic cloud and reported patch status for more than 3, 7, and 30 days. See **Time since last check** on page **753**.
- **Top 10 most critical patches**: List of the ten most critical patches sorted by the number of computers affected.
- **Top 10 programs with most available patches**: List of the ten programs with most missing patches available for installation.
- **Available patches trend**: Shows the trend of the number of patches that are pending installation on the computers on the network, grouped by severity. See **Available patches trend** on page **758**.

Cytomic Data Watch

Status of the Cytomic Data Watch deployment and list of computers with most Personally Identifiable Information (PII) files found on the network.

- **Deployment status**: See **Deployment status** on page **397**.
- **Files by personal data type**: See **Files by personal data type** on page **407**.

- **Computers with personal data**: See **Computers with personal data** on page **406**.
- **Top 10 computers with most personal data files**: See **Computers with personal data** on page **406**.

Encryption

Encryption status of computers. It includes these widgets and lists:

- **Encryption status**: See **Encryption status** on page **556**.
- **Computers supporting encryption**: See **Computers supporting encryption** on page **558**.
- **Encrypted computers**: See **Encrypted computers** on page **559**.
- **Authentication method applied**: See **Authentication method applied** on page **561**.
- **Last encrypted computers**: Lists the ten computers that have been encrypted most recently by Cytomic Encryption, sorted by encryption date. Each line in the list contains the computer name, group, operating system, authentication method, and encryption date.

Endpoint Access Enforcement

Connections detected and blocked on the computers on the corporate network. It includes these widgets and lists:

- **Connections by condition**: Shows the trend of connections by the reason why they were categorized as dangerous. For more information, see **Connections by condition** on page **528**.
- **Connections by monitored protocol**: Shows the connections made over monitored protocols over time. For more information, see **Connections by monitored protocol** on page **530**.
- **Top 10 computers reporting high-risk outbound connections**: Shows the IP addresses or names of the ten computers responsible for the highest number of high-risk connections to computers on the network. For more information, see **Top 5 computers reporting high-risk outbound connections** on page **526**
- **Top 10 computers reporting high-risk inbound connections**: Shows the names of the ten network computers that receive the highest number of high-risk inbound connections from managed computers. For more information, see **Top 5 computers reporting high-risk inbound connections** on page **527**

Chapter 27

Remediation tools

Advanced EPDR provides several remediation tools that help you resolve the issues found in the Protection, Detection, and Monitoring phases of the adaptive protection cycle. Some of these tools are automatic and do not require you to take any action. You can get access to other tools in the web console.

Chapter contents

Table **Table 27.1:** shows the tools available for each supported platform and their features.

Remediation tool	Platform	Type	Purpose
Automatic computer scanning and disinfection	Windows, macOS, Linux, Android	Automatic	Detects and disinfects malware when the solution detects movement in the file system (copy, move, run) or in a supported infection vector.
On-demand computer scanning and	Windows, macOS, Linux,	Automatic (scheduled)/Manual	Detects and disinfects malware in the file system when required, at specific

Remediation tool	Platform	Type	Purpose
disinfection	Android		time intervals, or after you create a remediation task.
On-demand restart	Windows	Manual	Forces a computer restart to apply updates, finish manual disinfection tasks, and fix protection errors.
Computer isolation	Windows, macOS, and Linux	Manual	Isolates a computer from the network, to prevent the exfiltration of confidential information and the spread of threats to other computers.
Remote computer control	Windows, macOS, and Linux	Manual	Enables you to remotely connect to computers on your network from the web console to check their status or start troubleshooting tasks.
Ransomware removal and system restore	Windows, macOS, and Linux	Manual	Enables you to detect ransomware attacks and remove threats. On Windows systems, you can recover a clean copy of the encrypted files.

Table 27.1: Advanced EPDR remediation tools

Automatic computer scanning and disinfection

The Advanced EPDR protection module automatically detects and disinfects threats in these security areas:

> *Automatic disinfection does not require administrator intervention. However,* ***File protection*** *must be enabled in the security settings assigned to the computers and devices. See* ***Security settings for workstations and servers*** *on page* ***327*** *for more information about blocking modes and the options available for the Advanced EPDR antivirus module.*

- **Advanced protection**: Blocks the execution of unknown malware.
- **Web**: Malware downloaded to targeted computers through a web browser.
- **Email**: Malware that reaches email clients as a message attachment.
- **File system**: Malware detected when a file that contains a known or unknown threat in the computer storage system is run, moved, or copied.
- **Network**: Intrusion attempts from a host on the network or Internet, blocked by the firewall.

When Advanced EPDR detects a known threat, it automatically cleans the affected items when there is a disinfection method available. If not, the solution quarantines the items.

Behavior based on the protection settings

When the antivirus and advanced protection modules are enabled, Advanced EPDR takes these actions:

Advanced protection mode	Antivirus protection	Behavior
Audit	Enabled	Detection, disinfection, and quarantine.
Hardening, Lock	Enabled	Detection, block unknown items, disinfection, and quarantine.
Audit	Disabled	Detection.
Hardening, Lock	Disabled	Detection, block unknown items.

Table 27.2: Product behavior based on the advanced protection and antivirus protection engine settings

On-demand computer scanning and disinfection

To scan and disinfect user computers on demand, Advanced EPDR uses the task infrastructure.

Required permissions

The user account used to access the web console must have the **Launch scans and disinfect** permission assigned to its role. For more information about the permissions system, see **Managing roles and permissions** on page **69**.

Types of on-demand scans

Immediate (Scan now option)

A task that starts immediately and which scans and disinfects the local file system (it does not scan network drives).

Advanced EPDR creates a task with these characteristics:

- **Maximum run time**: Unlimited.
- **Task start**:
    - If the target computer is turned on, the task starts as soon as it is launched.
    - If the target computer is turned off, the task is postponed until the computer becomes available within the next 7 days.
- The computer areas that are scanned are as follows:
    - **The entire computer:**
        - Memory.
        - Boot system.
        - Cookies.
        - Internal storage devices. Complete file system, all extensions.
        - Storage devices physically connected to the target computer (USB drives and others). Complete file system, all extensions.
    - **Critical areas**:
        - Memory.
        - Boot system.
        - Cookies.
        - %windir%\system32, %windir%\SysWow64. All extensions.
- The default action that is taken is:
    - **When detecting a disinfectable file**: The file is replaced with a clean version.
    - **When detecting a non-disinfectable file**: The file is deleted and a backup copy is moved to quarantine.

Scheduled (Scheduled scan option)

Create a task without settings. For more information about how to configure a scan task, see **Configuring a scan task**.

Accessing on-demand scan and disinfection tasks

From the computer tree

- Select **Computers** in the top menu. Select the **My organization** tab of the computer tree in the left panel.
- To launch an immediate scan on a group of computers, select the context menu of the group. Select **Scan now**. The **Select the type of scan** window opens.
- Select the scan type: **The entire computer** or **Critical areas (Recommended)**. Click **OK**. The **New scan task created** message appears and the task is added to the list in the **Tasks** section.
- To schedule a scan on a group of computers, click the context menu of the group. Select **Schedule scan**. A new scan task is created. For information about how to configure it, see **Configuring a scan task**.

From the computer tree list

- Select **Computers** in the top menu. Select the **My organization** tab of the computer tree in the left panel.
- Select the group of computers. Select the checkboxes of the computers you want to scan.
- To launch an immediate scan task, if you have selected a single computer, select the computer context menu. Select **Scan now.** If you have selected more than one, select **Scan now** in the toolbar above. The **Select the type of scan** window opens.
- To schedule a scan task, if you have selected a single computer, select the computer context menu. Select **Schedule scan**. If you have selected more than one, select **Schedule scan** in the toolbar above. A new scan task is created. For information about how to configure it, see **Configuring a scan task**.

Configuring a scan task

- Enter general details about the task in the **Name** and **Description** fields.
- If no recipients are defined, click the **No recipients selected** link in the **Recipients** section. A page opens where you can select the computers that will receive the configured task.

> *To access the computer selection page, you must first save the task. If you have not saved the task, a warning message is shown.*

- Select the types of computers that will receive the task: **Workstation**, **Laptop**, or **Server**.
- Click ⊕ to add individual computers or computer groups. Click 🗑 to remove them.
- Click the **View computers** button to view the computers that will receive the task.
- Schedule the task. You can configure these three parameters:

- **Starts:** Indicate the task start date/time.

Value	Description
As soon as possible (selected)	The task is launched immediately provided the computer is available (turned on and accessible from the cloud), or as soon as it becomes available within the time interval specified **if the computer is turned off**.
As soon as possible (cleared)	The task is launched on the date selected in the calendar. Specify whether the time on the computer or the Advanced EPDR server time should be considered.
If the computer is turned off	If the computer is turned off or cannot be accessed, the task will not run. The task scheduler enables you to establish the task expiration time, from 0 (the task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available). • **Do not run:** The task is immediately canceled if the computer is not available at the scheduled time. • **Run the task as soon as possible, within:** Define a time interval during which the task will be run if the computer becomes available. • **Run when the computer is turned on:** There is no time limit. The solution waits indefinitely for the computer to be available to launch the task.

Table 27.3: Task launch parameters

- **Maximum run time**: Indicates the maximum time that the task can take to complete. After that time, the task is canceled returning an error.

- **Scan options:**

Value	Description

Scan type	• **The entire computer**: Runs an in-depth scan of the computer that includes all connected storage devices.
	• **Critical areas**: Runs a quick scan of these areas:
	  • `%WinDir%\system32`
	  • `%WinDir%\SysWow64`

Value	Description
	• Memory • Boot system • Cookies • **Specific items**: Specify the paths you want to scan on the mass storage devices. This option supports environment variables. The solution scans the specified path and every folder and file it contains.
Detect viruses	Detects programs that enter computers with malicious purposes. This option is always enabled.
Detect hacking tools and PUPs	Enable this toggle to detect potentially unwanted programs, as well as programs that hackers can use to carry out actions that cause problems for the user of the affected computer.
Detect suspicious files	Scheduled scans can scan computer software statically without the need to run the software. This reduces the likelihood that the scan detects some types of threats. Enable this toggle to use heuristic scan algorithms and improve detection rates. Only programs detected by the heuristic protection are considered suspicious programs.
Scan compressed files	Enable this toggle to decompress compressed files and scan their contents.

Value	Description
Exclude the following files from scans	• **Do not scan files excluded from the permanent protections**: Select this checkbox to not scan files that the administrator allowed to execute, as well as any file that is globally excluded in the console. • **Extensions**: Specify the extensions of the files you do not want to scan. Enter multiple file extensions separated by commas. • **Files**: Specify the names of the files you do not want to scan. Enter multiple file names separated by commas. • **Directories**: Specify the names of the folders you do not want to scan. Enter multiple folders separated by commas.

Table 27.4: Scan options

Lists generated by scan tasks

Scan tasks generate lists with results.

Accessing the lists

Follow these steps to access these lists:

- Go to the **Tasks** menu at the top of the console. Click **View results** in the scan task whose results you want to view. The **Task results** list opens.
- From the **Task results** list, click **View detections** to access the list of detected items.

Required permissions

Permissions	Access to lists
No permissions	**Scan task results** list.
View detections and threats	Access to the **View detections** list of a task.

Table 27.5: Permissions required to access scan task lists

Scan task results list

This list shows the malware items detected on the computers on your network:

Field	Description	Value
Computer	Name of the computer where the task ran.	Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Detections	Number of detections made on the computer.	Character string
Status	Status of the task.	• All statuses • Pending • In progress • Finished • Failed • Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Start date	Task start date.	Date
End date	Task end date.	Date

Table 27.6: Fields in the Scan task results list

Filter tools

Field	Comment	Value
Status	Status of the task.	• All statuses • Pending • In progress • Finished • Failed

Field	Comment	Value
		• Canceled (the task could not start at the scheduled time) • Canceled • Canceling • Canceled (maximum run time exceeded)
Detections	Computers where detections were or were not made.	• All • With detections • No detections

Table 27.7: Filters available in the Scan task results list

View detections list

This list shows detailed information about each malware detection made by the scan task.

Field	Description	Value
Computer	Computer name.	Character string
Group	Folder in the Advanced EPDR folder tree that the computer belongs to.	Character string
Threat type	Malware category based on the actions the threat is designed to perform.	• Virus and ransomware • Spyware • Tracking cookies • Hacking tools and PUPs • Phishing • Dangerous actions blocked • Malware URLs • Other

Field	Description	Value
Path	Threat location on the computer.	Character string
Action	Action taken on the computer.	• Quarantined • Deleted • Disinfected • Blocked • Process ended
Date	Date the action was taken.	Date

Table 27.8: Fields in the View detections list

Threat details page

Click any of the rows in the list to view the threat details page. See **Computer details** on page **252** for more information.

Computer restart

If you need to restart a Windows computer to finish an update or to fix a protection problem, you can force the computer to restart:

- Go to the **Computers** menu at the top of the console. From the right panel, find the computer you want to restart:
  - **To restart a single computer**: Click the computer's context menu icon. Select **Restart** from the menu displayed.
  - **To restart multiple computers**: Use the checkboxes to select the computers you want to restart. Click the icon on the action bar.

> *If the target computer is not available (offline), the restart command remains active for 7 days.*

Computer isolation

With Advanced EPDR, you can isolate computers on demand to prevent the spread of threats and to block the exfiltration of confidential data.

> *This feature is compatible with Windows, macOS, and Linux workstations and servers. It is not supported on Android devices.*

When a computer is isolated, its communications are restricted except for:

- Access to the computer from the console. This enables you to analyze and resolve any detected problems with the tools in Advanced EPDR.
- Access to the computer and remote control through Panda Systems Management. This enables you to collect extended information and resolve any detected problems with the solution remote management tools (remote desktop, remote command line, remote event viewer, etc.).

> *For more information about the remote management tools provided by Cytomic, see the Panda Systems Management Administration Guide available at* ***https://www.pandasecurity.com/rfiles/enterprise/documentation/pcsm/docswebpage/SYSTEMSMANAGEMENT-Guide-EN.pdf****.*

Any other products and services installed on the affected workstation or server cannot communicate over the Internet/local network unless you set the appropriate exceptions. See **Advanced options**.

Computer isolation statuses

The **Isolate computer** and **Stop isolating the computer** operations are performed in real time. However, they could delay if the target computer is offline. To show the exact situation of a computer, Advanced EPDR distinguishes among four different isolation statuses through these icons:

Icon	Description
Isolating 	You launched a request to isolate one or more computers. The request is being processed.
Isolated 	The isolation process has been completed and the computer communications are restricted.
Stopping isolation 	You launched a request to stop isolating one or more computers. The request is being processed.

Icon	Description
Not isolated	The process to stop isolating a computer has been completed. The computer can communicate with other computers based on settings configured in other modules, products, or the operating system.

Table 27.9: Computer isolation statuses

These icons appear next to the **IP address** column in the **Licenses** and **Protection status** lists, and in the **Computers** area.

Isolating one or more computers from the organization network

Follow these steps to isolate one or more computers from the network:

- From the top menu, select **Computers**, or select one of these computer lists:
    - **Protection status** list.
    - **Licenses** list.
- Select the checkboxes for the computers you want to isolate.
- In the action bar, select **Isolate computer**. A dialog box opens and shows the **Advanced options** link.
- In **Advanced options**, type the programs you want to exclude from the isolation process. These programs can communicate normally with other computers in the organization or external computers.
- Click **Isolate**. The computer status changes to **We're trying to isolate this computer**.
- Follow these steps to isolate a computer group:
    - From the top menu, select **Computers**.
    - In the computer tree, select the folder view. Select the group you want to isolate.
    - From the group context menu, select the **Isolate computers** option. Click **Isolate**.
    - To isolate all computers on the network, expand the context menu of the **All** node.

Stopping isolation

- For more information, see section **Isolating one or more computers from the organization network**.
- In the action bar, select **Stop isolating the computer**.
- The computer status changes to **We're trying to stop isolating this computer**.

Advanced options

Allow processes

When you isolate a computer, you deny all communications to and from the computer except those required by the Cytomic product processes. All other processes, including those belonging to user programs, are prevented from communicating with the other computers in the organization.

To exclude specific programs from this behavior:

- Click the **Advanced options** link in the dialog box shown when you isolate a computer.
- In the **Allow the following processes** text box, type the programs you want to exclude from the isolation process.

These programs can communicate normally with other computers in the organization or external computers, unless otherwise indicated in the settings established for other Advanced EPDR modules, in other products installed on the computer, or in the operating system firewall.

If you excluded programs in a previous isolation operation, they display in the text box. You can edit the values in the text box.

Show custom message (Windows computers only)

Type a descriptive message to inform users that their computer has been isolated from the network. The Advanced EPDR agent will show a pop-up window with the content of the message. To not show the custom message to the user, enable the **I prefer not to show any messages this time** toggle. The message is not shown until you disable the toggle.

This feature is only compatible with Windows workstations and servers.

Communications allowed and denied on isolated computers

Advanced EPDR denies all communications to and from isolated computers except those required to perform remote forensic analyses and to use the remediation tools in Advanced EPDR and Panda Systems Management. Next is a list with all communications allowed and denied on isolated computers.

Allowed processes and services

- System processes:
    - All services required for the computer to be part of the corporate network, including DHCP services to obtain IP addresses, ARP, WINS, and DNS host name resolution services, etc.
- Advanced EPDR processes:

  - Services required to communicate with the default gateway.
  - Services required to communicate with the Cytomic cloud to enable the protection engines to work, download signature files, and enable administrators to perform remote management tasks in the web console.
  - Services required by an isolated computer with the discovery computer role to perform discovery tasks.
  - Services required by an isolated computer with the cache role to act as a file server.
  - Services required by a computer with the Cytomic proxy role to act as a connection proxy.
- Services required by the Panda Systems Management agent to enable use of non-intrusive remote tools:
  - Remote access tools.
  - Services required for SNMP monitoring of devices not compatible with Panda Systems Management and with the connection node role assigned.

Blocked communications

All communications that are not listed in the section above are denied. This includes:

- Windows Update policies, macOS operating system updates, and Cytomic Patch updates through Panda Systems Management.

The Cytomic Patch module remains operational on isolated computers.

- Communication with the scripts and modules developed by the administrator or integrated from the Panda Systems Management ComStore.
- Web browsing, FTP, mail, and other Internet protocols.
- SMB file transfer between PCs on the network.
- Remote installation of Advanced EPDR.

Remote computer control

With Advanced EDR, you can remotely connect to the computers on your network from the web console to check their status or start troubleshooting tasks.

Remote access tools included in Advanced EPDR

- **Remote control terminal**: Remote shell that enables you to perform administrator operations on the file system and run programs on the remote computer.
- **Process manager**: Shows a list of running processes and enables you to stop, pause, and resume them.
- **Service manager**: Shows a list of the services installed on the computer and enables you to start and stop them.
- **File transfer**: Enables you to send and receive files between your computer and the user computer.
- **Command-line tools**: Use commands from the remote control terminal to collect information to enhance investigations, recover data for forensic analysis, and remedy security breaches:
  - **delete**: Deletes files from the target computer hard disk.
  - **dump**: Dumps the memory assigned to processes to disk.
  - **netinfo**: Shows information about network interfaces.
  - **pcap**: Captures network packets and dumps them to the computer hard disk.
  - **ports**: Shows processes with open ports on the computer.
  - **process**: Shows the processes loaded in memory and their modules.
  - **url**: Shows a history of all the URLs opened from the computer browser.

Required permissions

- To view and modify the remote control settings, the user account must have the **Configure remote control** permission.
- To remotely access computers on the network, the user account must have the **Remote computer control** permission.

*For more information about available permissions, see **Understanding permissions** on page 72.*

Requirements

The remote control feature is available on Windows, Linux, and macOS computers.

To use the remote access and remote command line tools, the user computer and the network perimeter firewall must allow traffic to and from these URLs and ports:

- **dir.rc.pandasecurity.com through port 443**
- **eu01.rc.pandasecurity.com through ports 8080 and 443.**
- **eu02.rc.pandasecurity.com through ports 8080 and 443.**
- **eu03.rc.pandasecurity.com through ports 8080 and 443.**
- **eu04.rc.pandasecurity.com through ports 8080 and 443.**
- **eu05.rc.pandasecurity.com through ports 8080 and 443.**
- **eu06.rc.pandasecurity.com through ports 8080 and 443.**
- **ams01.rc.pandasecurity.com through ports 8080 and 443.**
- **ams02.rc.pandasecurity.com through ports 8080 and 443.**

Remote control settings

To enable remote control for the Windows computers on the network, you must assign a remote control settings profile to the computers you want to access.

- From the top menu, select **Settings**. From the side menu, select **Remote control**. A page opens and shows the existing remote control settings profiles.
- In the upper-right corner of the page, click **Add**. The **Add settings** page opens.
- In the **Name** text box, type a name for the settings profile. (Optional) In the **Description** text box, type a description of the settings profile.
- Click **Save**.
- Click the **No recipients selected yet** link. Select the computers or computer groups that you want to assign the remote control settings profile to.
- Enable the toggles for the features you want to be available on the Windows computers:
    - **Terminal**: Remote access to the console terminal.
    - **Process monitor**: Remote monitoring of processes.
    - **Service monitor**: Remote configuration of services.
    - **File transfer**: Remote transfer of files to or from your computer.
- In the upper-right corner of the page, click **Save**. The profile is assigned to the target computers and you can establish remote control sessions to them.

Accessing the remote control feature

To start a remote control session from a list, click the context menu of the target computer. Select  **Remote control**. This option is available in these lists:

- Licenses
- Hardware
- Risks by computer
- Computer protection status
- Encryption status
- Patch management status
- Data Control status
- Computer list

*For more information about the lists available in Advanced EPDR, see **Templates, settings, and views** on page **48***

The remote control feature is also available from the computer details page, which you can open by clicking a row in any of the aforementioned lists.

Remote control tool description

Process manager

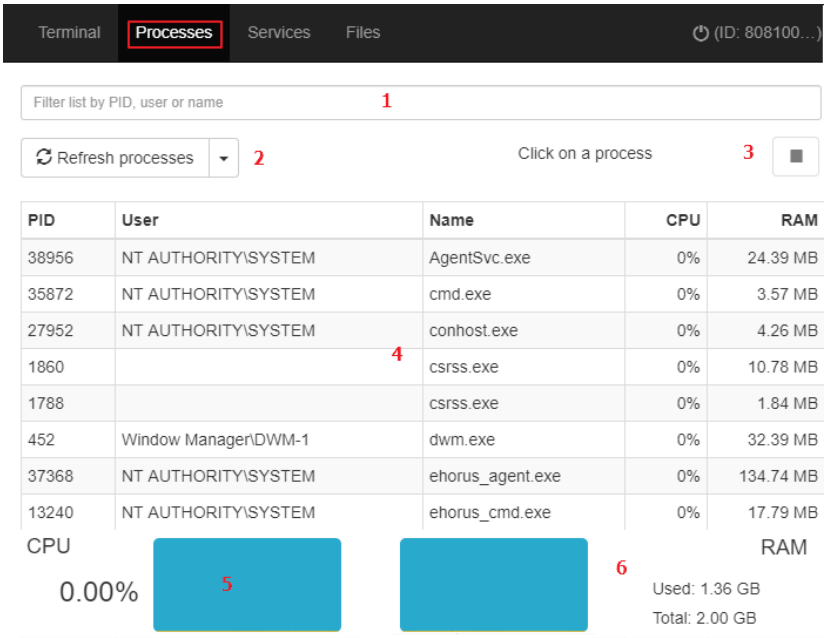


Figure 27.1: Process manager

The **Process manager** shows all processes in the remote computer memory and enables you to search for, stop, and start specific processes remotely. It also provides details on the RAM and CPU used by each process.

It includes these resources:

- **Search tool (1)**: Filters the list by process ID (PID) or name. You can type only a partial string.
- **Auto refresh (2)**: Specify the frequency that Advanced EPDR refreshes the information in the process list.
- **Stop button (3)**: Stops a process.
- **Process list (4)**: Shows the list of processes in the remote computer memory.
- **CPU (5)**: Shows the percentage of CPU used by all the processes in the remote computer memory. Also, it includes a line chart showing a history of CPU usage since the process manager was opened.
- **Memory (6)**: Shows the percentage of RAM used by all the processes in the remote computer memory. Also, it includes a line chart showing a history of RAM usage since the process manager was opened.

The process list **(4)** shows information about each process in the remote computer memory:

Field	Description
PID	Process ID.
User	User account that loaded the process.
Name	Process name.
CPU	CPU used by the process.
RAM	Memory used by the process.

Table 27.10: Fields in the Processes list

Service manager

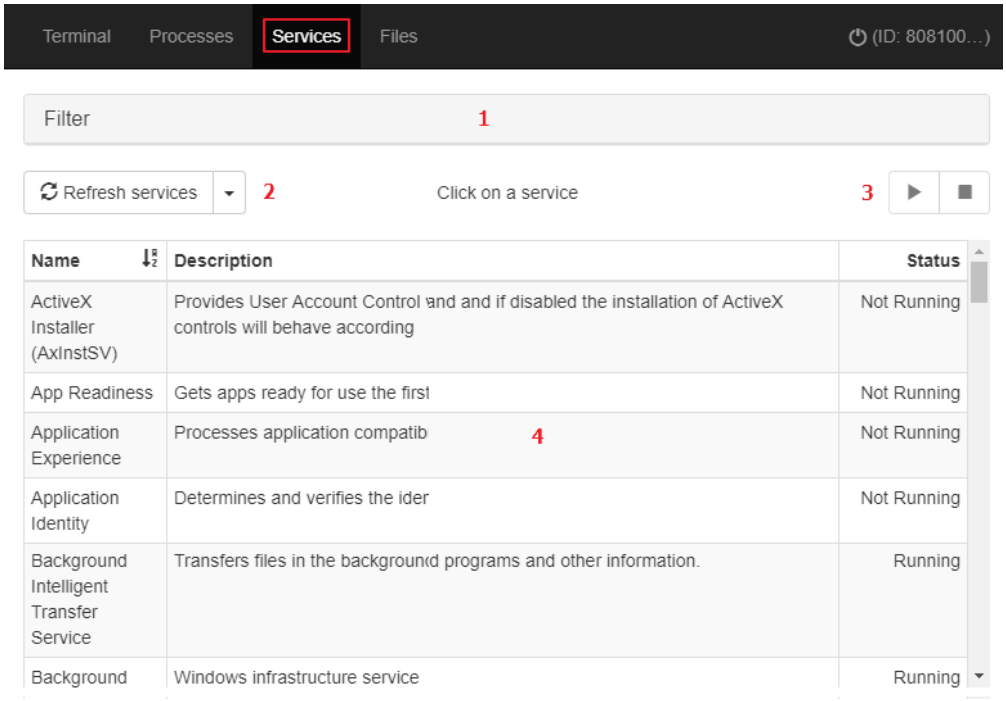


Figure 27.2: Service manager

The **Service manager** shows all services configured on the remote computer and enables you to find specific services to change their status. It includes these resources:

- **Search tool (1)**: Filters the list by service name or description. You can type only a partial string.
- **Auto refresh (2)**: Specify the frequency that Advanced EPDR refreshes the information in the service list.
- **Service start and stop buttons (3)**: Stops or starts the selected service.
- **Service list (4)**: Shows the list of services in the remote computer memory.

The service list **(4)** shows information about each service configured on the computer:

Field	Description
Name	Service name.
Description	Service description.
Status	Service status: • **Running**: The service is running. • **Not running**: The service is stopped.

Table 27.11: Fields in the Services list

File transfer

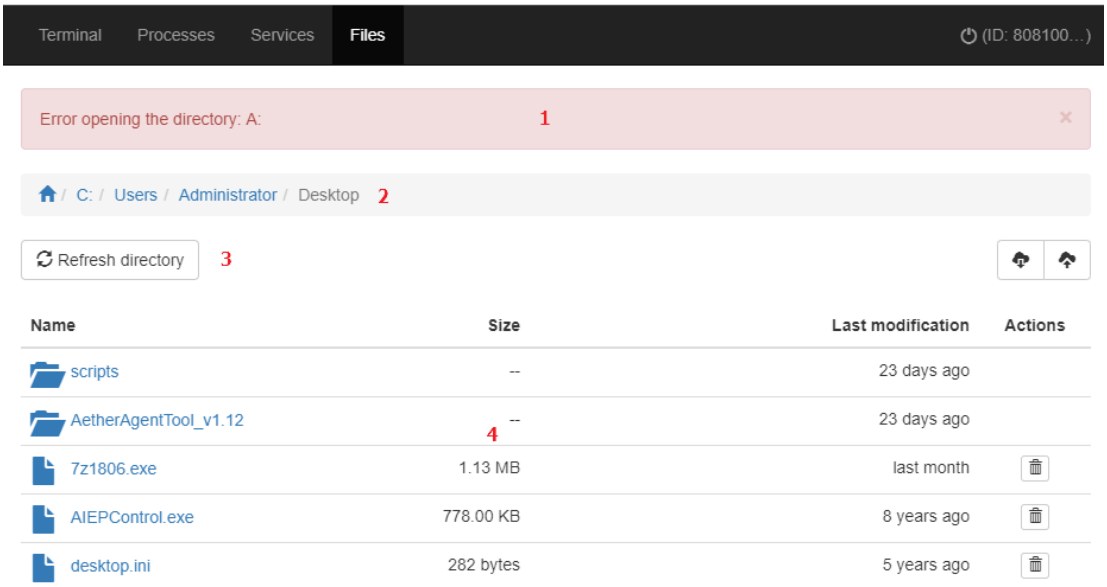


Figure 27.3: File manager

The **File manager** enables you to transfer files to and from your computer to the remote computer. You can also navigate the file system on the remote computer and delete files. It includes these resources:

- **Message bar (1)**: If there are errors when you try to get access to the remote computer file system, a message bar shows.
- **Path (2)**: The file path shows at the top of the window.
    - To change directories, click another drive or folder in the file path or in the **Name** column.
    - To show the list of devices connected to the computer, click the icon.
- **Auto refresh (3)**: Specify the frequency that Advanced EPDR refreshes the information in the file list.
- **File list (4)**: Shows the list of files in the selected path **(2)**.
- **Folders** : Click a folder to view the files it contains. The path **(2)** updates automatically.
- **Delete** : Deletes the file and removes it from the computer.

The file list **(4)** shows information about each file found on the remote computer:

Field	Description
Name	File name.
Size	File size.

Field	Description
Last modified	Date when the file was last modified.
Actions	Actions you can take on the file: • Deletes the file.

Table 27.12: Fields in the Files list

Remote control terminal

Windows

On the Terminal page of the Remote Control tool, you can run commands compatible with the command interpreter on the remote computer. Also, you can launch programs that generate text output. The remote control terminal runs under the LOCAL_SYSTEM account on the remote computer and is installed here:

```
C:\Program Files (x86)\Panda Security\Panda Aether
Agent\Remote access\
```

Linux/macOS

You can open a bash terminal to run compatible commands that generate text output. Commands are run with root permissions on the remote computer.

RT.exe program for Windows computers

Advanced EPDR supports `rt.exe`. This program provides access to a set of tools you can use to respond to security incidents. These tools enable you to recover information to perform a subsequent forensic analysis, and restore devices affected by a security breach to their original state.

You can access the `rt.exe` program from the remote command line. The program has the following syntax:

```
rt.exe [command] [-h|--help]
```

Consider these aspects about the `rt.exe` program:

- Each `command`indicates an action to take and each command supports different parameters.
- Wildcards * and ? are not supported.

- Some parameters allow partial searches that use substrings of characters that represent the start, middle, or end of a string. For example, to search for "malware", you can enter these substrings: "mal" or "ware".
- If a command supports dumping output to a file, this is specified with `-f`.
- To separate multiple items of the same type, enter the pipe character (|).
- Next, we describe the parameters supported by each command.

Delete command

This command deletes the files specified with the parameters `-n`, `-m`, or `-s` which are in the path indicated by the parameter `-p`. If the file is in use, the `delete` command returns an error.

Short form	Full parameter	Description	Notes
-h	**--help**	Opens command help.	
-f	**--force**	Deletes files permanently.	
-r	**--restore**	Restores selected files from the Recycle Bin.	Restores files to their original location.
-p	**--path**	Absolute path from the root directory where you want to search for files to delete. The security product only deletes files in the specified path.	• Use the backslash character (\) to separate folders. • Wildcards are not supported.
-n	**--name**	Names of the files you want to delete.	• To specify multiple files, separate file names with the pipe character (|). • Wildcards are not supported.
-m	**--md5**	MD5 values of the files you want to delete.	• To specify multiple MD5 values, separate values with the pipe character

Short form	Full parameter	Description	Notes
			(|). • Wildcards are not supported.
-s	**--sha256**	SHA256 values of the files you want to delete.	• To specify multiple SHA256 values, separate values with the pipe character (|). • Wildcards are not supported.

Table 27.13: Delete command parameters

Dump command

This command dumps to disk the memory space allocated to a system or user process.

Short form	Full parameter	Description	Notes
-h	**--help**	Opens command help.	
-p	**--pid**	PID of the process to dump.	For information on how to dump the PID of the process, see **Process command**.
-s	**--system**	Kernel dump.	Supported values: • **mini**: Short dump of the stack content. • **kernel**: Full dump. • **full**: Dump of the entire physical memory of the computer, even if it is not in use.
-f	**--filename**	Name of the file	

Short form	Full parameter	Description	Notes
		that contains the dump.	
-z	**--zip**	Stores the dump in a ZIP file.	

Table 27.14: Dump command parameters

Netinfo command

Used with the `-a` parameter, this command shows the settings of the network interfaces installed on the computer.

Short form	Full parameter	Description	Notes
-h	**--help**	Opens command help.	
-a	**--all**	Shows the settings of the network interfaces installed on the computer.	
-f	**--filename**	Name of the file that contains the data.	
-z	**--zip**	Stores the information in a ZIP file.	

Table 27.15: Netinfo command parameters

Pcap command

This command captures the network traffic sent and received by the remote computer. Specify the start and end of the capture with the parameters - `a start| stop`. Packet capture generates temporary files on the computer so there must be sufficient hard disk space. The end result is a PCAP file that can be used directly by the Wireshark/Ethereal program.

Short form	Full parameter	Description	Notes
-h	**--help**	Opens command help.	
-a	**--action**	Executes an action: • **start**: Starts the capture process.	

Short form	Full parameter	Description	Notes
		• **stop**: Stops the capture process. • **queryStatus**: Shows the status of the capture process.	
-m	**--maxsize**	Maximum size of the packet to capture.	• In megabytes (MB). • Default value: 200 MB.
-i	**--maxtime**	Maximum capture time.	• In seconds. • Default value: 86400 seconds (1 day).
-f	**--filename**	Name of the file that contains the data.	
-z	**--zip**	Stores the information in a ZIP file.	

Table 27.16: Pcap command parameters

Ports command

Used with the `-a` parameter, this command shows the sockets open on the computer and the processes that opened them,

Short form	Full parameter	Description	Notes
-h	**--help**	Opens command help.	
-a	**--all**	Shows all open ports and their associated processes.	
-p	**--pid**	Filters the results by process PID.	
-n	**--name**	Filters the results by process name.	You can type only a partial string.

Short form	Full parameter	Description	Notes
-f	**--filename**	Name of the file that contains the data.	

Table 27.17: Ports command parameters

Process command

Used with the `-a` parameter, this command shows all processes loaded in the memory of the computer and their modules.

Short form	Full parameter	Description	Notes
-h	**--help**	Opens command help.	
-a	**--all**	Shows all processes loaded in the memory of the computer and their modules.	
-p	**--pid**	Filters the results by process PID, showing the process modules.	
-u	**--user**	Shows the processes launched by a user and their modules.	
-f	**--filename**	Name of the file that contains the data.	

Table 27.18: Process command parameters

Url command

Used with the `-a any` parameter, this command shows all the URLs accessed by users through the remote computer's web browser. This command requires that the Advanced EDR web access control feature be enabled.

Short form	Full parameter	Description	Notes
-h	**--help**	Opens command help.	
-a	**--action**	Filters the URL list by the action taken by the web access control feature:	

Short form	Full parameter	Description	Notes
		• **allow**: Shows allowed URLs. • **deny**: Shows denied URLs. • **any**: Shows all visited URLs.	
-c	**--count**	Maximum number of URLs to show.	Default value: unlimited.
-g	**--category**	Filters the URL list by the category assigned by the web access control feature.	
-b	**--begindate**	Enables you to specify the start date from when to show visited URLs.	• **Date format**: "`YYYY-MM-DD HH:MM`". • **Default value**: 30 days before the date you run the command.
-e	**--enddate**	Enables you to specify the end date to show visited URLs up to.	• **Date format**: "`YYYY-MM-DD HH:MM`". • **Default value**: Date you run the command.
-n	**--urlpattern**	Filters URLs by substring.	
-u	**--userpattern**	Filters URLs by user.	
-f	**--filename**	Name of the file that contains the data.	
-z	**--zip**	Stores the information in a ZIP file.	

Table 27.19: Url command parameters

Reporting a problem

As with any technology, the Advanced EPDR software installed on your network computers might occasionally function incorrectly. Some symptoms could include:

- Errors reporting a computer status.
- Errors downloading knowledge or engine updates.
- Protection engine errors.

If Advanced EPDR functions incorrectly on a computer on the network, you can contact the Cytomic support department through the console and automatically send all the information required for diagnosis. From the top menu, select **Computers**. Click the context menu for the computer with errors. From the menu that opens, select **Report a problem**.

If Advanced EPDR functions incorrectly on a computer on the network, you can contact the Cytomic support department through the console and automatically send all the information required for diagnosis. From the top menu, select **Computers**. Click the context menu ⋮ for the computer with errors. From the menu that opens, select **Report a problem**.

Allowing external access to the web console

If you find problems you cannot resolve, you can grant the Cytomic support team access to your console. Follow these steps:

- From the top menu, select **Settings**. From the side menu, select **Users.**.
- On the **Users** tab, enable **Allow the Cytomic (Panda Security) team to access my console**.

Removing ransomware and restoring the system to a previous state

Ransomware threats encrypt the content of the files found on workstations and servers, demanding a ransom from the targeted company to get the recovery key that allows access to the encrypted information upon payment. These threats are extremely dangerous because of the impact they can have on business operations. Advanced EPDR implements multiple features to help organizations in both the attack detection and attack remediation phases.

Follow these steps if you detect a ransomware attack on your network:

> *Because the Shadow Copies feature makes a daily backup of computer files and keeps a maximum of seven copies, it is important that you recover a clean copy of the encrypted files within seven days after the attack takes place. Otherwise, all saved copies will be of encrypted files.*

- Use the **Isolate computers** feature to isolate affected computers. Note that isolating a computer could affect the normal operation of the computer. In the case of servers, it may prevent other computers on the network from working correctly. For more information about how to configure this feature, see **Computer isolation**.
- Verify that the protection software is working on all computers:
  - To see the protection status of your computers, see the **Protection status** on page **662** widget.
  - Reinstall the security software on computers where the protection status is **Error**.
  - Find computers without security software installed. For more information about how to configure this feature, see **Viewing discovered computers** on page **125**.
- Configure advanced protection with the following settings (for more information, see **Advanced protection** on page **333**).
  - Operating mode: **Lock**.
  - Enable and set advanced policies to **Block**.
  - Enable and set the Anti-exploit protection to **Block**.
  - Enable **Advanced code injection**.
- Enable and configure the File antivirus, Mail antivirus, and Web browsing antivirus to detect all types of threats. For more information about how to configure this feature, see **Antivirus** on page **342**.
- Configure anti-tamper protection. Set a password to prevent unauthorized uninstallation of the protection software. For more information about how to configure this feature, see **Configuring security against protection tampering** on page **321**.
- Verify that the maximum space for Shadow Copies is between 10% and 20% to prevent copies from being deleted because of lack of space. For more information about how to configure this feature, see **Configuring shadow copies** on page **325**.
- To remove ransomware, follow these steps:
  - Install at least the patches that fix the critical vulnerabilities detected. See **Cytomic Patch (Updating vulnerable programs)** on page **435**.
  - Run an on-demand scan. See **On-demand computer scanning and disinfection**.

    - Restart affected computers to close any remote connection in progress. For more information about how to configure this feature, see **Computer restart**.
    - If, after the affected computers are restarted, the ransomware is still active, contact Cytomic tech support.
- Restore encrypted files on each computer using Shadow Copies or the data recovery procedure in place in your company.
- Restore the security settings changed at the beginning of this procedure to their usual values.

Chapter 28

Tasks

A task is a resource implemented in Advanced EPDR that enables you to associate a process with two variables: repetition interval and execution time.

- **Repetition interval**: You can configure tasks to be performed only once, or repeatedly through specified time intervals.
- **Execution time**: You can configure tasks to be run immediately after being set (immediate task), or at a later time (scheduled task).

Chapter contents

Introduction to the task system

Accessing the task system

Depending on your need to configure all parameters of a task, these can be set up from different areas of the management console:

- Top menu **Tasks**.
- Computer tree (accessible from the top menu **Computers**).
- Lists associated with the different supported modules.

The computer tree and the lists enable you to schedule and launch tasks quickly and easily, without having to go through the entire configuration and publishing process described in section **Steps to launch a task**. However, they provide less configuration flexibility.

Steps to launch a task

The primary resource for creating a task is the **Tasks** area accessible from the menu at the top of the console. This area enables you to create tasks from scratch, configuring every aspect of the process.

The process of launching a task consists of three steps:

- **Task creation and configuration**: Select the affected computers, the characteristics of the task, the date/time the task will be launched, the task frequency, and the way it will behave in the event of an error. Task settings depend on the type of task. For more information about how to create and configure a task, see **Task types**
- **Task publication**: The tasks you create must be entered in the Advanced EPDR task scheduler to be run on the scheduled day/time.
- **Task execution**: The task is run when the configured conditions are met.

Task types

Advanced EPDR enables you to launch the following tasks:

- Scan and disinfect files. See **On-demand computer scanning and disinfection** on page **879** for more information.
- Install patches and updates for the operating system and other programs installed on user computers. For more information, see **Download and install patches** on page **442**.
- Search for IOCs across the computers on the network. See **Detection and management of IOCs** on page **587** for more information.

Permissions associated with task management

*For more information about the permission system implemented in Advanced EPDR, see **Understanding permissions** on page **72**.*

To create, edit, delete, or view tasks, you must use a user account that has the appropriate permission assigned to its role. Depending on the task, the required permissions are:

- **Launch scans and disinfect**: To create, delete, and edit **Scheduled scans** tasks.
- **Search for and manage IOCs**: To create, delete, and edit **Detect IOCs** tasks.

- **Install, uninstall, and exclude patches**: To create, delete, and edit **Install patches** tasks.
- **View detections**: To view the results of **Scheduled scans** tasks.

Creating a task from the Tasks area

- From the top menu, select **Tasks**. A list opens and shows all created tasks and their status.
- Click the **Add task** button. From the drop-down menu, select a task type. A page opens for you to enter the task details. This page is divided into multiple areas:
  - **Overview (1)**: Task name and description.
  - **Recipients (2)**: Computers that receive the task.
  - **Schedule (3)**: Task schedule (day and time the task runs).
  - **Settings (4)**: Specify the actions the task must take. This section varies based on the task type and is described in the documentation associated with the related module.

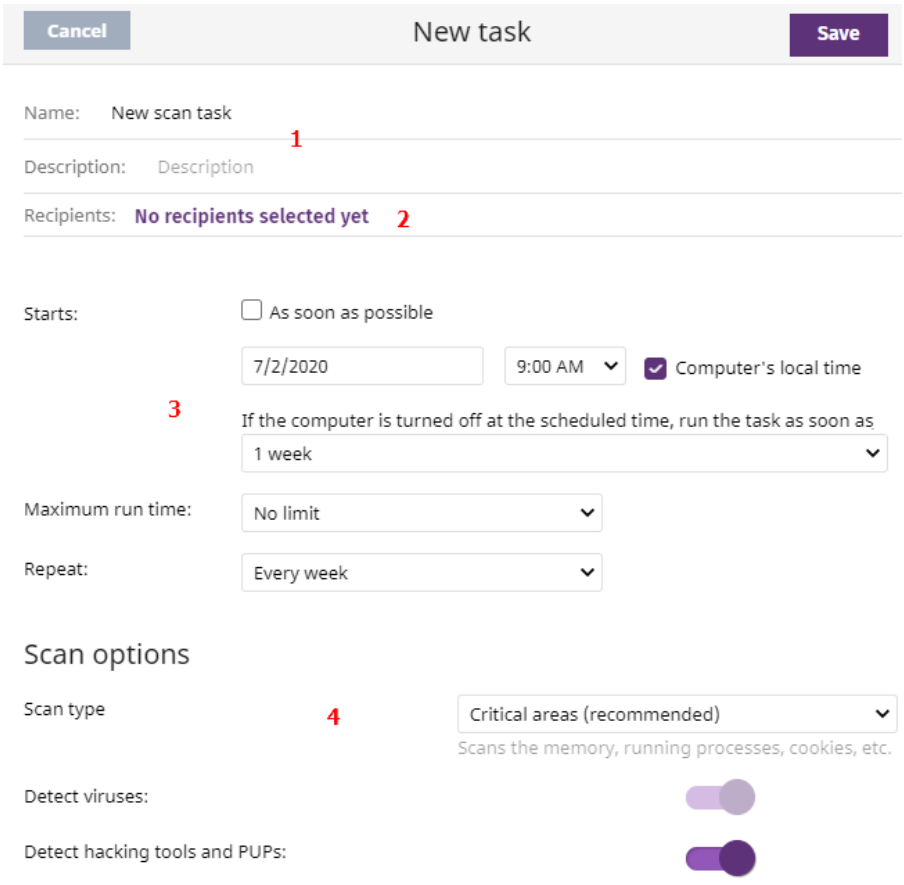


Figure 28.1: Overview of the New Task page for a scan task

Task recipients (2)

> *To access the computer selection page, you must first save the task. If you have not saved the task, a warning message is shown.*

- In the **Recipients** section, click the **No recipients selected yet** link. A page opens where you can select the computers that you want to receive the configured task.
- Select the types of computers that will receive the task: **Workstation**, **Laptop**, **Server**, or **Mobile device**. The type of computer that can receive a task depends on the task to run.
- Click the ⊕ button to add individual computers or computer groups. Click the 🗑 button to remove them.

> *If you are configuring a patch installation task and want to send it to test computers only, enable the **Run the task only on test computers**toggle. This option is applicable only to service providers who have CYTOMIC Nexus. For more information, see* ***Cytomic Patch features** on page **436***

- On the **Edit task** page, click the **View computers** button to view the computers that will receive the task.

Task schedule and frequency

You can configure these parameters:

- **Starts**: Indicates the task start date/time.

Value	Description
As soon as possible (selected)	The task runs immediately provided the computer is available (turned on and accessible from the cloud), or as soon as it becomes available within the time interval specified in the **If the computer is turned off** section
As soon as possible (cleared)	The task runs on the date selected in the calendar. Specify whether the time is based on the computer local time or the Advanced EPDR server time.
If the computer is turned off	If the computer is turned off or cannot be accessed, the task does not run. The task scheduler enables you to establish the task expiration time, from 0 (the task expires immediately if the computer is not available) to infinite (the

Value	Description
	task is always active and waits indefinitely for the computer to be available). • **Do not run:** The task is immediately canceled if the computer is not available at the scheduled time. • **Run the task as soon as possible, within:** Define a time interval during which the task will run if the computer becomes available. • **Run when the computer is turned on:** There is no time limit. The system waits indefinitely for the computer to be available to run the task.

Table 28.1: Task execution parameters

- **Maximum run time**: Indicates the maximum time that the task can take to complete. After that time, the task is canceled returning an error.

Value	Description
No limit	There is no time limit for the task to complete.
1, 2, 8, or 24 hours	There is a time limit for the task to complete. After that time, if the task has not finished, it is canceled returning an error.

Table 28.2: Task duration parameters

- **Frequency**: Set a repeat interval (every day, week, month, or year) from the date specified in the **Starts:** field.

Value	Description
One time	The task runs only once at the time specified in the **Starts:** field.
Daily	The task runs every day at the time specified in the **Starts:** field.
Weekly	Use the checkboxes to select the days of the week on which the task must run, at the time specified in the **Starts:** field.
Monthly	Choose an option: • Run the task on a specific day of every month. If you select the 29th, 30th, or 31st of the month, and the month does not have that day, the task runs on the last day of the month.

Value	Description
	• Run the task on the first, second, third, fourth, or last Monday to Sunday of every month.

Table 28.3: Task frequency parameters

Lower versions of the security software

If the recipient computers have a lower version of the security software installed, they might not correctly interpret frequency settings. Computers with lower versions of the security software interpret the task frequency settings as follows:

- **Daily tasks**: Unchanged.
- **Weekly tasks**: Recipient computers ignore the days selected in the task by the administrator in the latest software. The first run occurs on the specified start date and then runs again every 7 days.
- **Monthly tasks**: Recipient computers ignore the days selected in the task by the administrator in the latest software. The first run occurs on the specified start date and then runs again every 30 days.

Task publication

After you create and configure a task, it appears in the list of configured tasks. The status shows as **Unpublished** and it is not yet active.

To publish a task, click the **Publish** button. The task is added to the Advanced EPDR task scheduler, which runs it based on its settings.

Task list

Click **Tasks** in the top menu to view a list of all created tasks, their type, status, and other relevant information.

Field	Comment	Values
Icon	The task type.	• Patch installation or uninstallation task • On-demand

Field	Comment	Values
		scan task •  Disinfection task •  IOC detection task
Name	The task name.	Character string
Schedule	Date the task is set to run.	Character string
Status	• **No recipients**: The task will not run because there are no recipients assigned to it. Assign one or more computers to the task. • **Unpublished**: The task will not run because it has not been added to the scheduler queue. Publish the task so it can be launched by the scheduler based on its settings. • **In progress**: The task is running. • **Canceled**: The task was manually canceled. This does not mean that all processes that were running on the target computers have stopped. • **Finished**: The task finished running on all affected computers, regardless of whether it failed or was performed successfully. This status only applies to one-time tasks.	Character string

Table 28.4: Fields in the Tasks list

Filter tool

Field	Comment	Values
Type	The task type.	• Scan • Disinfection • Patch installation • Patch uninstallation

Field	Comment	Values
		• All • IOC search
Search task	Enter the task name.	Character string
Schedule	The task repeat frequency.	• Scan • Immediate • Once • Scheduled
Status	Task status	• Scan • No recipients • Unpublished • In progress • Canceled • Finished
Sort list	Task list sort order.	• Sort by creation date • Sort by name • Ascending • Descending

Table 28.5: Filters available in the Tasks list

Task management

From the top menu, select **Tasks** to delete, copy, cancel, or view the results of created tasks.

Selecting the tasks to manage

- To manage a single task, select the checkbox next to the task name.
- To manage all tasks on the page, select the checkbox next to the search bar in the upper-left corner of the page. To select all tasks in the entire list, click the **Select all x rows in the list** link.

Modifying a published task

Click a task name to view its settings page. There you can modify some of the task parameters.

> *For published tasks, you can change the name and description only. To modify other fields in a published task, you must create a copy of the task.*

Canceling a published task

Select the checkboxes next to the tasks you want to cancel. In the toolbar, click the **Cancel** icon. This cancels the tasks, but does not delete them from the task window, which enables you to view the results. You can cancel only tasks whose status is **In progress**.

Deleting a task

Executed tasks are not automatically deleted. To delete a task, select it using the checkboxes and click the icon. You must cancel a task before you can delete it.

> *When you delete a task, you also delete the task results.*

Copying a task

When you copy a task, you can copy all of its settings. If the task includes recipients, you can choose whether to copy them.

- From the top menu, select **Tasks**. Click the icon for the task you want to copy. From the drop-down menu, select the copy type.

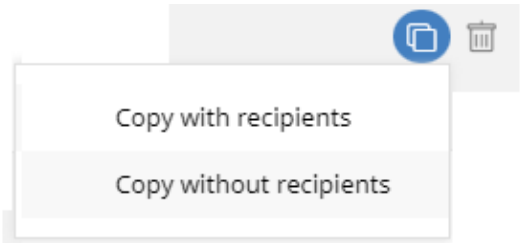


Figure 28.2: Copy task icon menu

- If you select **Copy without recipients**, the **Copy task** page opens.
  - To assign recipients, click the **No recipients selected yet** link. The **Recipients** page opens.
  - Select the task recipients. Click **Save** in the upper-right corner of the page.

> *With patch installation tasks, if you want to send the task to test computers only, enable the **Run the task only on test computers** toggle. This option is applicable only to service providers who have CYTOMIC Nexus. For more information, see **Cytomic Patch features** on page **436**.*

If you select **Copy with recipients**, the **Copy task** page opens and shows the recipients configured in the original task.

Exporting tasks

Click the  icon to export the list of tasks. A .CSV file is saved to the folder of your choice.

The downloaded file contains these columns:

Field	Definition
Task name	Task name
Task type	The type of task: • IOC search • Patch uninstallation • Patch installation • Scan
Schedule	The pattern of recurrence for the task: • Inmediate • Once • Scheduled
Status	The status of the task: • No recipients • Unpublished • In progress • Canceled • Finished

Field	Definition
Recipient group	The group that receives the task.
Workstation	• **Yes**: The task is assigned to computers of the Workstation type in the recipient group. • **No**: The task is not assigned to computers of the Workstation type in the recipient group.
Laptop	• **Yes**: The task is assigned to computers of the Laptop type in the recipient group. • **No**: The task is not assigned to computers of the Laptop type in the recipient group.
Server	• **Yes**: The task is assigned to computers of the Server type in the recipient group. • **No**: The task is not assigned to computers of the Server type in the recipient group.
Mobile device	• **Yes**: The task is assigned to mobile devices in the recipient group. • **No**: The task is not assigned to mobile devices in the recipient group.
Recipient computer	The computer that receives the task.
Recipient computer group	Type of computer that receives the task: • Workstation • Laptop • Server • Mobile device

Table 28.6: Tasks exported list

Task results

Click the **View results** link of a published task to view its results up to that point and access a filter tool for finding specific computers among those that received the task.

Some of the fields in the results list are specific to certain tasks. Those fields are described in the documentation associated with the relevant module. Next is a description of the fields common to all results lists.

Field	Description	Values
Computer	Name of the computer where the task was run.	Character string
Group	Folder within the Advanced EPDR folder tree the computer belongs to.	Character string
Status	Status of the task process on the affected computer: • **Pending**: The task's next recurrence has not started because it is scheduled to run at a later time.. • **In progress**: The task is running on the computer. • **Finished**: The task finished successfully. • **Failed**: The task failed and returned an error. • **Canceled (the task could not start at the scheduled time)**: The task could not start at the scheduled time because the target computer was turned off or in a state that prevented the task from running. • **Canceled**: The process was canceled on the computer. • **Canceling**: The task was canceled, but the target computer has not finished canceling the task process. • **Canceled (maximum run time exceeded)**: The task was automatically canceled because it exceeded its configured maximum run time.	Character string
Start date	The task start date.	Date
End date	The task end date.	Date

Table 28.7: Common fields in task results lists

Task filter tool

Field	Description	Values
Date	Drop-down menu with the date the task became active based on the configured schedule. An active task can be launched immediately or wait until the target computer is available. This date is shown in the Date column.	Date
Status	• **Pending**: The task has not been launched as the execution window has not started yet. • **In progress**: The task is currently running. • **Finished**: The task finished successfully. • **Failed**: The task failed and returned an error. • **Canceled (the task could not start at the scheduled time)**: The target computer was not accessible at the time the task was set to start or during the selected time period. • **Canceled**: The task was manually canceled. • **Canceled (maximum run time exceeded)**: The task was automatically canceled because it exceeded its configured maximum run time.	Enumeration

Table 28.8: Search filters in task results

Automatic adjustment of task recipients

If the administrator selects a computer group as the recipient of a task, the computers that finally run the task may vary from those initially selected. This is because groups are dynamic entities that change over time.

That is, you can define a task at a specific time (T1) to be run on a specific group containing a series of computers. However, at the time the task is run (T2), the computers in that group may have changed.

When it comes to determining which computers will receive a configured task, there are three cases depending on the task:

- Immediate tasks.
- One-time scheduled tasks.
- Recurring scheduled tasks.

Immediate tasks

These tasks are created, published, and launched almost simultaneously and only once. The target group is evaluated at the time the administrator creates the task. The task status for the affected computers is **Pending**.

Adding computers to the target group

You cannot add new computers to the target group. Even if you add new computers to the target group, they will not receive the task.

Removing computers from the target group

You can remove computers from the target group. Move a computer to another group to cancel the task on that computer.

One-time scheduled tasks

There are two possible scenarios for changing the computers included in the target group:

Tasks which started running less than 24 hours ago

Within the first 24 hours after a task stars running, it is still possible to add or remove computers from its target groups. This 24-hour period is established to cover all time zones for multinational companies with a presence in several countries.

Tasks which started running more than 24 hours ago

24 hours after a task starts running, it is not possible to add new computers to it. Even if you add new computers to the target group, they will not receive the task. To cancel the task on a computer, move it outside the target group.

Recurring scheduled tasks

These tasks allow the addition and removal of target computers at any time before they are canceled or completed.

Unlike immediate tasks, the status of the task on each computer is not automatically set to **Pending**. The status of the task on each computer is shown gradually in the console as the Cytomic platform receives the relevant information from each computer.

Chapter 29

Product features and requirements

Chapter contents

Supported features by platform

General

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Web-based console	X	X	X	X	X
Information in dashboards	X	X	X	X	X
Filter-based computer organization	X	X	X	X	X
Group-based computer organization	X	X	X	X	X
Languages	11	11	11	16	10

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
supported in the security software					

Table 29.1: General features

Lists and reports

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Frequency that malware, PUPs and exploit activity, and blocked programs are sent to the server	1 min	10 min	10 min	Immediately after scan completes	N/A
Frequency that other detections are sent to the server	15 min	15 min	15 min	Immediately after scan completes	15 min
List of detections	X	X	X	X	X
Executive reports	X	X	X	X	X
Scheduled executive reports	X	X	X	X	X

Table 29.2: List and report features

Protection

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Anti-phishing	X		X		X
Real-time permanent antivirus protection	X	X	X	X	
Contextual detections	X	X			
Network attack protection	X				
Anti-exploit protection (*)	X				
Zero-Trust Application Service: Hardening and Lock protection modes	X				
Indicators of attack (IOAs)	X	X	X		
Risk evaluation	X	X	X	X	X
Shadow copies	X				
Decoy files	X				
Firewall	X				
Web access control	X		X		X

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Device control	X				
Indicators of compromise (IOCs) compatible with STIX and Yara rules	X				
Advanced security policies	X				
Advanced indicators of attack (IOAs)	X				
Anti-theft				X	X

Table 29.3: Protection features

Hardware and software information

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Hardware information and list	X	X	X	X	X
Software information and list	X	X	X	X	X
Software change log	X	X	X	X	X
Information about installed OS	X				

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
patches					
Vulnerability assessment	X	X	X		

Table 29.4: Hardware and software information features

Settings

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Security settings for workstations and servers	X	X	X	N/A	N/A
Anti-tamper protection	X	X			
Two-factor authentication	X	X			
Password to uninstall the protection and take actions locally	X	X			
Secure VPN connections	X		X	X	
Secure access to Wi-Fi network	X		X	X	
Ability to establish multiple proxies	X	X	X	N/A	N/A
Ability to work as a	X			N/A	N/A

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Cytomic proxy					
Ability to access the Internet through a proxy	X	X	X	N/A	N/A
Ability to work as a repository or cache	X			N/A	N/A
Ability to use the repository or cache	X			N/A	N/A
Discovery of unprotected computers	X				
Email alerts in the event of an infection	X	X	X	X	N/A
Email alerts when finding an unprotected computer	X	X	X	X	N/A

Table 29.5: Configuration features

Remote actions from the web console

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Real-time actions	X	X	X	X	X
On-demand	X	X	X	X	N/A

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
scans					
Scheduled scans	X	X	X	X	N/A
Remote installation of the Cytomic agent	X				
Remote uninstallation of the Cytomic agent	X	X	X		
Ability to reinstall the agent and protection	X				
Computer restart	X	X	X		
Computer isolation	X	X	X		
Ability to authorize the execution of software	X				
Ability to block the execution of software	X				
Ability to report incidents (PSInfo)	X			X	X
Remote shell to manage processes and services, file transfers,	X	X	X		

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
command line tools, get dumps, pcap, etc.					
Ability to report problems	X	X	X	X	X

Table 29.6: Available remote actions

Security software updates and upgrades

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Signature updates	X	X	X	X	N/A
Protection upgrades	X	X	X	X	N/A
Ability to schedule protection upgrades	X	X	X	Google Play	App Store

Table 29.7: Security software update and upgrade features

Available modules

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Cytomic Insights	X	X	X		
Cytomic Patch	X	X	X		

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Cytomic Data Watch (*)	X				
Cytomic Encryption	X	X	X		

Table 29.8: Available modules

(*) The feature works on Windows (Intel) and partially on Windows (ARM).

Product features and requirements

Chapter contents

Supported features by platform

General

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Web-based console	X	X	X	X	X
Information in dashboards	X	X	X	X	X
Filter-based computer organization	X	X	X	X	X
Group-based computer organization	X	X	X	X	X

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Languages supported in the security software	11	11	11	16	10

Table 29.9: General features

Lists and reports

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Frequency that malware, PUPs and exploit activity, and blocked programs are sent to the server	1 min	10 min	10 min	Immediately after scan completes	N/A
Frequency that other detections are sent to the server	15 min	15 min	15 min	Immediately after scan completes	15 min
List of detections	X	X	X	X	X
Executive reports	X	X	X	X	X
Scheduled executive reports	X	X	X	X	X

Table 29.10: List and report features

Protection

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Anti-phishing	X		X		X
Real-time permanent antivirus protection	X	X	X	X	
Contextual detections	X	X			
Network attack protection	X				
Anti-exploit protection (*)	X				
Zero-Trust Application Service: Hardening and Lock protection modes	X				
Indicators of attack (IOAs)	X	X	X		
Risk evaluation	X	X	X	X	X
Shadow copies	X				
Decoy files	X				
Firewall	X				
Web access control	X		X		X

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Device control	X				
Indicators of compromise (IOCs) compatible with STIX and Yara rules	X				
Advanced security policies	X				
Advanced indicators of attack (IOAs)	X				
Anti-theft				X	X

Table 29.11: Protection features

Hardware and software information

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Hardware information and list	X	X	X	X	X
Software information and list	X	X	X	X	X
Software change log	X	X	X	X	X
Information about installed OS	X				

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
patches					
Vulnerability assessment	X	X	X		

Table 29.12: Hardware and software information features

Settings

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Security settings for workstations and servers	X	X	X	N/A	N/A
Anti-tamper protection	X	X			
Two-factor authentication	X	X			
Password to uninstall the protection and take actions locally	X	X			
Secure VPN connections	X		X	X	
Secure access to Wi-Fi network	X		X	X	
Ability to establish multiple proxies	X	X	X	N/A	N/A
Ability to work as a	X			N/A	N/A

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Cytomic proxy					
Ability to access the Internet through a proxy	X	X	X	N/A	N/A
Ability to work as a repository or cache	X			N/A	N/A
Ability to use the repository or cache	X			N/A	N/A
Discovery of unprotected computers	X				
Email alerts in the event of an infection	X	X	X	X	N/A
Email alerts when finding an unprotected computer	X	X	X	X	N/A

Table 29.13: Configuration features

Remote actions from the web console

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Real-time actions	X	X	X	X	X
On-demand	X	X	X	X	N/A

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
scans					
Scheduled scans	X	X	X	X	N/A
Remote installation of the Cytomic agent	X				
Remote uninstallation of the Cytomic agent	X	X	X		
Ability to reinstall the agent and protection	X				
Computer restart	X	X	X		
Computer isolation	X	X	X		
Ability to authorize the execution of software	X				
Ability to block the execution of software	X				
Ability to report incidents (PSInfo)	X			X	X
Remote shell to manage processes and services, file transfers,	X	X	X		

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
command line tools, get dumps, pcap, etc.					
Ability to report problems	X	X	X	X	X

Table 29.14: Available remote actions

Security software updates and upgrades

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Signature updates	X	X	X	X	N/A
Protection upgrades	X	X	X	X	N/A
Ability to schedule protection upgrades	X	X	X	Google Play	App Store

Table 29.15: Security software update and upgrade features

Available modules

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Cytomic Insights	X	X	X		
Cytomic Patch	X	X	X		

Available features	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Cytomic Data Watch (*)	X				
Cytomic Encryption	X	X	X		

Table 29.16: Available modules

(*) The feature works on Windows (Intel) and partially on Windows (ARM).

Requirements for Windows platforms

Supported operating systems

From 30 September 2024, you will not be able to add devices to the management console or install the protection software on new computers that run these operating system versions: Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008 (Windows 2008 R2 will continue to be supported). Existing computers in the management console will continue to be protected. See ***https://www.watchguard.com/wgrd-trust-center/end-of-life-policy***.

Workstations with an x86 or x64 microprocessor

- Windows XP SP3 (32-bit)
- Windows Vista (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)
- Windows 11 (64-bit)

Computers with an ARM microprocessor

- Windows 10 and Pro
- Windows 11 and Pro
- Windows Server 2025 Standard, Datacenter

Servers with an x86 or x64 microprocessor

- Windows 2003 (32-bit, 64-bit) and R2 SP2
- Windows 2008 (32-bit and 64-bit) and 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 and Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025 Standard, Datacenter
- Windows Server Core 2008, 2008 R2, 2012 R2, 2016, 2019, and 2022

IoT and Windows Embedded Industry

- Windows XP Embedded
- Windows Embedded for Point of Service
- Windows Embedded POSReady 2009, 7, 7 (64-bit)
- Windows Embedded Standard 2009, 7, 7 (64-bit), 8, 8 (64-bit)
- Windows Embedded Pro 8, 8 (64-bit)
- Windows Embedded Industry 8, 8 (64-bit), 8.1, 8.1 (64-bit)
- Windows IoT Core 10, 10 (64-bit)
- Windows IoT Enterprise 10, 10 (64-bit), 11
- Windows Server IoT 2019

Windows Embedded systems allow custom installations that could impact Advanced EPDR. After you install Advanced EPDR, we recommend that you confirm it works as expected.

Hardware requirements

- **Processor**: x86- or x64-compatible CPU with at least SSE2 support.
- **RAM**: 1 GB.
- **Available hard disk space for installation**: The minimum space required to install the security software varies depending on the operating system version installed on the computer. On average, the security software requires 650 MB of available space for installation.

Other requirements

Ports

Advanced EPDR requires access to multiple Internet-hosted resources. It requires access to ports 80 and 443.

The Advanced EPDR agent requires port 33000 for communication between protected computers and with the Firebox or Access Point devices (see **Endpoint Access Enforcement settings** on page **518** and **Network Access Enforcement** on page **318**

Root certificates

It is necessary to keep the root certificates of workstations and servers up to date. Also, the computers must be able to access these URLs:

http://*.globalsign.com

http://*.digicert.com

http://*.sectigo.com

Windows computers update root certificates automatically through Windows Update. Nevertheless, incorrectly installed updates might cause problems.

If root certificates are not up to date, some features such as the ability for agents to establish real-time communications with the management console, or the Cytomic Patch module, might not work.

*To identify and update root certificates, use the tool available at **https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Endpoint-Security/troubleshooting/psinfotool/psinfo-check-cert.html?Highlight=psinfo**.*

Time synchronization of computers (NTP)

Although not an essential requirement, we recommend that the clocks on computers protected by Advanced EPDR be synchronized. This synchronization is normally achieved using an NTP server.

If a computer is not synchronized, several security issues could arise:

- Lack of stability in communications between the computer and the Cytomic servers.
- Errors checking certificates, which appear as valid or expired based on the computer system date, not the real date.
- Date errors in alerts generated by protections, which show the computer system date, not the real date.
- Scan and patch installation tasks show the computer system date, not the real date.
- The installer expiration date is not respected.
- The time periods defined in the web access control feature are not adhered to.
- Some scheduled actions might not run correctly, such as computer restarts and problem notifications.

Support for SHA-256 driver signing

To keep security software up to date, the workstation or server must support SHA-256 driver signing. Some versions of Windows do not include this feature by default and you must update them:

Windows platform	Updates required	URL
Windows Vista x86/Vista x64	SP2 and KB4474419	**KB4474419** **SP2**
Windows Server 2008 x86/Server 2008 x64	SP2 and KB4474419	**KB4474419** **SP2**
Windows 7 x86/Windows 7 x64	SP1 and KB4474419	**KB4474419** **SP1**
Windows 2008 R2 x64	KB4474419	**KB4474419**

Table 29.17: Updates required to support SHA-256 signed drivers

Computers that do not support SHA-256 driver signing will not have their protection software updated beyond protection version 4.00.00. These computers are not shown in the **Outdated protection** on page **666** widget as candidates to be updated. These computers are shown with the warning **Cannot upgrade this computer's protection to the latest version**. For more information about computer alerts and how to display them, see **Computer details** on page **252**.

To find computers that do not support SHA-256 driver signing, create a filter in the filter tree with the parameters described in **Filter computers not compatible with SHA-256 signed drivers** on page **221**. For more information about the filter tree, see **Filter tree** on page **214**.

We recommend that you update all computers to make sure they are protected with the latest available version of the security software.

After you install the patches indicated, the latest available version of the security software downloads within four hours. You must restart the computer to complete the update.

Windows XP and Windows 2003 operating systems

For advanced protection to operate correctly on these operating systems, Internet Explorer 7 or higher must be installed on the computer.

You cannot install or upgrade the security software directly on Windows XP computers. You must use a computer with the cache role. For more information, see **Configuring downloads from cache computers** on page **315**

You can install or upgrade the security software on Windows 2003 computers only if the operating system is fully updated and all required patches are installed. Otherwise, you must use a computer with the cache role. For more information, see **Cytomic Patch (Updating vulnerable programs)** on page **435**.

Requirements for macOS platforms

From 30 September 2024, you will not be able to add devices to the management console or install the protection software on new computers that run these operating system versions: macOS Yosemite, El Capitan, Sierra, High Sierra, or Mojave. Existing computers in the management console will continue to be protected. See ***https://www.watchguard.com/wgrd-trust-center/end-of-life-policy***.

Supported operating systems

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11 Big Sur
- macOS 12 Monterey

- macOS 13 Ventura
- macOS 14 Sonoma
- macOS 15 Sequoia

Hardware requirements

- **Processor**: Intel® Core 2 Duo.
- **RAM**: 2 GB.
- **Available hard disk space for installation**: The minimum space required to install the security software varies depending on the operating system version installed on the computer. On average, the security software requires 400 MB of available space for installation.
- **Ports**: Ports 3127, 3128, 3129, and 8310 must be accessible for the web filtering and malware web detection to work. The Advanced EPDR agent requires port 33000 for communication between computers.

IP addresses required for product activation

To install the security software, make sure the corporate firewall allows traffic to these IP address ranges:

- 17.248.128.0/18
- 17.250.64.0/18
- 17.248.192.0/19

Required permissions

For the security software to operate correctly, you must enable:

- Network extensions.
- System extensions.
- Full disk access.
- Background execution.

Complete the appropriate procedure for your macOS version:

For macOS Catalina or higher

To enable system extensions:

- Open the Advanced EPDR agent on the user computer. Click **Open Security Preferences**.
- The **Security & Privacy** dialog box opens. In the lower-left corner, click the lock icon.
- Enter the administrator **User Name** and **Password**. Click **Unlock**.
- Click **Allow**. System extensions are enabled.

To enable Full Disk Access:

- Open the Advanced EPDR agent on the user computer. Click **Open hard disk access preferences**.
- The **Security & Privacy** dialog box opens. In the lower-left corner, click the lock icon.
- Enter the administrator **User Name** and **Password**. Click **Unlock**.
- Select **Protection Agent**.
- Click **Quit & Reopen**. Full Disk Access is enabled.

For macOS Mojave 10.14 or lower

When your Advanced EPDR software for macOS starts, macOS might block the kernel extensions necessary for it to work.

The reason for this is that macOS 10.14 and lower contain a security feature that requires user approval before it can load new third-party kernel extensions.

For more information, see ***https://developer.apple.com/library/archive/technotes/tn2459/_index.html#//apple_ref/doc/uid/DTS40017658****.*

When a request is made to load a kernel extension that the user has not yet approved, the load request is denied. You might receive these notifications:

- System Extension Blocked message.
- Your Computer Is Not Protected message.

To manually approve the kernel extension:

- When you receive the **System Extension Blocked** message, click **OK**. Or, click **Open System Preferences** when you receive the **Your Computer Is Not Protected** message. The **System Preferences** dialog box opens.
- Click **Security & Privacy**.
- In the lower-left corner, click the lock icon.
- In the **Security & Privacy** dialog box, click **Allow**.

For macOS Ventura 13

The security software might stop working on computers if the agent is not allowed to run in the background. For this reason, you must allow the **Background execution** permission on the computer.

Requirements for Linux platforms

Advanced EPDR can be installed on Linux workstations and servers. On computers with no graphical environment, the URL filtering and web detection features are disabled. To manage the security software on computers with no graphical environment, use the `/usr/local/protection-agent/pa_cmd` tool.

Supported distributions

64-bit distributions

- **Ubuntu**: 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS, 16.10, 17.04, 17.10, 18.04 LTS, 18.10, 19.04, 19.10, 20.04 LTS, 20.10, 21.04, 21.10, 22.04 LTS, 22.10, 23.04, 23.10, 24.04, and 24.10.
- **Fedora**: 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40 and 41.
- **Debian**: 8, 9, 10, 11, and 12.
- **RedHat**: 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, and 9.5.
- **CentOS**: 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4, and 8.5.
- **CentOS Stream**: 8 and 9.
- **Rocky Linux**: 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, and 9.5.
- **AlmaLinux**: 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, and 9.5.
- **Linux Mint**: 18, 18.1, 18.2, 18.3, 19, 19.1, 19.2, 19.3, 20, 20.1, 20.2, 20.3, 21, 21.1, 21.2, 21.3 22 and 22.1.
- **SUSE Linux Enterprise**: 11 SP2, 11 SP3, 11 SP4, 12, 12 SP1, 12 SP2, 12 SP3, 12 SP4, 12 SP5, 15, 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5, and 15 SP6.
- **Oracle Linux:** 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, and 9.5.
- **openSUSE**: 15.3, 15.4, 15.5, and 15.6.
- **Amazon Linux:** 2

32-bit distributions

- **Red Hat**: 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.
- **CentOS**: 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.

Supported kernel versions

For more information about the supported Linux distributions and kernels, see **https://info.cytomicmodel.com/resources/help/EPDR/v16/es/Content/28_ hardware_ software_ network_requirements/linux_kernels.htm**.

Advanced EPDR is not supported on special or modified versions of the Linux kernel.

Supported file managers

- Nautilus
- PCManFM
- Dolphin

Hardware requirements

- **Processor**: x86 or x64-compatible CPU with at least SSE2 support.
- **RAM**: 1.5 GB.
- **Available hard disk space for installation**: The minimum space required to install the security software varies depending on the operating system version installed on the computer. On average, the security software requires 500 MB of available space for installation.
- **Ports**: Ports 3127, 3128, 3129, and 8310 must be accessible for the web filtering and malware web detection to work. The Advanced EPDR agent requires port 33000 for communication between computers.

Installation script checks

When you run it, the installation script performs a number of checks that require installation of one of these packages or binaries:

- wget
- curl
- semanage (if you need to integrate the security software using SELinux policies)

If none of these packages are installed, the installation process fails returning an error.

Installation package dependencies

The Linux agent uses the distribution package manager to download all dependencies that are not satisfied. Generally, the packages required are:

- **Libcurl**: For Debian-based distributions, see **Libcurl libraries**
- **OpenSSL**
- **GCC and compilation utilities**: make and makeconfig only on Fedora.

The installation process on Fedora includes compilation of the modules required by the Advanced EPDR agent to work correctly.

To show the agent dependencies, run these commands on a terminal based on the target distribution:

- For Debian-based distributions: `dpkg --info package.deb`
- For Fedora-based distributions: `rpm --qRp package.rpm`

Libcurl libraries

The protection module requires the installation of the 32-bit `libcurl3` or 32-bit `libcurl4` library. If you already have one of these libraries installed (for 64-bit systems), make sure the package manager downloads the same library (`libcurl3` or `libcurl4`) with the same version for 32-bit systems. Otherwise, Advanced EPDR does not run correctly on the computer and you must manually install the appropriate library.

For example, if your computer has the `libcurl3 x.y.z` library (for 64-bit systems), the package manager must download the `libcurl3 x.y.z` library (for 32-bit systems), and not `libcurl4 x.y.z` (for 32-bit systems).

Supported kernels

Last updated: Tuesday, April 1, 2025

For more information about the supported Linux distributions and kernels, see **Supported kernels**.

Requirements for Android platforms

Supported operating systems

- Android Marshmallow 6.0
- Android Nougat 7.0 - 7.1
- Android Oreo 8.0
- Android Pie 9.0
- Android 10
- Android 11
- Android 12
- Android 13
- Android 14

Hardware requirements

The minimum space required to install the security software varies depending on the operating system version installed on the device. On average, the security software requires 10 MB of available space for installation.

Network requirements

For push notifications to work, open ports 5228, 5229, and 5230 to all IP addresses contained in the IP blocks listed in Google's ASN 15169.

Permissions required on the device

To use all of the Advanced EPDR features, the user of the device must allow these permissions:

- Camera access
- Read phone state
- Make calls
- Get location
- Device location services
- Draw over other apps
- Act as device administrator
- Access external storage
- Background location access

On mobile devices that run Android 12, these permissions are also required:

- Disable app hibernation
- Ignore battery optimizations

On mobile devices that run Android 13, this permission is also required:

- Send notifications

Requirements for iOS platforms

Supported operating systems

- iOS 13 / iPadOS 13
- iOS 14 / iPadOS 14
- iOS 15 / iPadOS 15

- iOS 16 / iPadOS 16
- iOS 17 / iPadOS 17

Hardware requirements

The minimum space required to install the security software varies depending on the operating system version installed on the device. On average, the security software requires 12 MB of available space for installation.

Network requirements

The application installed on the mobile device uses the Apple Push Notification service to communicate with Advanced EPDR. If the device is connected to the network by 2G, 3G, or 4G, there are no specific network requirements.

If the device is connected to the network by Wi-Fi, Access Point (AP), or other method, it connects to specific servers. Make sure these ports are available:

- TCP 5223 to communicate with the Apple Push Notification service.
- TCP 443 or 2197 to send notifications.

Servers that make up the Apple Push Notification service use load balancing. The device will not always connect to the same IP address. We recommend that you configure your firewall to allow connections to the entire 17.0.0.0/8 range assigned to Apple. If this is not possible, allow connections to these IP ranges:

For IPv4:

- 17.249.0.0/16
- 17.252.0.0/16
- 17.57.144.0/22
- 17.188.128.0/18
- 17.188.20.0/23

For IPv6:

- 2620:149:a44::/48
- 2403:300:a42::/48
- 2403:300:a51::/48
- 2a01:b740:a42::/48

*For more information, see **https://support.apple.com/en-us/HT203609**.*

Permissions required on the device

To use all of the Advanced EPDR features, the user of the device must allow these permissions:

- Get location
- Device location services
- Background location access
- Filter network content
- Receive push notifications
- Send notifications
- Allow background app refresh

Local ports and URL access

Local ports

To implement certain features, the security software installed on the computers on the network uses these listening ports:

Windows

- **TCP port 18226**: Used by computers with the cache role on all network interfaces. See **Cache role** on page **310**.
- **TCP port 21226**: Used by computers with the cache role to request the files to download on all network interfaces. See **Cache role** on page **310**.
- **TCP port 3128**: Used by computers with the proxy role on all network interfaces. See **Cytomic proxy role** on page **308**.
- **UDP port 21226**: Used by computers with the discovery computer role on all network interfaces. See **Discovery computer role** on page **312**
- **TCP port 33000**: Used by computers that make a VPN connection to the Firebox on all network interfaces, and for communication between computers. See **Network Access Enforcement** on page **318** and **Endpoint Access Enforcement settings** on page **518**.
- **UDP port 35621**: Used by the protection module on the localhost interface.

Linux

- **UDP port 21226**: Used by computers with the discovery computer role on all network interfaces. See **Discovery computer role** on page **312**
- **TCP port 4575**: Used by the protection module on the localhost interface.
- **TCP port 8310**: Used by the protection module on the localhost interface.

- **TCP port 5560**: Internal process communication on the localhost interface.
- **TCP port 33000**: Used by computers that make a VPN connection to the Firebox on all network interfaces, and for communication between computers. See **Network Access Enforcement** on page **318** and **Endpoint Access Enforcement settings** on page **518**.

macOS

- **UDP port 21226**: Used by computers with the discovery computer role on all network interfaces. See **Discovery computer role** on page **312**
- **TCP port 33000**: Used by computers that make a VPN connection to the Firebox on all network interfaces. See **Network Access Enforcement** on page **318**.
- **TCP port 4575**: Used by the protection module on the localhost interface.
- **TCP port 8310**: Used by the protection module on the localhost interface.
- **TCP port 5560**: Internal process communication on the localhost interface.
- **TCP port 33000**: Used by computers that make a VPN connection to the Firebox on all network interfaces, and for communication between computers. See **Network Access Enforcement** on page **318** and **Endpoint Access Enforcement settings** on page **518**.

Access to the web console

You can access the management console with the latest version of these browsers:

- Chrome
- Microsoft Edge
- Firefox
- Opera

Access to service URLs

For Advanced EPDR to work correctly, the protected computers must be able to access these URLs.

Product name	URLs
Advanced EPDR	• https://*.pandasecurity.com • Downloading of installers, the generic uninstaller, and policies. • Agent communications (registration, configuration, tasks, actions, status, real-time communications). • Communications between the protection and Collective Intelligence. • Downloading of signature files on Android systems.

Product name	URLs
	• http://*.pandasecurity.com • Downloading of signature files (on all systems except Android). • https://*.windows.net URLs to send unknown files: • cmg-fusmb.pandasecurity.com • cmp-fusmb.pandasecurity.com • cpg-fusmb.pandasecurity.com • cpp-fusmb.pandasecurity.com • cppi-fusmb.pandasecurity.com • cppl-fusmb.pandasecurity.com • cppe-fusmb.pandasecurity.com • rpuws.pandasecurity.com
Root certificates	• http://*.globalsign.com • http://*.digicert.com • http://*.sectigo.com
Web filtering	• https://rp.cloud.threatseeker.com • https://wg.cloud.threatseeker.com
Cytomic Data Watch	• https://pandasecurity.devo.com
Cytomic Orion	To perform remediation actions from Cytomic Orion, you must allow access to these URLs on the computer local firewall if it is from a vendor other than Cytomic: • dir.rc.pandasecurity.com through ports 8080 and 443. • eu01.rc.pandasecurity.com through ports 8080 and 443. • eu02.rc.pandasecurity.com through ports 8080 and 443. • eu03.rc.pandasecurity.com through ports 8080 and 443. • eu04.rc.pandasecurity.com through ports 8080 and 443. • eu05.rc.pandasecurity.com through ports 8080 and 443.

Product name	URLs
	• eu06.rc.pandasecurity.com through ports 8080 and 443. • ams01.rc.pandasecurity.com through ports 8080 and 443. • ams02.rc.pandasecurity.com through ports 8080 and 443.
Activity testing	For Windows protection versions higher than 8.00.16. • http://proinfo.pandasoftware.com/connectiontest.html For connectivity tests: • http://*.pandasoftware.com
Network attack protection	• https://cpg-nap.pandasecurity.com/nap/buffer • https://cpp-nap.pandasecurity.com/nap/buffer
MITRE	• **Windows**: **cpp-fuelg.pandasecurity.com** • **Linux**: **cppl-fuelg.pandasecurity.com** • **Mac**: **cppi-fuelg.pandasecurity.com** • cppe-fuelg.pandasecurity.com • cpg-fuelg.pandesecurity.com

Table 29.18: Service access URLs

Access to URLs for patch and update downloads (Cytomic Patch)

For a complete list of the URLs that must be accessible to the network computers that receive patches or have the cache/repository role, see this support article: **https://www.pandasecurity.com/uk/support/card?id=700044**.

Chapter 30

Format of the events contained in telemetry data

Advanced EPDR monitors the processes that run on customer computers and sends the generated telemetry data to the Cytomic cloud. Specialized threat hunters use this data to detect indicators of attack (IOA) on customer IT resources.

Telemetry data is stored in events which consist of several fields. Analysts must understand the meaning of each of these fields to correctly interpret event information.

The information about the event that triggered the IOA is available in JSON format on the IOA details page, as well as in the attack graphs. For more information about the IOA detection module, see **Indicators of attack settings** on page **609**.

You can also access the full telemetry data generated by a computer on the **Investigation** tab on the computer details page. See **Investigation section (5)** on page **275**.

For more information about the types of events, see **Fields in the Events Received by Cytomic Orion**.

Glossary

A

Active Directory

Proprietary implementation of LDAP (Lightweight Directory Access Protocol) services for Microsoft Windows computers. It enables access to an organized and distributed directory service for finding a range of information in network environments.

Activity graph/execution graph

Graphical representation of the actions triggered by threats over time.

Adaptive protection cycle

A new security approach based on the integration of a group of services providing protection, detection, monitoring, forensic analysis, and remediation capabilities into a single management console accessible from anywhere at any time.

Advanced EPDR client software

Program installed on the computers to protect. It consists of two modules: the Cytomic agent and the protection.

Advanced protection

Technology that continuously monitors and collects information from all processes running on the computers on your network, and sends it to the cloud for analysis. This information is analyzed using

machine learning techniques in Big Data environments, returning an accurate classification (goodware or malware).

Advanced reports

See Adware.

Adware

Program that automatically runs, displays, or downloads advertising to the computer.

Alert

See Incident.

Anti-spam

Technology that searches for unwanted email based on its contents.

Anti-Tamper protection

A set of technologies aimed at preventing tampering of the Advanced EPDR processes by unauthorized users and APTs looking for ways to bypass the security measures in place.

Anti-Theft

Set of technologies incorporated into Advanced EPDR and designed to locate lost or stolen mobile devices and minimize data exposure in the case of theft.

Antivirus

Protection module that relies on traditional technologies (signature files, heuristic scanning, contextual analysis, etc.), to detect and remove computer viruses and other threats.

APT (Advanced Persistent Threat)

A set of strategies implemented by hackers and aimed at infecting customers' networks through multiple infection vectors simultaneously. They are designed to go undetected by traditional antivirus programs for long periods of time. Their main aim is financial (through theft of confidential information, intellectual property, etc.).

ARP (Address Resolution Protocol)

A telecommunication protocol used for resolution of Internet layer addresses into link layer addresses. On IP networks, this protocol translates IP addresses into physical MAC addresses.

ASLR (Address Space Layout Randomization)

Address Space Layout Randomization (ASLR) is a security technique used in operating systems to prevent buffer overflow-driven exploits. To prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, ASLR randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap, and libraries. This prevents attackers from illegitimately using calls to certain system functions as they will not know where in memory those functions reside.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

A set of resources developed by the MITRE Corporation to describe and categorize dangerous actions of cybercriminals based on observations from around the world. ATT&CK is a structured list of the known behaviors of attackers, broken down into tactics and

techniques, and expressed as a matrix. As this list is a comprehensive representation of the behaviors that hackers use when they infiltrate networks, it is a useful resource to develop defensive, preventive, and remedial strategies for organizations. See MITRE Corporation.

Audit

A Advanced EPDR operational mode that enables you to view the processes run on the protected network without taking any remedial action (disinfect or block).

Automatic assignment of settings

See Inheritance.

B

Backup

Storage area for non-disinfectable malicious files, as well as the spyware items and hacking tools detected on your network. All programs classified as threats and removed from the system are temporarily moved to the backup/quarantine area for a period of 7/30 days based on their type.

Behavior change

Advanced EPDR can behave in two ways when an unknown item that was allowed by the administrator is finally classified as goodware or malware: Delete it from the list of allowed threats: If the item is classified as goodware it will continue to run. However, if it is classified as malware, it will be prevented from running. Keep it on the list of allowed threats: The item will be allowed to run regardless of whether it is malware or goodware.

BitLocker

Software installed on certain versions of Windows 7 and above computers and designed to encrypt and decrypt the data stored on computer volumes. This software is used by Cytomic Encryption.

Block

Action performed by Advanced EPDR to prevent programs installed on the user's computer from running due to one of the following reasons: The program is classified as a threat. The program is unknown to Advanced EPDR, the advanced protection policy is configured in Lock or Hardening mode, and the program's source is untrusted. The program is blocked by a policy defined by the administrator.

Broadcasting

In computer networking, broadcasting refers to transmitting a packet that will be received by every device on the network simultaneously, without the need to send it individually to each device. Broadcast packets do not go through routers and use different addressing methodology to differentiate them from unicast packets.

Buffer overflow

Anomaly affecting the management of the input buffers of a process. In a buffer overflow, if the size of the data received is greater than the allocated buffer, the redundant data is not discarded, but is written to adjacent memory locations. This may allow attackers to insert arbitrary executable code into the memory of a program on systems prior to Microsoft's implementation of the DEP (Data Execution Prevention) technology.

C

Cache/Repository (role)

Computers that automatically download and store all files required so that other computers with Advanced EPDR installed can update their signature file, agent, and protection engine without having to access the Internet. This saves bandwidth as it is not necessary for each computer to separately download the updates it needs. All updates are downloaded centrally for all computers on the network.

CKC (Cyber Kill Chain)

In 2011, Lockheed-Martin drafted a framework or model for defending computer networks, which stated that cyberattacks occur in phases and each of them can be interrupted through certain controls. Since then, the Cyber Kill Chain (CKC) has been adopted by IT security organizations to define the phases of cyberattacks. These phases range from remote reconnaissance of the target's assets to data exfiltration.

Cloud (Cloud computing)

Cloud computing is a technology that allows services to be offered across the Internet. Consequently, the term 'the cloud' is used as a metaphor for the Internet in IT circles.

Compromised process

A vulnerable process hit by an exploit attack in order to compromise the security of a user's computer.

Computers without a license

Computers whose license has expired or are left without a license because the user has exceeded the maximum number of installations allowed. These computers are not protected, but are shown in the web management console.

CVE (Common Vulnerabilities and Exposures)

List of publicly known cybersecurity vulnerabilities defined and maintained by The MITRE Corporation. Each entry on the list has a unique identifier, enabling CVE to offer a common naming scheme that security tools and human operators can use to exchange information about vulnerabilities with each other.

Cytomic agent

One of the modules included in the Advanced EPDR client software. It manages communications between computers on the network and the Cytomic cloud-based servers, in addition to managing local processes.

Cytomic Data Watch service

A module compatible with Advanced EPDR that finds the PII files stored on an organization's network and monitors access to them in order to ensure compliance with applicable data processing and storage regulations such as the GDPR.

Cytomic Encryption service

A module compatible with Advanced EPDR and designed to encrypt the content of computers' internal storage devices. It aims to minimize the exposure of the data stored by organizations in the

event of loss or theft, or when unformatted storage devices are replaced or withdrawn.

Cytomic Insights service

A real-time, advanced service for leveraging the knowledge generated by the products Advanced EDR and Advanced EPDR. It enables organizations to detect unknown threats, targeted attacks, and APTs, with graphical representations of the activities performed by the processes run by users, emphasizing events related to security and data extraction.

Cytomic Patch service

A module compatible with Advanced EPDR that updates and patches the programs installed on an organization's workstations and servers in order to remove the software vulnerabilities stemming from programming bugs and reduce the attack surface.

Cytomic SIEMConnect service

A module compatible with Advanced EPDR that sends the telemetry generated by the processes run on an organization's workstations and servers to the company's SIEM server.

D

DEP (Data Execution Prevention)

A feature implemented in operating systems to prevent the execution of code from memory pages marked as non-executable. This feature was developed to prevent buffer-overflow exploits.

Device control

Module that enables organizations to define the way protected computers must behave when connecting a removable or mass storage device to them.

DHCP

Service that assigns an IP address to each computer on a network

Dialer

Program that redirects users who connect to the Internet using a modem to a premium-rate number. Premium-rate numbers are telephone numbers for which prices higher than normal are charged.

Discovery computer (role)

Computers capable of finding unmanaged workstations and servers on the network in order to remotely install the Advanced EPDR agent on them.

Disinfectable file

A file infected by malware for which there is an algorithm that can convert the file back to its original state.

DNS (Domain Name System)

Service that translates domain names into different types of information, generally IP addresses.

Domain

Windows network architecture where the management of shared resources, permissions, and users is centralized in a server called a Primary Domain Controller (PDC) or Active Directory (AD).

Dwell time

Length of time that a threat has remained undetected on the network.

E

Entity

Predicate or complement included in the action tables of the forensic analysis module.

Entity (Cytomic Data Watch)

A set of data which, taken as a whole, has its own meaning.

Environment variable

A string consisting of environment information such as a drive, path, or file name, which is associated with a symbolic name that Windows can use. You can use the System applet in the Control Panel or the 'set' command at the command prompt to set environment variables.

EOL (End of Life)

A term used with respect to a product supplied to customers, indicating that the product is in the end of its useful life. After a product reaches its EOL stage, it stops receiving updates or fixes from the relevant vendor, leaving it vulnerable to hacking attacks.

Event

An action executed by a process on the user's computer and monitored by Advanced EPDR. Events are sent to the Cytomic cloud in real time as part of the telemetry. Analysts, threat hunters, and automated machine learning processes analyze them in

context to determine if they could be part of the CKC of a cyberattack. See "CKC (Cyber Kill Chain)".

Exchange Server

Mail server developed by Microsoft. Exchange servers store inbound and/or outbound emails and distribute them to users' email inboxes.

Excluded program

Programs that were initially blocked as they were classified as malware or PUP, but have been selectively and temporarily allowed by the administrator, who excluded them from the scans performed by the solution.

Exploit

Generally speaking, an exploit is a sequence of specially crafted data aimed at causing a controlled error in the execution of a vulnerable program. After the error occurs, the compromised process will mistakenly interpret certain parts of the data sequence as executable code, triggering dangerous actions that may compromise the security of the targeted computer.

F

Filter

A dynamic-type computer container that automatically groups together items that meet the conditions defined by the administrator. Filters simplify the assignment of security settings and facilitate management of all computers on the network.

Filter tree

Collection of filters grouped into folders, used to organize all computers on the network and facilitate the assignment of settings.

Firewall

Technology that blocks the network traffic that matches certain patterns defined in rules established by the administrator. A firewall prevents or limits the communications established by the applications run on computers, reducing the attack surface.

Folder tree

Hierarchical structure consisting of static groups, used to organize all computers on the network and facilitate the assignment of settings.

Forensic analysis

A series of actions and processes carried out by network administrators with special tools in order to track malicious programs and assess the consequences of an infection.

FQDN (Fully Qualified Domain Name)

A fully qualified domain name (FQDN) is a domain name that specifies the exact location of a host within the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain and the root zone.

Fragmentation

On data transmission networks, when the MTU of the underlying protocol is not sufficient to accommodate the size of the transmitted packet, routers divide the packet into smaller segments

(fragments) which are routed independently and assembled in the right order at the destination.

G

GDPR (General Data Protection Regulation)

A regulation that governs the protection of the personal data of all individuals within the European Union (EU). See the following link: http://www.privacy-regulation.eu/en/index.htm for the full regulation.

Geolocation

Geographical positioning of a device on a map from its coordinates.

Goodware

A file which, after analysis, has been classified as legitimate and safe.

Group

Static container that groups one or more computers on the network. Computers are assigned to groups manually. Groups simplify the assignment of security settings and facilitate management of all computers on the network.

H

Hacking tool

Programs used by hackers to perform actions that cause problems for the user of the affected computer (control the computer, steal confidential information, scan communication ports, etc.).

Hardening

A Advanced EPDR operational mode that blocks programs classified as malware and unknown files coming from an untrusted source: The Internet. External storage drives. Other computers on the customer's network.

Heap Spraying

Heap Spraying is a technique used to facilitate the exploitation of software vulnerabilities by malicious processes. As operating systems improve, the success of vulnerability exploit attacks has become increasingly random. In this context, heap sprays take advantage of the fact that, on most architectures and operating systems, the start location of large heap allocations is predictable and consecutive allocations are roughly sequential. This enables attackers to insert and later run arbitrary code in the target system's heap memory space. This technique is widely used to exploit vulnerabilities in web browsers and web browser plug-ins.

Heuristic scanning

Static scanning that employs a set of techniques to statically inspect potentially dangerous files. It examines hundreds of characteristics of a file to determine the likelihood that it may take malicious or harmful actions when run on a user's computer.

Hoaxes

Spoof messages, normally emails, warning of viruses/threats which do not really exist.

I

ICMP (Internet Control Message Protocol)

Error notification and monitoring protocol used by the IP protocol on the Internet.

Identifier

Keyword used in the Cytomic Data Watch searches and which allows an entity type to be selected.

IDP (Identity Provider)

Centralized service for managing user identity verification.

IFilter

A plug-in that allows Microsoft's search engines to index various file formats so that they become searchable.

Incident

Message relating to the Advanced EPDR advanced protection that may require administrator intervention. Incidents are reported to the administrator through the management console or email (alerts), and to users through pop-up messages generated by the agent and displayed locally on the protected device.

Indexing

A process that parses the content of files and stores it in a quick-access database to speed up searching processes.

Indicator

The detection of an anomalous chain of actions of the processes running on customers' computers. These are sequences of unusual

actions that are analyzed in detail to determine whether or not they belong to a cyberattack. See “CKC (Cyber Kill Chain)”.

Indicator of attack (IOA)

This is an indicator with a high probability of representing a cyberattack. These are generally attacks in early stages or in exploit phase. These attacks do not generally use malware, as attackers commonly take advantage of legitimate operating system tools to perform the attack and hide their activity. See Indicator.

Indirect assignment of settings

See Inheritance.

Infection vector

The means used by malware to infect users’ computers. The most common infection vectors are web browsing, email, and pen drives.

Inheritance

A method for automatically assigning settings to all subsets of a larger, parent group, saving management time. Also referred to as 'automatic assignment of settings' or 'indirect assignment of settings.'

Inventory

Database kept by which contains the files classified as PII found across the network.

IP (Internet Protocol)

Principal Internet communications protocol for sending and receiving datagrams generated at the underlying link level.

IP address

Number that identifies a device interface (usually a computer) logically and hierarchically on a network that uses the IP protocol.

Item reclassification

See Behavior change.

J

Joke

These are not viruses, but tricks that aim to make users believe they have been infected by a virus.

L

Linux distribution

Set of software packets and libraries that make up an operating system based on the Linux kernel.

Lock

A operational mode that blocks unknown programs as well as all files classified as malware.

M

MAC address

48-bit hexadecimal number that uniquely identifies a network card or interface.

Machine learning

This is a branch of artificial intelligence whose aim is to develop technologies capable of predicting behaviors from unstructured

data delivered in the form of examples.

Malware

This term is used to refer to all programs that contain malicious code (MALicious softWARE), whether it is a virus, a Trojan, a worm, or any other threat to the security of IT systems. Malware tries to infiltrate or damage computers, often without users knowing, for a variety of reasons.

Malware Freezer

A feature of the quarantine/backup module whose goal is to prevent data loss due to false positives. All files classified as malware or suspicious are sent to the quarantine/backup area, thereby avoiding deleting and losing data if the classification is wrong.

Malware lifecycle

Breakdown of all the actions unleashed by a malicious program from the time it is first seen on a customer's computer until it is classified as malware and disinfected.

Manual assignment of settings

Direct assignment of a set of settings to a group, as opposed to the automatic or indirect assignment of settings, which uses the inheritance feature to assign settings without administrator intervention.

MD5 (Message-Digest Algorithm 5)

A cryptographic hash function producing a 128-bit value that represents data input. The MD5 hash value calculated for a file is used to identify it unequivocally or check that it has not been tampered with.

Microsoft Filter Pack

IFilter library package that covers all file formats generated with the Microsoft Office suite.

MITRE Corporation

A not-for-profit company that operates several federally-funded R&D centers dedicated to addressing security issues. It offers practical solutions in the fields of defense and intelligence, aviation, civil systems, national security, judiciary, health, and cybersecurity. It is the creator of the ATT&CK framework. See ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

MTU (Maximum Transmission Unit)

Maximum packet size (in bytes) an underlying protocol can transmit.

N

Network adapter

Hardware that allows communication among different computers connected through a data network. A computer can have more than one network adapter installed and is identified in the system through a unique identifier.

Network topology

Physical or logical map of network nodes.

Normalization

In Cytomic Data Watch, normalization is a task that is part of the text indexing process. It consists of removing all unnecessary characters

(typically separator characters and delimiters), before storing them in a database.

O

OU (Organizational Unit)

Hierarchical method for classifying and grouping objects stored in directories.

P

Partner

A company that offers Cytomic products and services.

Passphrase

Also known as enhanced PIN or extended PIN, a passphrase is a PIN that incorporates alphanumeric and non-alphanumeric characters. A passphrase supports lowercase and uppercase letters, numbers, spaces, and symbols.

Patch

Small programs published by software vendors to fix their software and add new features.

Payload

In the IT and telecommunications sectors, a message payload is the set of useful transmitted data (as opposed to other data that is also sent to facilitate message delivery: header, metadata, control information, etc.).

PDC (Primary Domain Controller)

This is the role of a server on Microsoft domain networks, which centrally manages the assignment and validation of user credentials for accessing network resources. Active Directory currently exercises this function.

Phishing

A technique for obtaining confidential information from users fraudulently. The targeted information includes passwords, credit card numbers, and bank account details.

PII (Personally Identifiable Information)

Information that can be used to identify or locate an individual.

PIN (Personal Identification Number)

The PIN (Personal Identification Number) is a sequence of 8 to 20 numbers that serves as a simple password and is necessary to start a computer with an encrypted drive. Without the PIN, the boot sequence is not completed and it is impossible to access the computer.

Port

Unique ID number assigned to a data channel opened by a process on a device through which data is exchanged (inbound/outbound) with an external source.

Potentially Unwanted Program (PUP)

A program that may be unwanted, despite the possibility that users consented to download it. Potentially unwanted programs are often downloaded inadvertently along with other programs.

Protection (module)

One of the two components of the Advanced EPDR software which is installed on computers. It contains the technologies responsible for protecting the IT network, and the remediation tools used to disinfect compromised computers and assess the scope of the intrusion attempts detected on the customer's network.

Protocol

System of rules and specifications in telecommunications that allows two or more computers to communicate. One of the most commonly used protocols is TCP-IP.

Proxy

Software that acts as an intermediary for the communication established between two computers: a client on an internal network (an intranet, for example) and a server on an extranet or the Internet.

Proxy (role)

A computer that acts as a gateway to allow workstations and servers without direct Internet access to connect to the cloud.

Public network

Networks in public places such as airports, coffee shops, etc. These networks require that you establish some limitations regarding computer visibility and usage, especially with regard to file, directory, and resource sharing.

Q

QR (Quick Response) code

A matrix of dots that efficiently stores data.

Quarantine

See Backup.

R

Recovery key

If an anomalous situation is detected on a computer protected with Advanced EPDR, or you forget the unlock key, the system will request a 48-digit recovery key. This password is managed from the management console and must be entered in order to complete the startup process. Each encrypted volume has its own unique recovery key.

RIR (Regional Internet Registry)

An organization that manages the allocation and registration of IP addresses and Autonomous Systems (AS) within a particular region of the world.

Role

Specific permission configuration applied to one or more user accounts and which authorizes users to view and edit certain resources of the console.

Rootkit

A program designed to hide objects such as processes, files, or Windows registry entries (often including its own). This type of

software is used by attackers to hide evidence and utilities on previously compromised systems.

ROP

Return-oriented programming (ROP) is a computer security exploit technique that enables attackers to run arbitrary code in the presence of protection technologies such as DEP and ASLR. Traditional stack buffer overflow attacks occurred when a program wrote to a memory address on the program's call stack outside of the intended data structure, which is usually a fixed-length buffer. However, those attacks were rendered ineffective when techniques such as DEP were massively incorporated into operation systems. These techniques prevent the execution of code in regions marked as non-executable. In a ROP attack, the attacker gains control of the call stack to hijack program control flow and then executes carefully chosen machine instruction sequences that are already present in the machine's memory, called 'gadgets'. Chained together, these gadgets enable the attacker to perform arbitrary operations on the targeted machine.

RWD (Responsive Web Design)

A set of techniques that enable the development of web pages that automatically adapt to the size and resolution of the device being used to view them.

S

SCL (Spam Confidence Level)

Normalized value assigned to a message that indicates the likelihood that the message is spam, based on its characteristics

(content, headers, etc.)

Settings

See Settings profile.

Settings profile

Specific settings governing the protection or any other aspect of the managed computer. Profiles are assigned to a group or groups and then applied to all computers that make up the group.

SIEM (Security Information and Event Management)

Software that provides storage and real-time analysis of the alerts generated by network devices.

Signature file

File that contains the patterns used by the antivirus to detect threats.

SMTP server

Server that uses SMTP (Simple Mail Transfer Protocol) to exchange email messages between computers.

Spam

This term refers to unsolicited email messages that usually contain advertising and are generally sent out massively. Spam can have a range of negative effects on the recipient.

Spyware

A program that is automatically installed with another (usually without the user's permission and even without the user realizing), and collects personal data.

SSL (Secure Sockets Layer)

Cryptographic protocol for the secure transmission of data sent over the Internet.

Suspicious item

A program with a high probability of being malware and classified by our heuristic scanner. This type of technology is only used in the scheduled and on-demand scans launched from the Tasks module, never in real-time scans. Heuristic scanning is used to compensate for the lower detection capability of scheduled scan tasks, in which program code is scanned statically, without running the program. See Heuristic scanning.

SYN

Flag in the TOS (Type Of Service) field of TCP packets that identifies them as connection start packets.

System partition

Area of the hard disk that remains unencrypted and which is necessary for computers with Cytomic Encryption enabled to start up properly.

T

Tactic

In ATT&CK terminology, tactics represent the ultimate motive or goal of a technique. It is the adversary's tactical objective: the reason for taking an action. See ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

Task

Set of actions scheduled for execution at a configured frequency during a specific period of time.

TCO (Total Cost of Ownership)

Financial estimate of the total direct and indirect costs of owning a product or system.

TCP (Transmission Control Protocol)

The main transport-layer Internet protocol, aimed at connections for exchanging IP packets.

Technique

In ATT&CK terminology, the techniques represent the way (or the strategy) that an adversary achieves a tactical objective. In other words, 'how'. For example, an adversary, in order to achieve the objective of accessing credentials (tactic), executes a dump of the data (technique). See ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

Threat hunting

A set of specialized technologies and human resources that allows lateral movements and other early indicators of malware activity to be detected, before they can take harmful actions against corporate security.

TLS (Transport Layer Security)

New version of protocol SSL 3.0.

TPM (Trusted Platform Module)

The TPM is a chip that is part of the motherboard of desktops, laptops, and servers. Its main aim is to protect users' sensitive data, stored passwords, and other information used in login processes. The TPM is also responsible for detecting changes in the chain of startup events on a computer, for example preventing access to a hard drive from a computer other than the one used for its encryption.

Trojans

Programs that reach computers disguised as harmless software to install themselves on computers and carry out actions that compromise user confidentiality.

Trusted network

Networks in private places such as offices and households. Connected computers are generally visible to the other computers on the network, and there is no need to establish limitations on file, directory, and resource sharing.

U

UDP (User Datagram Protocol)

A transport-layer protocol which is unreliable and unsuited for connections for exchanging IP packets.

Unblocked program

Program blocked during the classification process but temporarily and selectively allowed by the administrator to avoid disrupting user activity.

USB key

A device used on computers with encrypted volumes and which allows the recovery key to be stored on a portable USB drive. With a USB key, it is not necessary to enter a password to start up the computer. However, the USB device with the startup password must be plugged into the computer's USB port.

User (console)

Information set used by Advanced EPDR to regulate administrator access to the web console and establish the actions that administrators can take on the computers on the network.

User (network)

A company's worker using computing devices to do their job.

User account

See User (console).

V

VDI (Virtual Desktop Infrastructure)

Desktop virtualization solution that hosts virtual machines in a data center accessed by users from a remote terminal with the aim to centralize and simplify management and reduce maintenance costs. There are two types of VDI environments: Persistent VDIs: The storage space assigned to each user persists between restarts, including the installed software, data, and operating system updates. Non-persistent VDIs: The storage space assigned to each user is deleted when the VDI instance is restarted, returning to its initial state and undoing all changes made.

Virus

Programs that enter computers and IT systems in a number of ways, causing effects that range from simply annoying to highly destructive and irreparable.

VPN (Virtual Private Network)

Network technology that allows private networks (LAN) to interconnect across a public medium, such as the Internet.

Vulnerable process

A program which, due to a programming bug, cannot interpret certain input data correctly. Hackers take advantage of specially crafted data packets (exploits) to cause vulnerable processes to malfunction and run malicious code designed to compromise the security of the target computer.

W

Web access control

Technology that enables organizations to control and filter the URLs requested by the network's Internet browsers in order to allow or deny access to them, taking as reference a URL database divided into content categories.

Web console

Tool to manage the advanced security service Advanced EPDR, accessible anywhere, anytime through a supported Internet browser. The web console enables administrators to deploy the security software, push security settings, and view the protection status. It also provides access to a set of forensic analysis tools to assess the scope of security problems.

Widget (Panel)

Panel containing a configurable graph representing a particular aspect of network security. The Advanced EPDR dashboard is made up of different widgets.

Window of opportunity

The time it takes between when the first computer in the world is infected with a new malware specimen and its analysis and inclusion by antivirus companies in their signature files to protect computers from infections. This is the period when malware can infect computers without antivirus software being aware of its existence.

Workgroup

Windows network architecture where shared resources, permissions, and users are managed independently on each computer.

Z

Zero-Trust Application Service service

A service included in the basic license which classifies 100 percent of the processes run on the organization's workstations and servers, identifying them accurately as goodware or malware without false positives or false negatives.