



Aviso legal

Ni los documentos ni los programas a los que usted pueda acceder pueden ser copiados, reproducidos, traducidos o transferidos por cualquier medio electrónico o legible sin el permiso previo y por escrito de Cytomic (Unidad de Negocio de Panda Security), Santiago de Compostela, 12, 48003 Bilbao (Bizkaia), ESPAÑA.

Marcas registradas.

Windows Vista y el logotipo de Windows son marcas o marcas registradas de Microsoft Corporation en los Estados Unidos y otros países. Todos los demás nombres de productos pueden ser marcas registradas de sus respectivas compañías.

© Cytomic 2025(Unidad de Negocio de Panda Security). Todos los derechos reservados

Información de contacto.

Oficinas centrales:

Cytomic (Unidad de Negocio de Panda Security)

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 España.

<https://www.pandasecurity.com/spain/about/contact/>

Versión: 4.50.00

Autor: Cytomic

Fecha: 4/22/2025

Acerca de la Guía de administración de Advanced EDR

Para obtener la versión más reciente de la documentación en formato PDF consulta la dirección web:

<https://info.cytomicmodel.com/resources/guides/EDR/latest/es/EDR-guia-ES.pdf>

Para consultar un tema específico, accede a la ayuda web del producto disponible en:

<https://info.cytomicmodel.com/resources/help/EDR/latest/es/index.htm>

Información sobre las novedades de la versión

Para conocer las novedades de la última versión de Advanced EDR consulta la siguiente URL:

<https://info.cytomicmodel.com/releasenotes/?product=EDR&lang=es>

Documentación técnica no incluida en esta Guía de administración para módulos y servicios compatibles con Advanced EDR

Para acceder a la Guía del usuario para Cytomic Insights consulta la siguiente URL:

<https://info.cytomicmodel.com/resources/guides/Insights/es/INSIGHTS-guia-ES.pdf>

Para acceder a la Guía para el usuario de Cytomic Data Watch consulta la siguiente URL:

<https://info.cytomicmodel.com/resources/guides/DataWatch/es/DATAWATCH-guia-ES.pdf>

Para acceder a las guías de Cytomic SIEMConnect consulta las siguientes URLs:

<https://info.cytomicmodel.com/resources/guides/SIEMConnect/es/SIEMCONNECT-Manual-ES.pdf>

<https://info.cytomicmodel.com/resources/guides/SIEMConnect/es/SIEMCONNECT-ManualDescripcionEventos-ES.pdf>

Soporte técnico

Cytomic ofrece un soporte técnico global cuyo objetivo principal es responder a cuestiones específicas sobre el funcionamiento de sus productos. El equipo de soporte técnico también genera documentación sobre detalles técnicos del producto, que ofrece a través de su portal eKnowledge Base.

Para acceder a información específica del producto consulta la siguiente URL:

<https://www.cytomic.ai/es/soporte/edr/>

Para acceder al portal eKnowledge Base consulta la siguiente URL:

<https://www.cytomic.ai/es/soporte/>

Encuesta sobre la Guía de administración de Advanced EDR

Evalúa esta Guía de administración y envíanos sugerencias y peticiones para próximas versiones de la documentación en:

<https://es.surveymonkey.com/r/feedbackEDRGuideES>

Tabla de contenidos

Tabla de contenidos	4
Prólogo	17
¿A quién está dirigida esta Guía de administración?	17
¿Qué es Advanced EDR?	17
Iconos	18
Información básica de Advanced EDR	19
Beneficios de Advanced EDR	19
Características de Advanced EDR	20
Características de la plataforma Cytomic	21
Principales beneficios de Cytomic	21
Arquitectura de Cytomic	23
Cytomic en los equipos de usuario	24
Componentes principales	25
Servicios Advanced EDR	28
Perfil de usuario del producto	32
Dispositivos e idiomas soportados	32
La consola de administración	35
Beneficios de la consola web	36
Acceso a la consola web y requisitos	36
Requisitos para acceder a la consola web	36
Acceso la consola web	37
Estructura general de la consola web	37
Menú superior (1)	38
Menú lateral (2)	42
Panel central (3)	42
Acceso a Cytomic Insights (4)	42
Elementos básicos de la consola web	42
Esquema general de la zona Estado	45
Gestión de listados	47
Plantillas, configuraciones y vistas	48

Secciones de los listados	52
Operaciones con listados	54
Listados incluidos por defecto	57
Acceso, control y supervisión de la consola de administración	59
Conceptos generales	60
Gestión de cuentas de usuario	60
Crear la primera cuenta de usuario	61
Crear cuentas de usuario sucesivas	62
Cambiar los datos personales de una cuenta de usuario	63
Cambiar la dirección de correo o la contraseña de una cuenta de usuario	63
Borrar o bloquear cuentas de usuarios	64
Activar la verificación en dos pasos	64
Listado de usuarios	65
Gestión de roles y permisos	67
Conceptos básicos	67
Crear un rol	69
Borrar un rol	70
Copiar un rol	70
Modificar un rol	70
Descripción de los permisos implementados	70
Registro de la actividad de las cuentas de usuario	80
Registro de sesiones	80
Registro de acciones de usuario	81
Eventos del sistema	96
Instalación del software cliente	99
Instalación en sistemas Windows	100
Visión general del despliegue de la protección	100
Requisitos de instalación	103
Generar el paquete de instalación y despliegue manual	104
Instalación del paquete descargado	106
Integración de equipos según su dirección IP	107
Instalar con herramientas centralizadas	108
Instalar mediante generación de imágenes gold	110
Descubrimiento de equipos e instalación remota del software cliente	117
Visualizar equipos descubiertos	121
Detalle de los equipos descubiertos	125
Borrar y ocultar equipos	129

Instalación remota del software cliente	130
Instalación en sistemas Linux	133
Visión general del despliegue de la protección	133
Requisitos de instalación	134
Generar el paquete de instalación y despliegue manual	136
Instalación en plataformas Linux	137
Instalación en sistemas macOS	141
Visión general del despliegue de la protección	141
Requisitos de instalación	143
Despliegue manual del agente macOS	144
Instalación del paquete descargado	145
Comprobar el despliegue	145
Eliminación automática de equipos	148
Desinstalar el software	150
Desinstalación manual	150
Desinstalación desde la consola de administración	152
Reinstalación remota	153
Licencias	157
Definiciones y conceptos clave	158
Mantenimientos	158
Estado de los equipos	158
Estado de las licencias y grupos	158
Tipos de licencias	159
Asignar licencias	159
Liberar licencias	160
Procesos asociados a la asignación de licencias	160
Caso I: Equipos con licencia asignada y equipos excluidos	160
Caso II: Equipos sin licencia asignada	161
Paneles / widgets del módulo licencias	162
Listados del módulo Licencias	164
Licencias caducadas	167
Comportamiento de los productos basados en Cytomic al caducar sus licencias	167
Comportamiento cuando caduca uno de los mantenimientos contratados	168
Comportamiento de Advanced EDR tras caducar todas las licencias	169
Renovar antes de 90 días tras caducar las licencias	169
Renovar tras más de 90 días desde la caducidad de las licencias	169
Mensajes de caducidad próxima y vencida	169

Buscar equipos según su estado de licencia	170
Actualización del producto	171
Módulos actualizables en el software cliente	171
Actualización del motor de protección	172
Actualizaciones	173
Actualización del agente de comunicaciones	174
Actualizaciones del conocimiento	175
Dispositivos Windows, Linux y macOS	175
Actualización de la consola de administración	175
Consideraciones previas para actualizar la versión de la consola	175
Gestión de equipos y dispositivos	177
La zona equipos	178
El panel Árbol de equipos	179
Árbol de filtros	180
Definición de filtro	180
Filtros predefinidos	180
Crear y organizar filtros	182
Configurar filtros	184
Casos de uso comunes	185
Árbol de grupos	188
Crear y organizar grupos	190
Mover equipos entre grupos	192
Filtrar resultados por grupos	193
Filtrar grupos	194
Listados disponibles para gestionar equipos	194
Listado de equipos	194
El panel Mis listados	208
Información de equipo	218
Sección general (1)	219
Sección alertas de equipo (2)	220
Sección Detalles (3)	230
Sección Detecciones (4) en Windows, Linux y macOS	238
Sección Investigación (5)	238
Conexiones monitorizadas (6)	243
Sección Hardware (7)	244
Sección Software (8)	245
Sección Configuración (9)	247

Barra de acciones (10)	247
Iconos ocultos (11)	249
Gestión de configuraciones	251
Estrategias para crear la estructura de configuraciones	252
Visión general para asignar configuraciones a equipos	252
Introducción a las clases de configuraciones	253
Perfiles de configuración modulares vs monolíticos	256
Crear y gestionar configuraciones	258
Asignación manual y automática de configuraciones	261
Asignación directa / manual de configuraciones	261
Asignación indirecta de configuraciones: las dos reglas de la herencia	263
Límites de la herencia	264
Sobre-escritura de configuraciones	265
Movimiento de grupos y equipos	267
Excepciones a la herencia indirecta	268
Configuraciones recibidas desde el partner	268
Características de las configuraciones enviadas por el partner	269
Requisitos	269
Visualizar las configuraciones asignadas	269
Configuración remota del agente	271
Configuración de los roles del agente Cytomic	272
Rol de Proxy Cytomic	272
Rol de caché	274
Rol de descubridor	276
Configuración de listas de acceso a través de proxy	277
Configuración de las descargas mediante equipos caché	279
Requisitos para usar un equipo con el rol de caché asignado	279
Configuración de la comunicación en tiempo real	281
Configuración del idioma del agente	281
Configuración de la visibilidad del agente	282
Control de acceso a redes	282
Requisitos	283
Comprobación de los requisitos	284
Acceso a la configuración de Control de acceso a redes	284
Configurar la seguridad frente a manipulaciones no deseadas de las protecciones	285
Activar verificación en dos pasos (2FA)	286

Excepciones al copiar perfiles con configuraciones de tipo Seguridad frente a manipulaciones no deseadas de las protecciones	288
Configuración de Shadow Copies	289
Acceso a la funcionalidad de Shadow Copies	290
Configuración de la seguridad en estaciones y servidores	291
Acceso a la configuración y permisos necesarios	292
Introducción a la configuración de la seguridad	292
Configuración General	293
Alertas en los equipos	293
Actualizaciones	294
Desinstalar otros productos de seguridad	294
Archivos y rutas excluidas del análisis	294
Protección avanzada	296
Funcionalidades según el sistema operativo	296
Comportamiento	297
Tecnología AMSI (Anti-Malware Scan Interface)	299
Políticas avanzadas de seguridad	299
Anti-exploit	302
Protección contra ataques de red	305
Privacidad	305
Uso de la red	305
Modo auditoría	306
Visualizar los equipos en modo auditoría	306
Modo detallado	306
Requisitos y limitaciones del modo detallado	307
Activar y desactivar el modo detallado	307
Visualizar los equipos en modo detallado	309
Cytopic Data Watch (Supervisión de información sensible)	311
Introducción al funcionamiento de Cytopic Data Watch	312
Requisitos de Cytopic Data Watch	315
Plataformas soportadas	315
Instalación del componente Microsoft Filter Pack	315
El proceso de indexación	315
Inventario de ficheros PII	316
Monitorización continua de ficheros	317
Búsqueda de ficheros	317
Propiedades y requisitos de las búsquedas	318

Crear una búsqueda	321
Búsquedas almacenadas	322
Visualizar los resultados de una búsqueda	323
Sintaxis de las búsquedas	325
Búsqueda de ficheros duplicados	328
Borrado y restauración de ficheros	329
Borrar ficheros de los equipos de la red	329
Restaurar ficheros previamente borrados por el administrador	331
Configuración de Cytomic Data Watch	332
Requisitos para buscar y seguir documentos Microsoft Office	333
Información personal (inventario, búsquedas y seguimiento)	333
Monitorización de archivos por reglas	333
Opciones avanzadas de indexación	336
Escritura en unidades de almacenamiento extraíbles	337
Paneles / widgets del módulo Cytomic Data Watch	337
Listados del módulo Cytomic Data Watch	350
Extensiones de programas soportadas	370
Empaquetadores y algoritmos de compresión soportados	372
Entidades y países soportados	373
Cytomic Patch(Actualización de programas vulnerables)	375
Funcionalidades de Cytomic Patch	376
Requisitos mínimos de Cytomic Patch	378
Flujo general de trabajo	380
Comprobar que Cytomic Patch funciona correctamente	380
Comprobar que los parches publicados están instalados	381
Aislar los equipos con vulnerabilidades conocidas sin parchear	382
Descargar e instalar parches	382
Descargar los parches de forma manual	390
Desinstalar los parches defectuosos	393
Comprobar el resultado de las tareas de instalación / desinstalación de parches	394
Excluir parches en todos o en algunos equipos	394
Comprobar que los programas no han entrado en EoL	395
Comprobar el histórico de instalaciones de parches y actualizaciones	395
Comprobar el nivel de parcheo de los equipos con incidencias	396
Configuración del descubrimiento de parches sin aplicar	396
Configuración general	397
Instalación de parches	397

Frecuencia de la búsqueda	398
Criticidad de los parches	398
Paneles/widgets en Cytomic Patch	398
Listados del módulo Cytomic Patch	416
Configuración de Control de Acceso a Endpoints	458
Configuración de Control de Acceso a Endpoints	459
Opciones de configuración de Control de Acceso a Endpoints	459
Mapa de conexiones	462
Estructura del mapa de conexiones	463
Navegación por el mapa de conexiones	464
Configuración del mapa de conexiones	464
Paneles/widgets de Control de Acceso a Endpoints	466
Listados del módulo Control de Acceso a Endpoints	472
Cytomic Encryption(Cifrado de dispositivos)	481
Introducción a los conceptos de cifrado	482
Visión general del servicio de Cytomic Encryption	485
Características generales de Cytomic Encryption	486
Requisitos mínimos de Cytomic Encryption	487
Gestión de equipos según su estado de cifrado previo	488
Proceso de cifrado y descifrado en Windows	488
Comportamiento de Cytomic Encryption ante errores	494
Proceso para obtener la clave de recuperación	494
Obtener el identificador de volumen cifrado (Windows)	495
Obtener el identificador de la clave de recuperación asociada al equipo (macOS)	497
Obtener la clave de recuperación	497
Buscar la clave de recuperación	497
Paneles / widgets del módulo Cytomic Encryption	499
Listados en Cytomic Encryption	506
Configuración del cifrado	513
Opciones de configuración de Cytomic Encryption	514
Filtros disponibles	515
Configuración del bloqueo de programas	517
Configuración de Bloqueo de programas	518
Opciones de configuración de Bloqueo de programas	518
Listados del módulo Bloqueo de programas	519
Paneles / widgets del módulo Bloqueo de programas	522

Configuración de software autorizado	525
Software autorizado y exclusiones de elementos	526
Configuración de Software autorizado	527
Opciones de configuración del módulo Software autorizado	527
Gestión y detección de IOCs	531
Conceptos de IOCs	532
Flujo de trabajo general con IOCs	533
Gestión de IOCs	533
Galería de IOCs	534
Crear un nuevo IOC	535
Copiar un IOC	536
Borrar IOCs	536
Importar y exportar IOCs	537
Visualizar IOCs importados	538
Búsqueda de IOCs en la red	540
Configurar una tarea de búsqueda de IOCs	540
Listados de IOCs encontrados	543
IOCs encontrados por cada tarea	544
IOCs detectados	546
Paneles / widgets de IOCs	550
Últimas tareas de búsqueda de IOCs	550
IOCs más detectados	551
Evolución de los IOCs detectados	552
Configuración de indicadores de ataque	553
Introducción a los conceptos de IOAs	554
Gestión de detecciones de indicadores de ataque	559
Mostrar las detecciones de IOAs en el parque	560
Buscar los equipos con detecciones de un tipo de IOA	560
Buscar las detecciones de IOAs en un equipo	560
Buscar equipos y detecciones de IOAs relacionados	560
Archivar una o varias detecciones de IOAs	561
Marcar detecciones de IOAs como pendientes	561
Mostrar el detalle de una detección de IOA y las recomendaciones	562
Detección y protección frente ataques RDP	562
Configuración de Indicadores de ataque (IOA)	566
Listados del módulo Indicadores de ataque (IOA)	569
Acceso a los listados	569

Permisos requeridos	569
Indicadores de ataque (IOA)	569
Diagramas de grafos	580
Configuración del diagrama de grafos	581
Información contenida en diagramas de grafos	589
Paneles / widgets del módulo Indicadores de ataque	592
Configuración del servicio MDR	603
Configuración del servicio MDR	604
Opciones de configuración de MDR	604
Visibilidad del malware y del parque informático	607
Paneles/Widgets del módulo de seguridad	608
Listados del módulo de seguridad	621
Evaluación de riesgos	645
Configuración de la evaluación de riesgos	646
Listados del módulo Evaluación de riesgos	651
Listado Riesgos	656
Paneles/widgets del módulo Evaluación de riesgos	659
Evaluación de vulnerabilidades	667
Requisitos de la evaluación de vulnerabilidades	668
Configuración de Evaluación de vulnerabilidades	669
Configuración general	670
Frecuencia de la búsqueda	670
Criticidad de los parches	670
Paneles/widgets de Evaluación de vulnerabilidades	671
Listados del módulo Evaluación de vulnerabilidades	686
Gestión de amenazas, elementos en clasificación y cuarentena	701
Introducción a las herramientas de gestión de amenazas	702
Permitir y volver a impedir la ejecución de elementos	705
Información de elementos bloqueados en clasificación	710
Listado de amenazas y programas desconocidos permitidos	723
Política de reclasificación	732
Cambiar la política de reclasificación	733
Trazabilidad de las reclasificaciones	734
Estrategias para supervisar la clasificación de ficheros	735
Gestión de la zona de backup / cuarentena	736
Análisis forense	739

Detalle de los programas bloqueados	740
Detección del malware y PUP	740
Detección exploit	743
Detalles del driver	746
Bloqueo por política avanzada de seguridad	748
Acceso a la ventana Bloqueo por política avanzada de seguridad	748
Bloqueo de programas desconocidos en clasificación e Historial de programas bloqueados	750
Tablas de acciones	754
Grafos de ejecución	759
Ficheros exportados Excel	764
Interpretación de las tablas de acciones y grafos	768
Alertas	775
Alertas por correo	775
Envío programado de informes y listados	785
Características de los informes	785
Tipos de informes	786
Requisitos para generar informes	787
Acceso al envío de informes y listados	787
Gestión de informes	788
Configuración de los informes y listados	789
Contenido de los informes y listados	792
Listados	792
Listados de dispositivos	793
Informe ejecutivo	793
Herramientas de resolución	797
Análisis y desinfección automática de equipos	798
Análisis y desinfección bajo demanda de equipos	799
Listados generados por tareas de análisis	800
Listado Resultados tarea de análisis	801
Listado Ver detecciones	802
Reiniciar equipos	803
Aislar un equipo	804
Estados de los equipos aislados	804
Aislar uno o varios equipos de la red de la organización	805
Quitar el aislamiento de un equipo	805
Opciones avanzadas	806

Comunicaciones permitidas y denegadas de un equipo aislado	806
Control remoto de los equipos	807
Herramientas de acceso remoto incluidas en Advanced EDR	808
Permisos requeridos	808
Requisitos	808
Configuración de control remoto	809
Acceso a la funcionalidad de control remoto	810
Descripción de las herramientas de control remoto	811
Notificar un problema	821
Permitir el acceso externo a la consola Web	822
Eliminar el ransomware y recuperar el estado anterior	822
Tareas	825
Introducción al sistema de tareas	825
Crear tareas desde la zona Tareas	827
Publicar tareas	830
Listado de tareas	830
Gestionar tareas	832
Resultados de una tarea	836
Ajuste automático de los destinatarios de una tarea	838
Funcionalidades del producto y requisitos	841
Funcionalidades por plataforma	841
Funcionalidades del producto y requisitos	847
Funcionalidades por plataforma	847
Requisitos de plataformas Windows	852
Sistemas operativos soportados	852
Requisitos hardware	853
Otros requisitos	854
Requisitos de plataformas macOS	856
Requisitos de plataformas Linux	859
Distribuciones soportadas	859
Versiones del kernel soportadas.	860
Gestores de ficheros soportados	860
Requisitos hardware	860
Kernels soportados	861
Puertos locales y acceso a URLs	862
Puertos locales	862
Acceso a la consola web	863

Acceso a URLs del servicio	863
Acceso a URLs para la descarga de parches y actualizaciones (Cytomic Patch)	865
Formato de los eventos recogidos en la telemetría	867
Glosario	869

Capítulo 1

Prólogo

La Guía de administración contiene información básica y procedimientos de uso para obtener el máximo beneficio del producto Advanced EDR.

Contenido del capítulo

¿A quién está dirigida esta Guía de administración?	17
¿Qué es Advanced EDR?	17
Iconos	18

¿A quién está dirigida esta Guía de administración?

Esta documentación está dirigida a los administradores de red que gestionan la seguridad informática de su organización.

Para interpretar correctamente la información ofrecida por el producto y extraer conclusiones que ayuden a fortalecer la seguridad de su empresa son necesarios conocimientos técnicos sobre entornos Windows a nivel de procesos, sistema de ficheros y registro, así como entender los protocolos de red utilizados con mayor frecuencia.

¿Qué es Advanced EDR?

Advanced EDR es un servicio gestionado que protege los equipos informáticos de las empresas, acota el alcance de los problemas de seguridad encontrados y ayuda a establecer planes de respuesta y prevención frente a las amenazas desconocidas y a los ataques dirigidos avanzados (APTs).

Advanced EDR está dividido en dos áreas funcionales bien diferenciadas:

- Advanced EDR
- Plataforma Cytomic

Advanced EDR

Es el producto que implementa todas las características orientadas a garantizar la seguridad de los puestos de usuario y servidores, sin requerir la intervención del administrador de la red.

Plataforma Cytomic

Es el ecosistema donde se ejecutan los productos de Cytomic. Cytomic entrega en tiempo real, de forma ordenada y con un gran nivel de detalle toda la información generada por Advanced EDR sobre los procesos, los programas ejecutados por los usuarios y los dispositivos que pertenecen a la infraestructura IT de las organizaciones.

Cytomic es una plataforma eficiente, extensible y escalable, diseñada para cubrir las necesidades de la gran cuenta y de MSPs.

Iconos

En esta Guía de administración se utilizan los siguientes iconos:



Aclaraciones e información adicional, como, por ejemplo, un método alternativo para realizar una determinada tarea.



Sugerencias y recomendaciones.



Consulta en otra sección de la Guía de administración.

Capítulo 2

Información básica de Advanced EDR

Advanced EDR es una solución completa de seguridad para puestos de usuario y servidores, formada por múltiples tecnologías que ofrecen a los clientes un completo servicio de protección contra el malware, sin necesidad de instalar, gestionar o mantener nuevos recursos hardware en la infraestructura de la organización.

Contenido del capítulo

Beneficios de Advanced EDR	19
Características de Advanced EDR	20
Características de la plataforma Cytomic	21
Principales beneficios de Cytomic	21
Arquitectura de Cytomic	23
Cytomic en los equipos de usuario	24
Componentes principales	25
Servicios Advanced EDR	28
Perfil de usuario del producto	32
Dispositivos e idiomas soportados	32

Beneficios de Advanced EDR

Advanced EDR es una solución basada en múltiples tecnologías de protección que completa las carencias de los productos de antivirus tradicionales, protegiendo a los equipos de la empresa frente a todo tipo de malware, incluyendo APTs (Advanced Persistent Threat) y otras amenazas avanzadas.

Ejecución de software lícito

Advanced EDR supervisa y clasifica todos los procesos ejecutados en los equipos Windows del parque informático en base a su comportamiento y naturaleza. Gracias a este servicio los puestos de usuario y servidores son protegidos limitando la ejecución de los programas instalados a aquellos que han sido previamente certificados como seguros.

Adaptación al entorno de la empresa

A diferencia de los antivirus tradicionales, Advanced EDR utiliza un nuevo concepto de seguridad que le permite adaptarse con precisión al entorno particular de cada empresa. Para ello, supervisa la ejecución de todas las aplicaciones y aprende constantemente de las acciones desencadenadas por los procesos lanzados en los puestos de usuario y servidores.

Tras un breve periodo de aprendizaje, Advanced EDR es capaz de ofrecer un nivel de protección muy superior al de un antivirus tradicional.

Alcance y solución de problemas de seguridad

La oferta de seguridad se completa con herramientas monitorización, análisis forense y resolución, que acotan el alcance de los problemas detectados y los solucionan.

La monitorización aporta datos valiosos sobre el contexto en el que se sucedieron los problemas de seguridad. Con esta información, el administrador podrá determinar el alcance de los incidentes e implantar las medidas necesarias para evitar que vuelvan a producirse.

Multiplataforma

Advanced EDR es un servicio multiplataforma alojado en la nube y compatible con Windows, macOS y Linux, y con entornos virtuales y VDI, tanto persistentes como no persistentes.

Advanced EDR no necesita nueva infraestructura IT en la empresa para su gestión y mantenimiento, y por esta razón reduce el TCO de la solución a niveles muy bajos.

Características de Advanced EDR

Advanced EDR ofrece un servicio de seguridad garantizada frente a amenazas y ataques avanzados dirigidos a las empresas a través de cuatro pilares:

- **Visibilidad:** trazabilidad de cada acción realizada por las aplicaciones en ejecución.



Figura 2.1: Los cuatro pilares de la protección avanzada de Advanced EDR

- **Detección:** monitorización constante de los procesos en ejecución y bloqueo en tiempo real de ataques *Zero-day*, ataques dirigidos y otras amenazas avanzadas, diseñadas para pasar desapercibidas a los antivirus tradicionales.
- **Resolución y Respuesta:** información forense para investigar en profundidad cada intento de ataque, y herramientas de mitigar sus efectos.
- **Prevención:** evita futuros ataques modificando la configuración de los distintos módulos de protección y parcheando las vulnerabilidades de los sistemas operativos y de las aplicaciones instaladas.

Características de la plataforma Cytomic

Cytomic es la nueva plataforma de gestión, comunicación y tratamiento de la información desarrollada por Cytomic, que agrupa y centraliza los servicios comunes a todos sus productos.

La plataforma Cytomic gestiona las comunicaciones con los agentes desplegados en los equipos protegidos de los clientes, y presenta en la consola de administración, de forma ordenada y comprensible, toda la información recogida por Advanced EDR para su posterior análisis por parte del administrador de la red.

Este diseño modular de la solución evita la instalación de nuevos agentes o productos en los equipos del cliente por cada módulo adicional contratado. Todos los productos de Cytomic que funcionan sobre la plataforma Cytomic comparten un mismo agente en el equipo del usuario y una misma consola web de administración, facilitando su gestión y minimizando los recursos de los equipos.

Principales beneficios de Cytomic

A continuación, se presentan los principales servicios ofrecidos por Cytomic para todos los productos de Cytomic que sean compatibles con la plataforma:

Plataforma de gestión Cloud

Cytomic es una plataforma que reside en la nube de Cytomic, incorporando importantes ventajas de cara a su manejo, funcionalidad y accesibilidad:

No requiere servidores de gestión que alojen la consola de administración en las instalaciones del cliente: al funcionar desde la nube, es directamente accesible por todos los equipos suscritos al servicio, desde cualquier lugar y en cualquier momento, sin importar si están dentro de la oficina o desplazados.

El administrador de la red puede acceder a la consola de administración desde cualquier momento y en cualquier lugar, simplemente con un navegador compatible desde un equipo portátil, un equipo de sobremesa o incluso un dispositivo móvil como una tablet o un smartphone.

Es una plataforma ofrecida en régimen de alta disponibilidad, operativa el 99'99% del tiempo. El administrador de la red queda liberado de diseñar y desplegar costosos sistemas en redundancia para alojar las herramientas de gestión.

Comunicación con la plataforma en tiempo real

El envío de configuraciones y tareas programadas desde y hacia los equipos de la red se realiza en tiempo real, en el momento en que el administrador aplica la nueva configuración a los dispositivos seleccionados. El administrador puede ajustar los parámetros de la seguridad de forma casi instantánea para solucionar posibles brechas de seguridad o adaptar el servicio de seguridad al constante cambio de la infraestructura informática de las empresas.

Multi producto y Multiplataforma

La integración de los productos de Cytomic en una misma plataforma ofrece las siguientes ventajas al administrador:

- **Minimiza la curva de aprendizaje:** todos los productos comparten una misma consola, de esta forma se minimiza el tiempo que el administrador requiere para aprender el manejo de una nueva herramienta, redundando en menores costes de TCO.
- **Único despliegue para múltiples productos:** solo es necesario un único programa instalado en cada equipo para ofrecer la funcionalidad de todos los productos compatibles con Cytomic Platform. De esta forma se minimizan los recursos utilizados en los equipos de los usuarios en comparación con la utilización de productos independientes.
- **Mayores sinergias entre productos:** todos los productos reportan en una misma consola: el administrador dispone de un único panel de control donde observa toda la información generada, minimizando el tiempo y el esfuerzo invertido en mantener varios repositorios de información independientes y en consolidar la información generada en fuentes distribuidas.
- **Compatible con múltiples plataformas:** no es necesario contratar distintos productos para cubrir todo el espectro de dispositivos de la compañía: Cytomic Platform funciona para Windows, Linux y macOS, además de entornos virtuales y VDI tanto persistentes como no persistentes.

Configuraciones flexibles y granulares

El nuevo modelo de configuración permite acelerar la gestión de los equipos mediante la reutilización de configuraciones, haciendo uso de mecanismos específicos como la herencia y la asignación de configuraciones a equipos individuales. El administrador de la red podrá asignar configuraciones mucho más específicas y con menor esfuerzo.

Información completa y a medida

Cytomic Platform implementa mecanismos que permiten configurar la cantidad de datos mostrados a lo largo de una amplia selección de informes, según las necesidades del administrador o del consumidor final de la información.

La información se completa además con datos sobre los equipos, hardware y software instalado, así como un registro de cambios, que ayudarán al administrador a valorar el estado de la seguridad del parque informático administrado.

Arquitectura de Cytomic

La arquitectura de Cytomic está diseñada de forma escalable para ofrecer un servicio flexible y eficiente. La información se envía y se recibe en tiempo real desde / hacia múltiples fuentes y destinos de forma simultánea. Los orígenes y destinos pueden ser equipos vinculados al servicio, consumidores externos de información como sistemas SIEM o servidores de correo, instancias web para las peticiones de cambios de configuración y presentación de información de los administradores de red, entre otros.

Además, Cytomic implementa un backed y una capa de almacenamiento que utiliza una amplia variedad de tecnologías que le permite manipular los múltiples tipos de datos de forma ágil.

Estructura lógica de la plataforma Cytomic muestra un diagrama a alto nivel de Cytomic Platform.

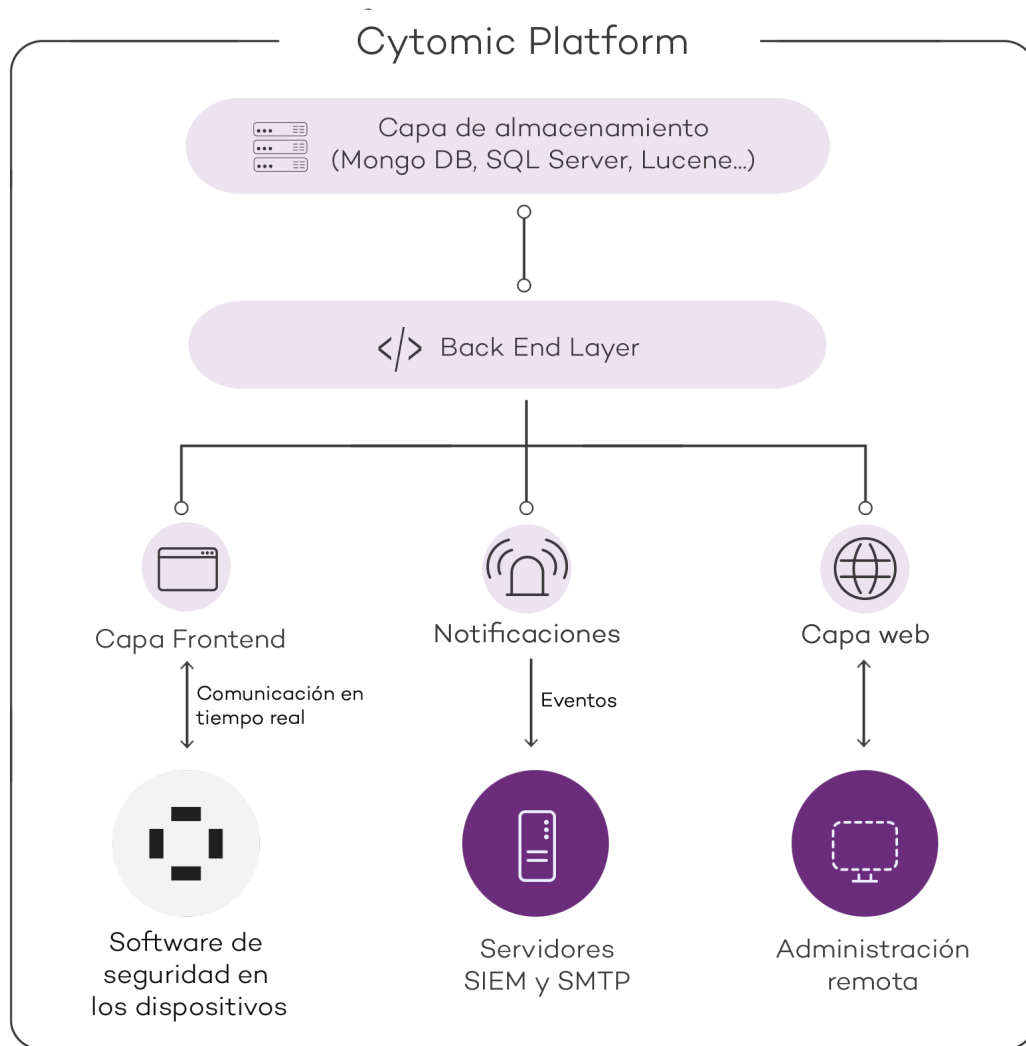


Figura 2.2: Estructura lógica de la plataforma Cytomic

Cytomic en los equipos de usuario

Los equipos de la red protegidos con Advanced EDR llevan instalado un software, formado por dos módulos independientes pero relacionados, que aportan toda la funcionalidad de protección y gestión:

- **Módulo Agente de comunicaciones Cytomic (agente Cytomic):** es el encargado de servir de puente entre el módulo de protección y la nube, gestionando las comunicaciones, eventos y configuraciones de seguridad implementadas por el administrador desde la consola de administración.
- **Módulo Protección Advanced EDR:** es el encargado de proteger de forma efectiva el equipo del usuario. Para ello se sirve del agente de comunicaciones para recibir las configuraciones y emite estadísticas y datos de las detecciones y elementos analizado.

Agente de comunicaciones en tiempo real Cytomic

El agente Cytomic se encarga de las comunicaciones entre los equipos administrados y el servidor de Advanced EDR, y de establecer un diálogo entre los equipos que pertenecen a una misma red del cliente.

Este módulo también gestiona los procesos de la solución de seguridad y recoge los cambios de configuración que el administrador haya realizado a través de la consola Web, aplicándolos sobre el módulo de protección.

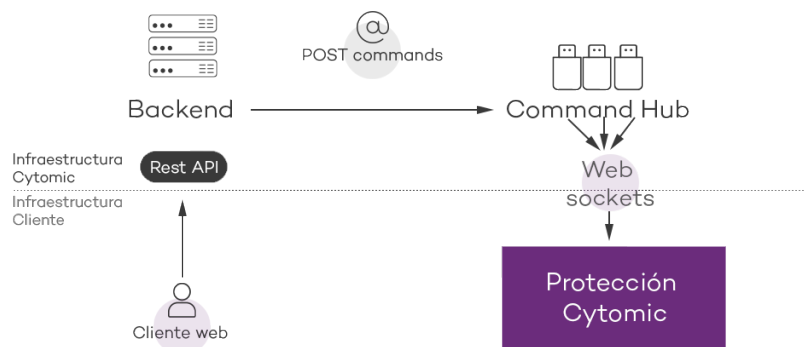


Figura 2.3: Recorrido de los comandos introducidos con la consola de administración

La comunicación entre los dispositivos y el Command Hub se implementa mediante conexiones websockets persistentes y en tiempo real, estableciendo una conexión por cada uno de los equipos para el envío y recepción de datos. Para evitar que dispositivos intermedios provoquen el cierre de las conexiones, se genera un flujo de keepalives constante.

Las configuraciones establecidas por el administrador de la red mediante la consola de administración Advanced EDR se envían mediante una API REST al backend; éste las reenvía al Command hub generando un comando POST, el cual finalmente ejecuta un push de la información a todos los dispositivos suscritos. Con un buen funcionamiento de las líneas de comunicación, los equipos recibirán la configuración en tiempo real.

Componentes principales

Advanced EDR es un servicio de seguridad que se apoya en el análisis del comportamiento de los procesos ejecutados en los equipos del parque de cada cliente. En este análisis se aplican técnicas de Machine Learning en infraestructuras Big Data alojadas en la nube.

Esquema general Advanced EDR representa el esquema general de Advanced EDR y los componentes que lo forman:

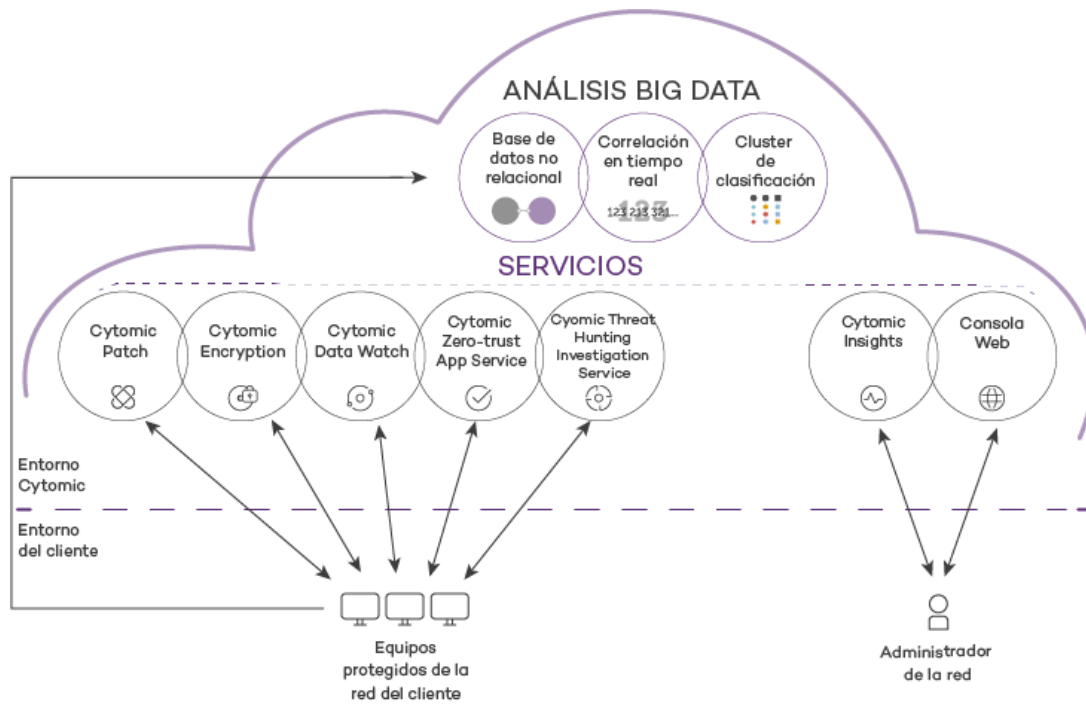


Figura 2.4: Esquema general Advanced EDR

- **Infraestructura de análisis big data**, formada por bases de datos no relacionales, servicios de correlación de eventos monitorizados en tiempo real y un cluster de clasificación de los procesos monitorizados.
- **Servicio Zero-Trust Application Service**: clasifica todos los procesos ejecutados en equipos Windows sin ambigüedades ni falsos positivos ni negativos.
- **Servicio Threat Hunting Investigation Service (THIS)**: investigación transversal incluido en la licencia básica del producto, que detecta amenazas desconocidas y ataques de tipo “Living off the Land”. Estos ataques dirigidos están diseñados para evadir las protecciones instaladas en el equipo.
- **Cytomic SIEMConnect (opcional)**: integra Advanced EDR con soluciones SIEM de proveedores externos.
- **Servicio Evaluación de vulnerabilidades**: localización de software con vulnerabilidades e información sobre parches disponibles.
- **Servicio Cytomic Insights (opcional)**: servicio de informes para generar inteligencia de seguridad avanzada.
- **Servicio Cytomic Patch (opcional)**: parcheo de sistemas operativos Windows y aplicaciones de terceros.
- **Servicio Cytomic Encryption (opcional)**: cifra los dispositivos de almacenamiento interno de los equipos Windows para minimizar la exposición de datos en caso de pérdida o robo, o al desechar dispositivos de almacenamiento sin borrar completamente su contenido.

- **Consola web:** servidor de la consola de administración.
- Equipos protegidos mediante el software Advanced EDR instalado.
- Equipo del administrador de red que accede a la consola Web.

Infraestructura de análisis Big Data

Es el clúster de servidores en la nube que recibe la telemetría generada en los equipos del parque informático del cliente. La telemetría está formada por las acciones ejecutadas por los programas del usuario y monitorizados por el módulo de protección, sus atributos estáticos y la información de contexto de ejecución. Todo ello forma flujo contante de información que se analiza en la nube mediante técnicas de inteligencia artificial para evaluar el comportamiento de dichos programas y emitir una clasificación por cada proceso en ejecución. Esta clasificación se devuelve al módulo de protección del equipo, y se toma como base para ejecutar las acciones configuradas con el objeto de mantenerlo protegido.

Las ventajas de este nuevo modelo de análisis de procesos frente al adoptado por los antivirus tradicionales basados en el envío de muestras al proveedor y análisis manual son:

- Todos los procesos de los equipos protegidos son monitorizados y analizados: se elimina la incertidumbre de los antivirus tradicionales, capaces únicamente de reconocer el malware sin considerar el resto de aplicaciones.
- El retraso en la clasificación de los procesos vistos por primera vez (ventana de oportunidad) es mínimo ya que Advanced EDR envía en tiempo real las acciones que ejecuta cada proceso. Los servidores en la nube trabajan de forma constante con esta información, disminuyendo de manera sustancial el tiempo necesario para emitir una clasificación, y por tanto el tiempo de exposición a las amenazas.
- La monitorización continua de cada proceso permite a Advanced EDR clasificar como malware elementos que inicialmente eran considerados goodware. Este cambio de comportamiento es muy habitual en los ataques dirigidos y otras amenazas avanzadas diseñadas para operar por debajo del radar.
- El consumo de recursos de CPU en el equipo del usuario es mínimo y está estimado en un 2% frente al 5%-15% de las soluciones de seguridad tradicionales, ya que todo el proceso de análisis y clasificación se realiza en la nube. El Agente instalado simplemente recoge la clasificación enviada por el servidor Advanced EDR y ejecuta una acción correctora.
- El análisis en la nube libera al cliente de instalar y mantener infraestructura de hardware y software junto al pago de licencias y la gestión de garantías del hardware, con lo que el TCO de la solución desciende significativamente.

Servidor Web de la consola de administración

La consola Web es compatible con los navegadores más comunes y es accesible desde cualquier lugar y en cualquier momento con cualquier dispositivo que tenga instalado un navegador compatible.



Para verificar si tu navegador es compatible con el servicio consulta [Acceso a la consola web](#) en la página **863**.

La consola Web es “responsive”, de modo que se puede utilizar sin problemas desde móviles y tablets.

Equipos protegidos con Advanced EDR

Advanced EDR requiere de la instalación de un componente software en todas las máquinas del parque informático susceptibles de sufrir problemas de seguridad. Este componente está formado por dos módulos: el agente de comunicaciones Cytomic y el módulo de la protección Advanced EDR.



Advanced EDR se instala sin problemas en máquinas con otras soluciones de seguridad de la competencia.

El módulo de la protección Advanced EDR contiene las tecnologías encargadas de proteger los equipos del cliente. Advanced EDR reúne en un mismo producto todos los recursos necesarios para detectar el malware de nueva generación y ataques dirigidos (APT), al tiempo que incorpora herramientas de resolución para desinfectar los equipos comprometidos y determinar el alcance de los intentos de intrusión en la red del cliente.

Servicios Advanced EDR

Cytomic ofrece otros servicios, algunos de carácter opcional, que integran la solución con la infraestructura IT del cliente, y obtener de forma directa la inteligencia de seguridad generada en los laboratorios de Cytomic.

Servicio Zero-Trust Application Service

Este servicio incluido por defecto en el producto en equipos Windows tiene como objetivo permitir la ejecución únicamente de los programas certificados por Cytomic. Para conseguirlo, se utiliza una mezcla de tecnologías locales en el equipo del usuario y en la infraestructura de análisis big data que clasifican de forma automática el 99'98% de los procesos ejecutados. Para el resto de procesos se aplican clasificaciones manuales ejecutadas por expertos en malware. Con este enfoque se consiguen clasificar el 100% de los binarios ejecutados en los equipos de los clientes sin falsos positivos ni negativos.

Los ficheros ejecutables encontrados en el equipo del usuario y desconocidos para la plataforma se envían de forma automática a la infraestructura de análisis big data para su análisis.



Los ficheros desconocidos se envían una sola vez para todos los clientes que usan Advanced EDR, por lo tanto, el impacto en el rendimiento de la red del cliente es prácticamente nulo. Además, se han implementado mecanismos de gestión del ancho de banda y límites por equipo y hora.

Threat Hunting Investigation Service (THIS)

Servicio que detecta amenazas y ataques de tipo “Living off the Land”, diseñados para evadir las protecciones instaladas en el equipo. Este servicio se apoya en el producto Cytomic Orion, la plataforma de Threat Hunting avanzada desarrollada por Cytomic.

Gracias a la telemetría que se envía desde los equipos, Cytomic Orion analiza de forma transversal los procesos ejecutados en la infraestructura IT de los clientes para detectar nuevos ataques y crear reglas avanzadas de hunting. Cuando se produce un indicio de ataque, el equipo de expertos en ciberseguridad de Cytomic valida y Advanced EDR muestra en la consola el indicador de ataque asociado (IOA) junto con una descripción de sus características y recomendaciones dirigidas al administrador para resolver la situación.

Este servicio está disponible en todas las licencias de Advanced EDR y Advanced EDR.



Para obtener más información sobre la configuración del módulo de indicadores de ataque consulta [Configuración de Indicadores de ataque \(IOA\)](#) en la página 566.

Servicio MDR (Managed Detection and Response)

Es un servicio de ciberseguridad 24/7 que permite a los partners ofrecer un servicio gestionado de detección y respuesta a sus clientes con una inversión mínima en un SOC (Security Operations Center). El servicio monitoriza la seguridad de los equipos de la empresa, busca amenazas, detecta ataques, investiga y ofrece recomendaciones guiadas para resolver los activos afectados y mejorar la seguridad de los clientes.

El servicio MDR está impulsado por tecnologías innovadoras que utilizan algoritmos de inteligencia artificial. Además, el servicio está completamente administrado por un equipo de expertos en ciberseguridad, lo que mejora de forma general la protección y resiliencia cibernética de los clientes y minimiza el tiempo de detección y respuesta.



Para obtener más información sobre el servicio MDR consulta [Configuración del servicio MDR](#) en la página 604.

Servicio Cytomic Insights (opcional)

Advanced EDR envía de forma automática y transparente toda la información recogida de los equipos al servicio Cytomic Insights, un sistema de almacenamiento y explotación del conocimiento.

Las acciones de los procesos ejecutados en el parque de IT se envían a Cytomic Insights donde se estudian y relacionan para extraer inteligencia de seguridad. El administrador dispondrá de información adicional sobre las amenazas y sobre el uso que los usuarios dan a los equipos de la empresa. Esta nueva información se presenta de forma flexible y visual para favorecer su comprensión.

El servicio Cytomic Insights es accesible directamente desde el panel de control de la propia consola Web de Advanced EDR.



Consulta la Guía de usuario de Cytomic Insights accesible desde la web de producto para configurar y sacar provecho del servicio de análisis de conocimiento y búsquedas avanzadas.

Servicio Cytomic SIEMConnect (opcional)

Advanced EDR se integra con las soluciones SIEM de proveedores externos implementadas por los clientes en sus infraestructuras de IT. La actividad de las aplicaciones que se ejecutan en el parque informático se entrega al servidor al SIEM, ampliada con todo el conocimiento ofrecido por Advanced EDR, y lista para ser utilizada.

A continuación, se listan los sistemas SIEM compatibles con Advanced EDR:

- QRadar
- AlienVault
- ArcSight
- LookWise
- Bitacora



Consulta la Guía de usuario de Cytomic SIEMConnect para una descripción detallada de la información recogida por Advanced EDR y enviada al sistema SIEM del cliente.

Servicio Cytomic Data Watch (opcional)

Es un módulo de seguridad integrado en la plataforma Advanced EDR que ayuda a cumplir con las regulaciones en materia de retención de datos personales (PII) almacenados en la infraestructura IT de las empresas.

Cytomic Data Watch descubre, audita y monitoriza en tiempo real el ciclo de vida completo de los ficheros PII almacenados en equipos Windows: desde datos en reposo, las operaciones efectuadas sobre ellos y su

transferencia al exterior. Con esta información, Cytomic Data Watch genera un inventario por cada equipo de la red que permite mostrar la evolución de los ficheros que contienen información personal.



Consulta **Cytomic Data Watch (Supervisión de información sensible)** en la página 311 para una descripción detallada del servicio.

Servicio Cytomic Patch (opcional)

Este servicio reduce la superficie de ataque de los puestos de usuario y servidores Windows actualizando el software vulnerable (sistemas operativos y aplicaciones de terceros) con los parches publicados por los proveedores correspondientes.

Además, permite localizar los programas que han entrado en EoL (End Of Life) considerados peligrosos por no tener mantenimiento de su proveedor original y ser el blanco de los hackers que aprovechan las vulnerabilidades conocidas y sin corregir. El administrador puede localizar con facilidad todos los programas en EoL y planificar una sustitución controlada de los mismos.

En caso de incompatibilidades o mal funcionamiento de las aplicaciones parcheadas, Cytomic Patch permite ejecutar un Rollback / desinstalación de los parches que lo permitan o excluirlos previamente para evitar su instalación.

Servicio Evaluación de vulnerabilidades

Este servicio gratuito realiza una búsqueda en los equipos para detectar software instalado que tenga vulnerabilidades. Con el fin de evitar que el malware aproveche estas brechas de seguridad para dañar e infectar los equipos y servidores, informa de la existencia de parches disponibles que eviten el impacto de las vulnerabilidades.

Para instalar de forma centralizada los parches disponibles es necesario obtener una licencia de Cytomic Patch.

Servicio Cytomic Encryption (opcional)

El cifrado de la información contenida en los dispositivos de almacenamiento interno de los equipos es un recurso fundamental a la hora de proteger los datos que contienen en caso de robo o pérdida y cuando la empresa recicla dispositivos de almacenamiento sin borrar completamente. Advanced EDR utiliza la tecnología BitLocker (Windows) y FileVault (macOS) para cifrar el contenido de los discos duros a nivel de sector y gestiona de forma centralizada las claves de recuperación en caso de pérdida o cambio de configuración de hardware.

El módulo Cytomic Encryption permite utilizar el módulo de plataforma segura TPM si está disponible, y ofrece varias configuraciones de autenticación para añadir flexibilidad a la protección de los datos contenidos en el equipo.

Perfil de usuario del producto

Aunque Advanced EDR es un servicio gestionado que ofrece seguridad sin intervención del administrador de la red, también provee información muy detallada y comprensible sobre la actividad de los procesos ejecutados por los usuarios en toda la infraestructura de IT de la empresa. Esta información puede ser utilizada por el administrador para precisar el impacto de problemas de seguridad y adaptar sus protocolos, evitando así la repetición de situaciones similares en el futuro.

Dispositivos e idiomas soportados



Para una descripción detallada de las plataformas y requisitos consulta **Funcionalidades del producto y requisitos** en la página **847** para más información.

Compatibilidad con sistemas operativos

- Windows Workstation
- Windows Server
- Sistemas virtuales y VDI persistentes y no persistentes
- macOS
- Linux

Compatibilidad con navegadores web

La consola de administración es compatible con las últimas versiones de los navegadores mostrados a continuación:

- Chrome
- Microsoft Edge
- Firefox
- Opera

Idiomas soportados en la consola web

- Español
- Inglés
- Sueco
- Francés
- Italiano

- Alemán
- Portugués
- Húngaro
- Ruso
- Japonés
- Finlandés (solo consola local)

Capítulo 3

La consola de administración

Advanced EDR utiliza las últimas tecnologías de desarrollo web para ofrecer una consola de administración alojada en la nube que permite interactuar de manera cómoda y ágil con el servicio de seguridad. Sus principales características son:

- **Adaptable:** diseño “responsive” que se adapta al tamaño del dispositivo empleado para administrar el servicio.
- **Amigable:** interface desarrollado con tecnología Ajax que evita las recargas de páginas completas.
- **Flexible:** interface adaptable que almacena los ajustes realizados para posteriores accesos.
- **Homogénea:** patrones de usabilidad bien definidos para minimizar la curva de aprendizaje del administrador.
- **Interoperable:** datos exportables en formato `CSV` con campos extendidos para su posterior consulta.

Contenido del capítulo

Beneficios de la consola web	36
Acceso a la consola web y requisitos	36
Requisitos para acceder a la consola web	36
Acceso la consola web	37
Estructura general de la consola web	37
Menú superior (1)	38
Menú lateral (2)	42
Panel central (3)	42
Acceso a Cytomic Insights (4)	42
Elementos básicos de la consola web	42
Esquema general de la zona Estado	45

Gestión de listados	47
Plantillas, configuraciones y vistas	48
Secciones de los listados	52
Operaciones con listados	54
Listados incluidos por defecto	57

Beneficios de la consola web

La consola Web es la herramienta principal del administrador para la gestión de la seguridad. Al tratarse de un servicio Web, hereda una serie de características que influirán de manera positiva en la forma de trabajo del departamento de IT.

Única herramienta para la gestión completa de la seguridad

El administrador podrá distribuir de forma centralizada el paquete de instalación Advanced EDR en los equipos de la red, establecer las configuraciones de seguridad, monitorizar el estado de la protección de los equipos y disponer de herramientas de resolución y análisis forense en caso de incidentes de seguridad. Toda la funcionalidad se ofrece desde una única consola Web, favoreciendo la integración de las distintas herramientas y minimizando la complejidad de utilizar varios productos de distintos proveedores.

Gestión centralizada de la seguridad para oficinas remotas y usuarios desplazados

La consola Web está alojada en la nube, por lo que no son necesarias configuraciones de VPN ni redirecciones de puertos en los routers corporativos para su acceso desde el exterior de la oficina. Tampoco son necesarias inversiones en infraestructuras IT, tales como servidores, licencias de sistemas operativos o bases de datos, ni es necesaria una gestión del mantenimiento / garantía para asegurar el funcionamiento del servicio.

Gestión de la seguridad desde cualquier lugar y en cualquier momento

La consola Web es de tipo “responsive / adaptable” con lo que se ajusta al tamaño del dispositivo utilizado por el administrador. De esta manera se puede gestionar la seguridad desde cualquier lugar y en cualquier momento, mediante un smartphone, un notebook o un PC de escritorio.

Acceso a la consola web y requisitos

Requisitos para acceder a la consola web

- Credenciales válidas (cuenta de usuario y contraseña) y un segundo factor de autenticación (opcional). Consulta [Acceso, control y supervisión de la consola de administración](#) en la página 59.
- Última versión de un navegador web certificado:
 - Google Chrome
 - Microsoft Edge

- Firefox
- Opera
- Conexión a Internet y comunicación por el puerto 443.

Acceso la consola web

Para acceder a la consola Web de Advanced EDR utiliza la siguiente URL:

<https://central.cytomic.ai>

- Abre un navegador compatible y accede a la URL <https://central.cytomic.ai>
- Escribe las credenciales de tu cuenta de usuario.
- Si tu cuenta de usuario tiene acceso a varias cuentas de cliente distintas, se abrirá la ventana **Selecciona la cuenta**. Elige el cliente que tiene asociada la consola a la que deseas acceder.
- Se abrirá la consola de Advanced EDR mostrando el panel de control Seguridad.

Estructura general de la consola web

La consola web cuenta con recursos que facilitan una experiencia de gestión homogénea y coherente, tanto para administrar la seguridad de la red como para resolver los incidentes y realizar un análisis forense.

El objetivo de la consola web es entregar al administrador una herramienta sencilla, pero a la vez flexible y potente, que le permita comenzar a gestionar la seguridad de la red de forma productiva en el menor período de tiempo posible.

A continuación, se incluye una descripción de los elementos de la consola y su modo de uso.

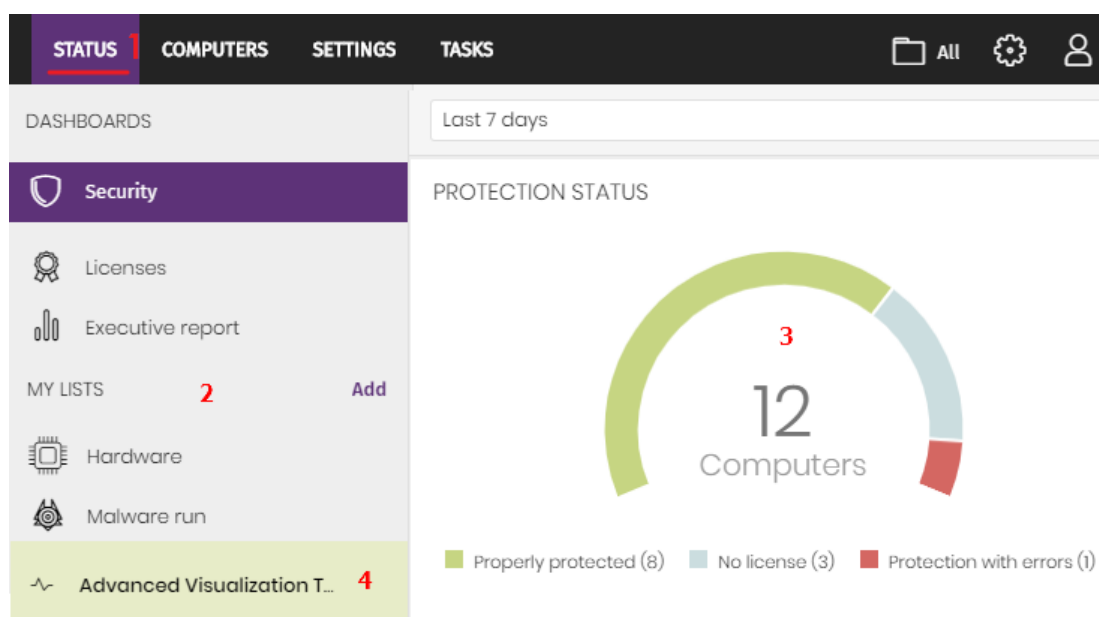


Figura 3.1: Vista general de la consola de administración Advanced EDR

Menú superior (1)

La consola distribuye toda su funcionalidad en varias zonas accesibles desde el menú superior:

- Botón Cytomic Central
- Estado
- Equipos
- Configuración
- Tareas
- Filtro por grupo
- Notificaciones web
- Configuración general
- Cuenta de usuario

Botón Cytomic Central

Haz clic en el botón  situado en el lateral izquierdo del menú superior para elegir el producto de seguridad contratado y gestionarlo o modificar la configuración de tu cuenta de usuario.

Menú superior Estado

Muestra el panel de control de la consola desde la cual el administrador tiene acceso de un vistazo a toda la información de seguridad, ya sea de forma gráfica mediante widgets como por los listados situados en el menú lateral. Consulta [Esquema general de la zona Estado](#) para más información.

Menú superior Equipos

Ofrece las herramientas básicas para definir la estructura de los equipos de la red que mejor se ajuste a la configuración de seguridad diseñada para el parque informático. Elegir una correcta estructura de dispositivos es fundamental a la hora de asignar configuraciones de seguridad. Consulta [La zona equipos](#) en la página [178](#) para más información.

Menú superior Configuración

Permite al administrador de la red definir el comportamiento de Advanced EDR en los equipos de usuario y servidores donde se encuentra instalado. La asignación de la configuración se establece de forma global para todos los equipos de la red, o únicamente para algunos equipos concretos mediante plantillas, dependiendo del tipo de configuración a establecer. Estas plantillas de configuración se pueden asignar a uno o más equipos de la red que tengan requerimientos de seguridad similares, permitiendo minimizar el tiempo del administrador dedicado a gestionar la seguridad de su red de equipos.



Consulta **Gestión de configuraciones** en la página **251** para obtener información detallada sobre cómo crear una configuración en Advanced EDR.

Menú superior Tareas

Permite la gestión de tareas de seguridad programadas para su ejecución en los intervalos de tiempo designados por el administrador. Consulta **Tareas** en la página **825**.

Icono Filtro por grupo

Limita la información generada mostrada en la consola por los equipos que pertenezcan al grupo o grupos elegidos. Consulta **Filtrar resultados por grupos** en la página **193** para más información.

Icono Notificaciones web

Al hacer clic en el icono se muestra un desplegable con las comunicaciones de carácter general que Cytomic pone en conocimiento para todos los usuarios de la consola, y ordenadas según su importancia:

- Paradas programadas de mantenimiento
- Avisos de vulnerabilidades críticas
- Consejos de seguridad
- Mensajes para iniciar el proceso de actualización de la consola. Consulta **Actualización de la consola de administración** en la página **175**.

Cada comunicación tiene asociada un nivel de prioridad:

-  Importante
-  Aviso
-  Informativa

El número del icono indica la cantidad de notificaciones web nuevas (que quedan por leer).

Para eliminar una notificación web, haz clic en su icono de aspa asociado. Las notificaciones así eliminadas no se volverán a mostrar, y el icono ajustará su número al total de notificaciones web que se muestran.

Icono Configuración General

Muestra un menú desplegable que permite el acceso a la documentación del producto, cambio de idioma de la consola y otras herramientas.

Entrada	Descripción
Ayuda online	Acceso a las ayudas web del producto.
Guía de administración de Cytomic Insights	Acceso a la guía para el administrador del módulo Cytomic Insights si está contratado.
Guía de administración de Advanced EDR	Acceso a la Guía de administración del producto Advanced EDR.
Guía de administración de Cytomic Data Watch	Acceso a la guía para el administrador del módulo Cytomic Data Watch si está contratado.
Soporte técnico	Carga la dirección web correspondiente al soporte técnico de Advanced EDR.
Buzón de sugerencias	Lanza la herramienta de correo local instalada en equipo para enviar un mensaje de correo al departamento de soporte técnico de Cytomic.
Acuerdo de licencia	Muestra el EULA (End User License Agreement).
Acuerdo sobre tratamiento de datos	Muestra el acuerdo de protección de datos de la plataforma según la normativa europea.
Novedades de Advanced EDR	Enlace a la página web de soporte que muestra los cambios y nuevas funcionalidades incluidas en la versión.
Idioma	Permite seleccionar el idioma en que se mostrará la consola de administración.
Acerca de...	Muestra la versión de los diferentes elementos de Advanced EDR. • Versión: versión del producto. • Versión de la protección: versión interna del módulo de protección instalado en los equipos. • Versión del agente: versión interna del módulo de comunicaciones instalado en los equipos.

Tabla 3.1: Menú Configuración general

Icono Cuenta de usuario



Muestra un menú desplegable con las siguientes entradas de configuración:

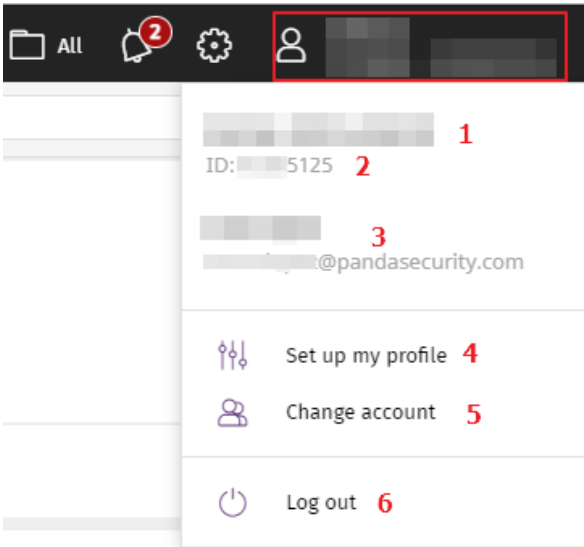


Figura 3.2: Menú desplegable Cuenta de usuario

Entrada	Descripción
Nombre del cliente (1)	Nombre y apellidos de la cuenta de usuario con la que se ha accedido a la consola.
Id de cliente (2)	El identificador de cliente es un número que Cytomic asigna a la cuenta de cliente para identificarlo. El departamento de Soporte de Cytomic puede requerirlo en sus comunicaciones con el cliente.
Dirección de correo (3)	Dirección de correo utilizada para acceder a la consola de administración.
Configurar mi perfil (4)	Modifica la información de la cuenta de usuario. Consulta Cambiar los datos personales de una cuenta de usuario en la página 63.
Cambiar de cuenta (5)	Muestra las cuentas de cliente accesibles desde la cuenta de usuario que inició la sesión, y permite seleccionar una cuenta de cliente diferente para operar con la consola asociada al producto.
Cerrar sesión (6)	Termina la sesión en la consola.

Tabla 3.2: Menú Cuenta de usuario

Menú lateral (2)

Muestra las diferentes subzonas dentro de la zona seleccionada, actuando como un selector de segundo nivel con respecto al menú superior.

El menú lateral varía en función de la zona presentada, adaptándose al tipo de información que se muestra.

Para maximizar el espacio de visualización del panel central reduce el tamaño del menú lateral haciendo clic en la barra de separación del panel. Si se reduce por debajo del tamaño de los nombres de las opciones, el menú lateral se contraerá completamente. Para volver expandirlo a su tamaño original haz clic en el icono .

Panel central (3)

Recoge toda la información relevante de la zona y subzona elegidas por el administrador. **Vista general de la consola de administración Advanced EDR** muestra la zona **Estado** subzona **Seguridad**, formada por los widgets que permiten interpretar la información de seguridad recogida. Para obtener más detalle acerca de los widgets consulta **Paneles/Widgets del módulo de seguridad** en la página 608.

Acceso a Cytomic Insights (4)

Cytomic Insights es el punto de entrada para la consola de gestión de los módulos Cytomic Data Watch y Cytomic Insights. Ambos comparten una consola especialmente diseñada para mostrar gráficas avanzadas y tablas con información relevante sobre la actividad de los todos procesos ejecutados en los puestos de usuario y servidores.

Elementos básicos de la consola web

Menú de pestañas superior

En las zonas de la consola más complejas se muestra un selector de tercer nivel en forma de pestañas que mantiene la información ordenada por categorías.

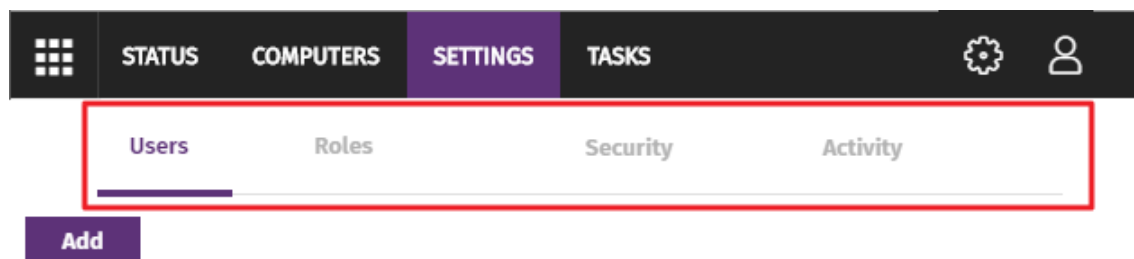


Figura 3.3: Menú de pestañas

Barra de acciones

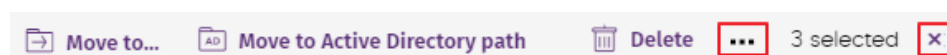


Figura 3.4: Barra de acciones

Para facilitar la navegación de la consola y el acceso a algunas operaciones comunes sobre los puestos de usuario y servidores administrados, se incorpora una barra de acciones en la parte superior de la pantalla. El número de botones mostrados se adapta al tamaño de la ventana. Los botones que quedan fuera se añaden al icono **...** situado a la derecha de la barra de acciones.

En la esquina derecha de la barra de acciones se muestra el número total de equipos seleccionados. Haz clic en el icono del aspa para deshacer la selección.

Herramientas de filtrado y búsqueda

Las herramientas de filtrado y búsqueda muestran los subconjuntos de información de interés para el administrador. Algunas herramientas de filtrado son generales y aplican a toda la zona de la consola mostrada, como por ejemplo en el menú superior **Estado** o menú superior **Equipos**.

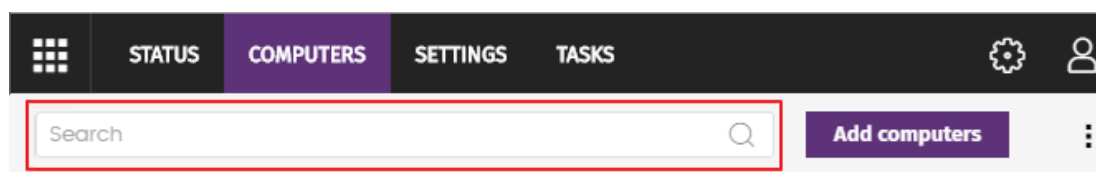


Figura 3.5: Herramienta de búsqueda

Parte de las herramientas de filtrado se ocultan por defecto bajo el desplegable **Filtros**, y permiten definir búsquedas por categorías, rangos y otros parámetros dependientes del tipo de información mostrada.

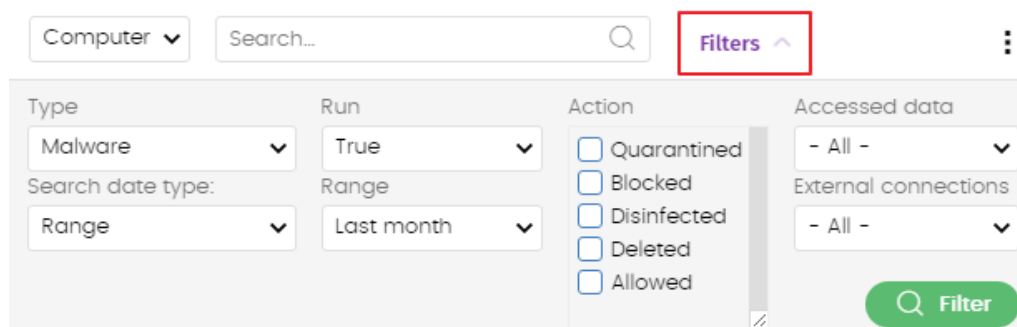


Figura 3.6: Sistema de filtrado de información en listados

Elementos de configuración

La consola web Advanced EDR utiliza controles estándar para introducir configuraciones, como son:

- Botones. **(1)**
- Links. **(2)**
- Casillas de activación y desactivación. **(3)**
- Desplegables de selección. **(4)**
- Combos de selección. **(5)**
- Cuadros de texto. **(6)**

Figura 3.7: Controles para el manejo de la consola de administración

Botón de ordenación

En algunos listados de elementos, como por ejemplo en la zona **Tareas** (menú superior **Tareas**) o en la zona **Configuración** (menú superior **Configuración**) se muestra el botón  en la esquina superior derecha o en algunos casos en la esquina inferior derecha. Este botón permite establecer el criterio de ordenación del listado:

- **Ordenado por fecha de creación** los elementos se ordenan según su fecha de incorporación al listado.
- **Ordenado por nombre** los elementos se ordenan por su nombre.
- **Ascendente**
- **Descendente**

Menús de contexto

Son menús desplegables que se muestran al hacer clic en el icono , con opciones que afectan al ámbito al que pertenecen según su posición.

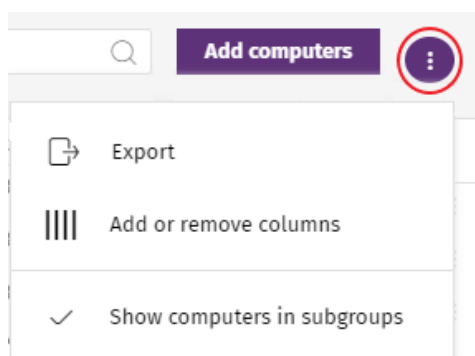


Figura 3.8: Menús de contexto

Copiar, pegar y borrar contenidos

Al pasar el puntero del ratón por las cajas de texto que admiten múltiples valores separados por espacios, se muestran dos botones flotantes para copiar y borrar su contenido.

- **Botón de copiar (1):** copia al portapapeles el contenido de los elementos que contiene la caja de texto separando cada uno de ellos con un retorno de carro. La consola muestra un mensaje cuando la operación se completa.
- **Botón de borrar (2):** limpia el contenido de la caja de texto.

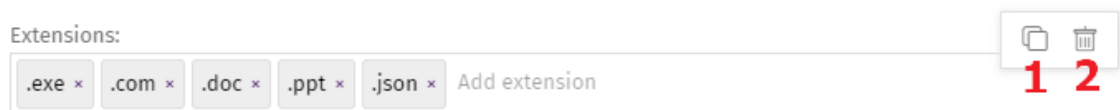


Figura 3.9: Botones Copiar y Borrar

- Al pulsar Control+v sobre una caja de texto se vuelca el contenido del portapapeles, siempre que éste contenga líneas de texto separadas por retornos de carro.

Esquema general de la zona Estado

El menú **Estado** reúne las principales herramientas de visibilidad, y está distribuido en varias secciones:

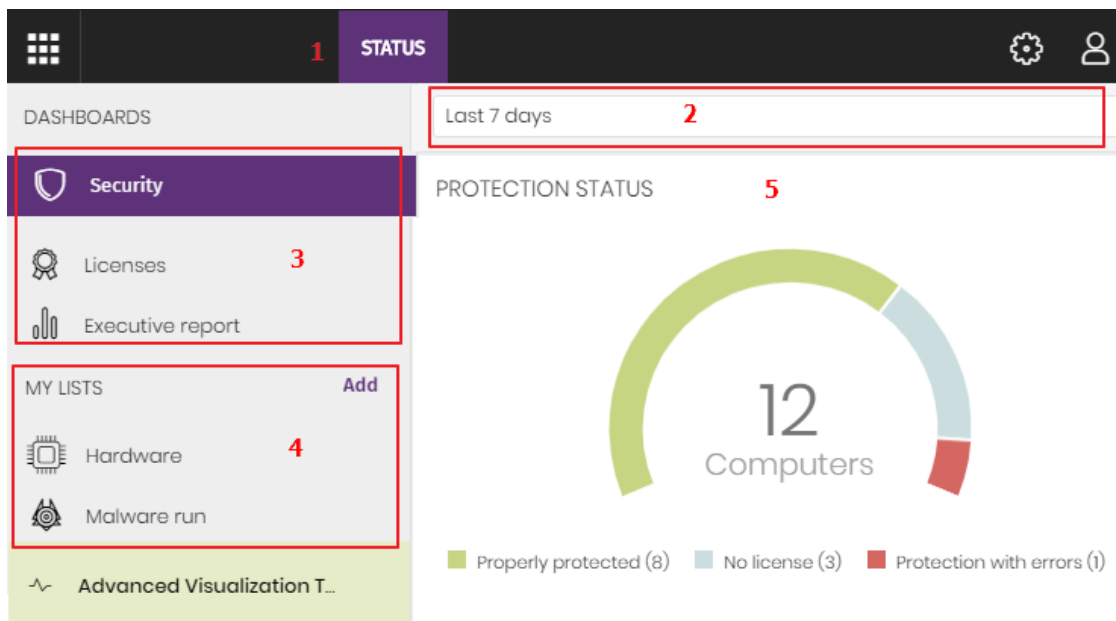


Figura 3.10: Ventana de Estado con el panel de control y acceso a los listados

Acceso al panel de control (1)

El acceso al panel de control se realiza mediante el menú superior **Estado**. Desde aquí se acceden a los diferentes widgets, así como a los listados.

Los widgets o paneles gráficos representan aspectos concretos del parque de equipos gestionado, dejando a los listados la entrega de datos más detallados.

Selector del intervalo de tiempo (2)

El panel de control muestra la información relevante en el intervalo de tiempo fijado por el administrador mediante la herramienta situada en la parte superior de la ventana **Estado**. Los intervalos disponibles son:

- Últimas 24 h.
- Últimos 7 días.
- Último mes.
- Último año.



No todos los paneles soportan el filtrado de datos por el último año. Los paneles que no soporten este intervalo de tiempo mostrarán una leyenda en la parte superior indicándolo.

Selector de panel (3)

- **Seguridad:** estado de la seguridad del parque informático. Para más información sobre los widgets incluidos consulta [Paneles/Widgets del módulo de seguridad](#) en la página 608

- **Cytomic Patch:** actualización del sistema operativo y del software instalado en los equipos. Para más información sobre los widgets incluidos consulta [Paneles/Widgets del módulo de seguridad](#) en la página **608**.
- **Cytomic Data Watch:** seguimiento de la información personal almacenada en los equipos de la red. Para más información sobre los widgets incluidos consulta [Introducción al funcionamiento de Cytomic Data Watch](#) en la página **312**.
- **Cytomic Encryption:** estado del cifrado de los dispositivos de almacenamiento internos en los equipos. Para más información sobre los widgets incluidos consulta [Paneles/Widgets del módulo de seguridad](#) en la página **608**.
- **Licencias:** estado de las licencias de Advanced EDR asignadas a los equipos de la red. Consulta [Licencias](#) en la página **157** para obtener más información acerca de la gestión de licencias.
- **Informes programados:** consulta [Envío programado de informes y listados](#) en la página **785** para obtener más información acerca de la configuración y generación de informes.

Mis listados (4)

Son tablas de datos con la información presentada en los paneles. Esta información se presenta con gran nivel de detalle e implementa herramientas de búsqueda y distribución que ayudan a localizar los datos requeridos.

Paneles informativos / Widgets (5)

Está formado por widgets o paneles informativos centrados en un único aspecto de la seguridad de la red.

Los paneles se generan en tiempo real y son interactivos: pasando el ratón por encima de los elementos se muestran tooltips con información extendida.

Todas las gráficas incluyen una leyenda que permite determinar el significado de cada serie representada, e incorporan zonas activas que al ser seleccionadas abren distintos listados asociados al widget con filtros predefinidos.

Advanced EDR utiliza varios tipos de gráficas para mostrar la información de la forma más conveniente según el tipo de dato representado:

- Gráficos de tarta.
- Histogramas.
- Gráficas de líneas.

Gestión de listados

Advanced EDR estructura la información recogida en dos niveles: un primer nivel que representa de forma gráfica los datos mediante paneles o widgets y un segundo nivel más detallado, donde la información se representa mediante listados compuestos por tablas. La mayor parte de los paneles tienen un listado asociado para que el administrador pueda acceder de forma rápida a un resumen gráfico de la información y después profundizar mediante los listados en caso de requerir mayor nivel de detalle.

Advanced EDR soporta el envío programado de listados por correo electrónico. De esta forma, el administrador no necesita acceder a la consola Web para conocer el detalle de los eventos que se producen en la red. Además, esta funcionalidad facilita la compartición de información entre departamentos y permite habilitar la construcción de un repositorio externo con el histórico de todos los eventos que se han producido, mas allá de los límites de la consola Web. Con este repositorio, el equipo directivo podrá realizar un seguimiento de la información generada libre de interferencias de terceros.

Plantillas, configuraciones y vistas

Un listado es la suma de dos elementos: una plantilla y una configuración de un filtro.

Una plantilla representa una fuente de datos sobre un apartado específico tratado por Advanced EDR.

Un filtro es una configuración específica de las herramientas de filtrado asociadas a cada plantilla.

Un filtro aplicado sobre una plantilla da como resultado una “vista de listado”, también llamado simplemente “listado”. El administrador puede crear y almacenar nuevos listados modificando los filtros asociados a una plantilla para su consulta posterior. De esta forma se evita reconfigurar los filtros de las plantillas más frecuentemente utilizadas, lo que lleva a un ahorro del tiempo de administración.

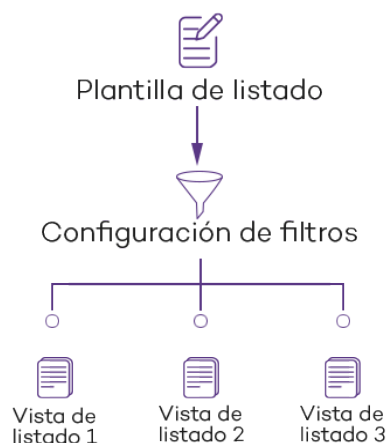


Figura 3.11: Generación de tres listados a partir de una misma plantilla / fuente de datos

Plantillas de listado

En el menú superior **Estado**, panel lateral **Mis listados** se encuentra el enlace **Añadir** que muestra una ventana con las plantillas disponibles agrupadas por su tipo:

Grupo	Listado	Descripción
General	Licencias	Muestra en detalle el estado de las licencias de los equipos de la red. Consulta Listados del módulo Licencias en la página 164 para más información.

Grupo	Listado	Descripción
	Equipos no administrados descubiertos	Muestra los equipos Windows de la red que no tienen el software Advanced EDR instalado. Consulta Listado Equipos no administrados descubiertos en la página 121 para más información.
	Equipos con nombre duplicado	Muestra los equipos con el mismo nombre y pertenecen al mismo dominio. Consulta Equipos con nombre duplicado en la página 214 para más información
	Software	Muestra el software instalado en los equipos del parque informático. Consulta Software en la página 212 para más información.
	Hardware	Muestra el hardware instalado en los equipos del parque informático. Consulta Hardware en la página 209 para más información.
Seguridad	Estado de protección de los equipos	Muestra en detalle el estado del módulo de la protección instalada en los equipos. Consulta Estado de protección de los equipos en la página 621 para más información.
	Actividad del malware y PUPS	Muestra el listado de las amenazas encontradas en los equipos protegidos con Advanced EDR. Consulta Actividad de malware / PUP en la página 628 para más información.
	Actividad de exploits	Muestra el número de ataques por explotación de vulnerabilidades recibidos en los equipos Windows de la red. Consulta Actividad de exploits en la página 632 para más información.
	Programas actualmente bloqueados en clasificación	Muestra una tabla con aquellos ficheros que, sin haber sido completada su clasificación, Advanced EDR ha detectado de forma preliminar algún riesgo en su ejecución. Consulta Actividad de malware / PUP en la página 628 para

Grupo	Listado	Descripción
		más información.
	Bloqueos por políticas avanzadas de seguridad	Muestra los scripts y programas desconocidos detectados que utilizan técnicas avanzadas de infección. Consulta Bloqueos por políticas avanzadas de seguridad en la página 636
	Bloqueos por políticas avanzadas de seguridad	Muestra el listado de las amenazas avanzadas encontradas en los equipos protegidos con Advanced EDR. Consulta Listados del módulo de seguridad en la página 621 para más información.
	IOCs detectados	Muestra los identificadores de compromiso encontrados en los equipos del cliente. Consulta Listados del módulo de seguridad en la página 621 para más información.
	Indicadores de ataque (IOA)	Muestra los indicios de ataques avanzados confirmados en el parque informático. Consulta Indicadores de ataque (IOA) en la página 569 .
Cytomic Patch	Estado de gestión de parches	Muestra en detalle todos los equipos de la red compatibles con Cytomic Patch Consulta Estado de gestión de parches en la página 418 para más información.
	Parches disponibles	Muestra el detalle de todos los parches sin instalar en los equipos de la red y publicados por Cytomic. Consulta Parches disponibles en la página 407 para más información.
	Historial de instalaciones	Muestra los parches que Advanced EDR intentó instalar y los equipos que los recibieron en un intervalo determinado. Consulta Historial de instalaciones en la página 438 para más información.
	Programas "End	Muestra la información relativa al "end of life" de los

Grupo	Listado	Descripción
	of Life"	programas instalados en los equipos de la red, agrupados según el plazo restante. Consulta Programas "End of Life" en la página 446 para más información.
	Parches excluidos	Muestra los pares equipo - parche que son excluidos de su instalación. Consulta Parches excluidos en la página 448 para más información.
Control de actividad	Programas bloqueados por el administrador	Muestra los intentos de ejecución de programas bloqueados por el administrador en los equipos de la red. Consulta Programas bloqueados por el administrador en la página 520 para más información.
Protección de datos	Estado del cifrado	Muestra toda la información referente a los equipos de la red compatibles con la funcionalidad de cifrado. Consulta Estado del cifrado en la página 506 para más información.
	Estado de Cytomic Data Watch	Muestra el estado del módulo Cytomic Data Watch de Advanced EDR. Consulta Estado de Cytomic Data Watch en la página 350 para más información.
	Archivos con información personal	Muestra todos los ficheros PII encontrados, así como su tipo, localización y otra información relevante. Consulta Archivos con información personal en la página 358 para más información.
	Equipos con información personal	Muestra el número de ficheros PII encontrados en cada uno de los equipos de la red. Consulta Equipos con información personal en la página 362 para más información.
	Archivos eliminados por el	Muestra el estado de los ficheros eliminados por el administrador mediante el módulo Cytomic Data Watch.

Grupo	Listado	Descripción
	administrador	Consulta Archivos eliminados por el administrador en la página 367 para más información.

Tabla 3.3: Listado de plantillas disponibles en Advanced EDR

Adicionalmente, existen otras plantillas accesibles directamente desde el menú de contexto de ciertos listados o desde algunos widgets del panel de control. Consulta el capítulo correspondiente al widget en cuestión.

Secciones de los listados

Los listados incorporan un conjunto de herramientas comunes que facilitan su interpretación. A continuación se muestran las partes principales de un listado de ejemplo.

Malware activity 1

Enter a description... 2

Computer Search... Filters 6 5

Type 7 Run Action Accessed data

Malware All

Dates: Last 7 days

Detected Quarantined Blocked Disinfected Deleted

10 Filter

Computer	Threat 8	Path	Action	Date ↓
WIN_SERVER_1	Trj/ChgtI4	calc14	Blocked	6/18/2019 11:18:00 AM
WIN_SERVER_1	Trj/ChgtI2	calc12	Blocked	6/18/2019 12:20:00 AM
WIN_SERVER_1	Trj/ChgtI0	calc10	Allowed by the end	6/17/2019 11:22:00 PM

9 25 rows 1 to 25 of 66

Figura 3.12: Elementos de las pantallas de listados

- **Nombre del listado (1):** identifica el tipo de datos que se muestran en el listado.
- **Descripción (2):** caja de texto libre donde el administrador puede indicar el objetivo del listado.
- **Salvar (3):** botón que salva la vista actual y crea un nuevo listado en el árbol Mis listados
- **Menú de contexto (4):** menú desplegable con las operaciones disponibles sobre el listado (copiar y eliminar. Consulta [Operaciones con listados](#) para más información.

- **Menú de contexto (5):** menú desplegable con las opciones de exportación del listado.
- **Enlace de herramientas de filtrado y búsqueda (6):** al hacer clic se despliega un panel con las herramientas de filtrado. Una vez configuradas haz clic en el botón **Filtrar (10)**.
- **Bloque de controles de filtrado y búsqueda (7):** filtra los datos mostrados en el listado.
- **Criterio de ordenación (8):** al hacer clic en el nombre de las columnas el listado se ordena tomando como referente esa columna. Haz clic varias veces en el nombre de la columna para cambiar el sentido de la ordenación (ascendente o descendente). El sentido de ordenación se muestra mediante una flecha ascendente ↑ o descendente ↓. Si accedes a la consola de administración

desde un dispositivo móvil de menor tamaño, haz clic en el icono  situado en la esquina inferior derecha para desplegar un menú con el nombre de las columnas.

- **Paginación (9):** en el pie de la página se incluyen una serie de controles para navegar la información mostrada.

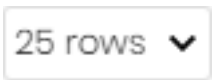
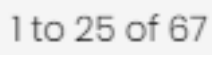
Icono	Descripción
	Selector del número de filas mostradas por página.
	Intervalo de registros mostrados del total disponible.
	Retroceso a la primera página.
	Retroceso a la página anterior a la actual.
	Acceso directo por número de páginas.
	Avance a la siguiente página.
	Avance a la última página.

Tabla 3.4: Herramientas de paginación

- **Envío programado del listado (11):** Advanced EDR permite el envío de correos electrónicos con el contenido del listado, adjuntando una exportación de los datos en formato csv. Consulta [Envío programado de informes y listados](#) en la página 785 para obtener más información.

Operaciones con listados

En el menú superior **Estado**, panel lateral **Mis listados** se muestran todos los listados que el administrador a creado previamente y los listados que Advanced EDR incorpora por defecto. Consulta [Listados incluidos por defecto](#) para más información.

Crear un listado personalizado

Hay varias formas de añadir un nuevo listado personalizado / vista:

- **Desde el panel lateral Mis listados**
 - Al hacer clic sobre el link **Añadir** del panel **Mis listados** se muestra una ventana con un desplegable que contiene las plantillas disponibles.
 - Elige una plantilla, configura las herramientas de filtrado, modifica el nombre y la descripción y pulsa el botón **Guardar (3)**.
- **Desde un panel del dashboard**
 - Haz clic en un widget en el panel de control para abrir su plantilla asociada.
 - Haz clic en el menú de contexto **(4)** y selecciona **Copiar**. Se creará un nuevo listado.
 - Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar (3)**.
- **Desde un listado ya creado**
 - Haz una copia de un listado ya generado mediante el menú contextual **(4)** y haz clic en **Copiar**. Se generará un nuevo listado con el nombre “copia de...”.
 - Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar (3)**.
- **Desde el menú de contexto del panel Mis listados**
 - Haz clic en el menú de contexto asociado al listado a copiar.
 - Haz clic en **Hacer una copia**. Se creará una nueva vista de la plantilla con el nombre “copia de...”.
 - Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar (3)**.

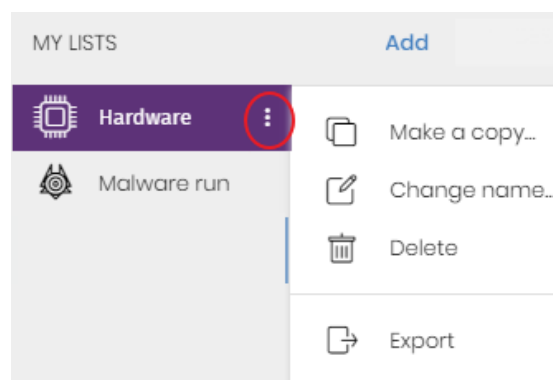


Figura 3.13: Menú de contexto de los listados accesibles desde el Panel de listados

Borrar un listado

Puedes borrar un listado de varias maneras:

- **Desde el panel Mis listados**
 - Haz clic el menú de contexto asociado al nombre del listado en el panel **Mis Listados**.
 - Haz clic en el icono .
- **Desde el propio listado**
 - Haz clic en el menú de contexto **(4)**.
 - Haz clic en el icono  del menú desplegable.

Copiar un listado

Puedes copiar un listado de varias maneras:

- Desde el panel **Mis listados**:
 - Haz clic en el menú de contexto asociado al nombre del listado en el panel **Mis listados**.
 - Haz clic en el icono .
- Desde el propio listado:
 - Haz clic en el menú de contexto **(4)**.
 - Haz clic en el icono  del menú desplegado.

Exportar un listado

Exporta un listado en formato csv para ampliar la información que se muestra en los listados de la consola Web. Los campos del fichero exportado están documentados en el capítulo correspondiente de esta Guía de administración. Puedes exportar un listado de varias maneras:

- Desde el panel **Mis listados**:
 - Si el listado no soporta la exportación del detalle haz clic en el icono . Se descargará un fichero .csv con los datos del listado.
 - Si el listado sí soporta la exportación del detalle haz clic en el icono  **(5)**. Se mostrará un menú desplegable.
 - Haz clic en **Exportar**. Se descargará un fichero .csv con los datos del listado.
- Desde el propio listado:
 - Haz clic en el menú de contexto **(4)**.
 - Haz clic en el icono  **Exportar** del menú desplegado. Se descargará un fichero .csv con los datos del listado.



Según el módulo o funcionalidad de que se trate, algunos listados pueden ofrecer un nivel mayor de detalle en los datos del fichero exportado.

Exportar los detalles de un listado

Exporta los detalles de un listado para ampliar la información mostrada en la exportación csv. Los campos del fichero exportado están documentados en el capítulo correspondiente de esta Guía de administración.

Puedes exportar un listado de varias maneras:

- **Desde el panel :**
 - Haz clic en el icono  (5). Se mostrará un menú desplegable.
 - Haz clic en **Exportación detallada**. Se descargará un fichero .csv con el detalle del listado.
- **Desde el propio listado:**
 - Haz clic en el menú de contexto (4). Se mostrará un menú desplegable.
 - Haz clic en el icono  **Exportación detallada** del menú desplegado. Se descargará un fichero .csv con el detalle del listado.



Según el módulo o funcionalidad de que se trate, algunos listados pueden ofrecer un nivel mayor de detalle en el fichero exportado.

Personalizar un listado

- Asigna un nuevo nombre al listado (1). Por defecto la consola forma un nuevo nombre para el listado añadiendo la cadena “Nuevo” al tipo de listado o “Copia” si el listado es la copia de uno anterior.
- Asigna una descripción (2): este paso es opcional.
- Haz clic en el enlace **Filtros** (6) para desplegar las herramientas de búsqueda y filtrado.
- Haz clic en **Filtrar** (10) para aplicar el filtro configurado con el objetivo de comprobar si el filtrado configurado se ajusta a las necesidades. En el cuerpo del listado se mostrará la búsqueda resultado.
- Haz clic en el botón **Guardar** (3). El listado se añadirá en el panel de la izquierda bajo **Mis listados**, y será accesible a partir de ese momento haciendo clic en su nombre.

Programar el envío de un listado

- Desde el menú de contexto del panel Listados:
 - Haz clic en el menú de contexto del listado que quieres enviar y elige la opción **Programar envío**.
 - Se mostrará una ventana con la información necesaria para enviar de forma automática la información.
- Desde el propio listado:
 - Haz clic en el icono  (11). Se mostrará una ventana con la información necesaria para enviar de forma automática la información.



Consulta [Envío programado de informes y listados](#) en la página 785 para obtener más información

Acciones sobre equipos en los listados

En algunos listados se incorporan casillas de selección por cada equipo. Al marcar uno o más equipos, se muestra la barra de acciones en la parte superior de la ventana, para facilitar la administración de los puestos de usuario y servidores seleccionados. Consulta [Barra de acciones \(10\)](#) en la página 247.

En cada página de los listados se muestra información sobre 25 equipos. Para operar sobre todos los equipos de una página, selecciona la casilla situada en la esquina superior izquierda del listado (1):

En el caso de los listados **Equipos** y **Equipos no administrados descubiertos**, una vez seleccionada la casilla se puede operar sobre todos los equipos de todas las páginas del listado (2).

The screenshot displays the 'Unmanaged computers discovered' section of the administration console. At the top, there are tabs for STATUS, COMPUTERS, SETTINGS, and TASKS. Below the title, there are action buttons: 'Hide and do not discover again', 'Delete', and 'Install Cytomic agent...'. A status bar indicates '25 selected'. Below this, a summary bar shows 'You have selected 25 rows' and a button 'Select all 47 rows in the list' (labeled 2). The main table has columns: Computer, Status, IP address, NIC manufacturer, Active Directory path, Last discovery computer, and Last seen. The first row is 'Unmanaged_WIN-SERVER-31' with status '-', and the second is 'Unmanaged_WIN-LAPTOP-28' with status 'cloud'. A red box labeled '1' highlights the selection checkbox in the first row.

Figura 3.14: Selección de equipos en los listados

Listados incluidos por defecto

La consola de administración incluye varios listados pre generados:

- Estaciones y portátiles desprotegidos.
- Servidores desprotegidos.
- Hardware
- Software

Estaciones y portátiles desprotegidos

Localiza todos los equipos de escritorio y portátiles, sin importar el sistema operativo instalado, considerados vulnerables a las amenazas debido a un problema en el funcionamiento de la protección:

- Equipos en proceso de instalación del software Advanced EDR o con error en la instalación.
- Equipos con la protección desactivada o en estado de error.
- Equipos sin licencia asignada o con licencia caducada.
- Consulta [Estado de protección de los equipos](#) en la página **621** para más información.

Servidores desprotegidos

Localiza todos los equipos de tipo servidor, sin importar el sistema operativo instalado, considerados vulnerables a las amenazas debido a un problema en el funcionamiento de la protección:

- Servidores en proceso de instalación del software Advanced EDR o con error en la instalación.
- Servidores con la protección desactivada o en estado de error.
- Servidores sin licencia asignada o con licencia caducada. Consulta [Estado de protección de los equipos](#) en la página **621** para más información.

Software

Muestra una relación de los programas instalados en el parque informático. Consulta [Software](#) en la página **212** para más información.

Hardware

Muestra una relación de los componentes hardware instalados en el parque informático. Consulta [Hardware](#) en la página **209** para más información.

Capítulo 4

Acceso, control y supervisión de la consola de administración

Advanced EDR implementa varios recursos diseñados para limitar, controlar y supervisar el acceso a su consola web de gestión, y las acciones que el administrador de la red tiene permitido ejecutar en ésta:

- Cuenta de usuario.
- Roles asignados a las cuentas de usuario.
- Registro de la actividad de las cuentas de usuario.

Contenido del capítulo

Conceptos generales	60
Gestión de cuentas de usuario	60
Crear la primera cuenta de usuario	61
Crear cuentas de usuario sucesivas	62
Cambiar los datos personales de una cuenta de usuario	63
Cambiar la dirección de correo o la contraseña de una cuenta de usuario	63
Borrar o bloquear cuentas de usuarios	64
Activar la verificación en dos pasos	64
Listado de usuarios	65
Gestión de roles y permisos	67
Conceptos básicos	67
Crear un rol	69
Borrar un rol	70
Copiar un rol	70
Modificar un rol	70

Descripción de los permisos implementados	70
Registro de la actividad de las cuentas de usuario	80
Registro de sesiones	80
Registro de acciones de usuario	81
Eventos del sistema	96

Conceptos generales

Cuenta de usuario

Es un recurso formado por un conjunto de datos que Advanced EDR utiliza para permitir el acceso de los administradores a la consola web, y establecer las acciones que éstos podrán realizar sobre los equipos de los usuarios.

Las cuentas de usuario son utilizadas únicamente por los administradores de IT que acceden a la consola web de Advanced EDR. Cada administrador puede tener una o más cuentas de usuario asignadas.

Las principales características de las cuentas de usuario son:

- Son cuentas gestionadas por el propio administrador, que puede crear o borrar cuentas nuevas, cambiar su contraseña, añadir o quitar permisos o activar la verificación en dos pasos.
- Una cuenta de usuario permite acceder a todos los productos contratados con Cytomic a través de Cytomic Central
- Una cuenta de usuario puede tener acceso a distintos clientes. El administrador podrá elegir el producto al que desea acceder en Cytomic Central, y después seleccionar la consola a la que desee acceder en la ventana **Selecciona cuenta**.

Cytomic Central

Es el portal que centraliza el acceso a todos los productos del portfolio de Cytomic. Una cuenta de usuario creada en un producto de Cytomic da acceso a este portal, desde donde el administrador puede acceder a la distintas consolas de los productos contratados.



Para más información, consulta <https://info.cytomic.ai/central/es/index.htm#t=001.htm>.

Cuenta de cliente

Es un recurso formado por datos confidenciales asociados a un cliente que tiene contratado algún producto con Cytomic. La dirección fiscal, el nombre completo, NIF y otros datos forman parte de la cuenta de cliente.

Gestión de cuentas de usuario

Una cuenta de usuario está formada por varias piezas de información que se generan en el momento de su creación:

- **Login de la cuenta:** identifica al usuario que accede a la consola.
- **Contraseña de la cuenta:** permite o impide el acceso a la consola de administración.
- **Rol asignado:** establece los equipos sobre los cuales la cuenta tiene capacidad de administración, y las acciones que puede ejecutar sobre ellos.

Crear la primera cuenta de usuario

El procedimiento para crear la primera cuenta de usuario es distinto al utilizado para crear cuentas posteriores. La primera cuenta de usuario siempre tendrá asignado el rol Control total, que permite al administrador realizar cualquier operación en la consola. Esta cuenta no se puede borrar ni modificar.

Recibe el mensaje de correo de bienvenida

- Al adquirir Advanced EDR recibirás un mensaje de correo electrónico procedente de Cytomic.
- Haz clic en el enlace **Haz clic aquí** del mensaje para acceder a la web desde donde podrás crear la primera cuenta de usuario.

Completa el formulario Crea tu cuenta Cytomic

- Escribe tu dirección de email y haz clic en el botón **Crear**. Recibirás un nuevo mensaje de correo electrónico en la dirección especificada en el formulario para activar la cuenta creada.

Activa la cuenta de usuario

- Haz clic en el botón de activación del mensaje recibido para confirmar la dirección proporcionada al crear la cuenta de usuario. Si el botón no funciona, copia en el navegador el enlace que se muestra en el mensaje. Se abrirá la ventana **Cytomic Cuenta**.
- Escribe la contraseña de la cuenta de usuario creada. Se requieren al menos 8 caracteres, de los cuales al menos uno debe ser numérico y otro debe ser una letra.
- Elige el país y haz clic en el botón **Activar cuenta**. Se mostrará la ventana **Un segundo y terminamos**.
- Escribe tu nombre y apellidos, tu fecha de nacimiento, número de teléfono y dirección y haz clic en el botón **Guardar**, o salta este paso haciendo clic en el botón **Ahora no**. Se mostrará el acuerdo de licencia de Cytomic Central.
- Haz clic en el botón **Aceptar y continuar**. Se abrirá la ventana Cytomic Central, desde donde podrás acceder a todos los servicios contratados con Cytomic.

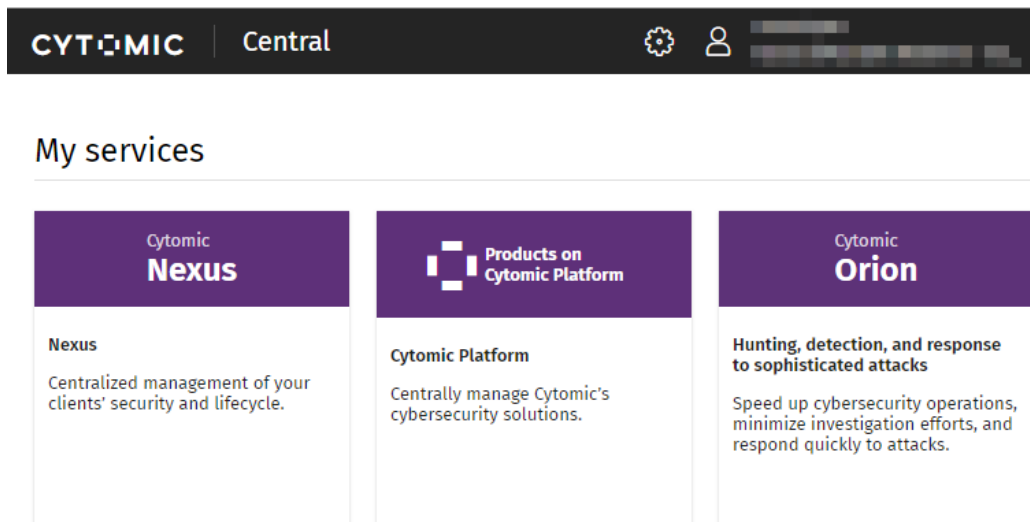


Figura 4.1: Ventana Cytomic Central

- Para acceder a la consola de Advanced EDR, haz clic en el panel Advanced EDR que encontrarás en **Mis servicios**. La primera vez que accedas se abrirá un asistente para aceptar los acuerdos de licencia y confidencialidad:
 - Haz clic en el botón **Aceptar y continuar** de la ventana **Acuerdo de licencia**.
 - Haz clic en el botón **Ir al acuerdo sobre tratamiento de datos** de la ventana **Acuerdo sobre tratamiento de datos**.
 - Haz clic en el botón **Aceptar** de la ventana **Data Processing Agreement**. Se abrirá la consola Advanced EDR.

Una vez que el proceso ha terminado, la cuenta de usuario de WatchGuard podrá acceder a la consola Advanced EDR. Consulta [Acceso la consola web](#) en la página 37.

Crear cuentas de usuario sucesivas

Una vez creada la primera cuenta de usuario, el administrador tendrá acceso a la consola de administración de Advanced EDR, desde donde se pueden crear el resto de cuenta de usuario que necesite.

- Comprueba que el usuario tiene asignado el permiso **Gestionar usuarios y roles**. Consulta [Descripción de los permisos implementados](#).
- En el menú superior **Configuración** haz clic en el menú lateral **Usuarios**.
- Haz clic en la pestaña **Usuarios**. Se mostrará el listado de usuarios creados en la consola de administración.
- Haz clic en el botón **Añadir**. Se abrirá la ventana **Añadir usuario**.
- Escribe la cuenta de correo del usuario de la consola en el campo **Email de acceso** y la descripción si es necesaria.

- Indica el rol que tendrá asignada la cuenta de usuario. Consulta [Descripción de los permisos implementados](#).
- Haz clic en el botón **Guardar**. Advanced EDR enviará un correo a la cuenta de correo indicada para que el usuario pueda generar una contraseña de acceso y aceptar los términos de la licencia y el tratamiento de sus datos.



Antes de iniciar este procedimiento, comprueba que has cerrado la sesión en WatchGuard Portal y en la consola de Advanced EDR, así como el navegador web.

Cambiar los datos personales de una cuenta de usuario

- Haz clic en el icono situado en la parte superior derecha de la consola de administración. Se abrirá un menú desplegable.
- Haz clic en **Configurar mi perfil**.

Cytomic Central

- Se abrirá la ventana **Cytomic cuenta**.
- Haz clic en el panel izquierdo **Información personal** y escribe en el formulario los datos personales de la cuenta.
- Haz clic en el botón **Guardar**. Los cambios se almacenarán en el servidor de Cytomic.

Cambiar la dirección de correo o la contraseña de una cuenta de usuario

- Haz clic en el icono situado en la parte superior derecha de la consola de administración. Se abrirá un menú desplegable.
- Haz clic en **Configurar mi perfil**.

Cytomic Central

- Se abrirá la ventana **Cytomic cuenta**.
- Haz clic en el panel izquierdo **Inicio de sesión** y en los enlaces **Cambiar dirección de email** o **Cambiar contraseña**. Se abrirá una ventana para validar la información antigua e introducir la nueva.
- Haz clic en el botón **Cambiar**.

Borrar o bloquear cuentas de usuarios

- Comprueba que el usuario tiene asignado el permiso **Gestionar usuarios y roles**. Consulta [Descripción de los permisos implementados](#).
- En el menú superior **Configuración** haz clic en el menú lateral **Usuarios**.
- Haz clic en la pestaña **Usuarios**. Se mostrará el listado de usuarios creados en la consola de administración.
- Haz clic en el icono  asociado a la cuenta de usuario que quieres borrar.
- Para desactivar temporalmente el acceso de la cuenta a la consola web, haz clic en una cuenta de usuario y desplaza el control deslizante **Bloquear este usuario**. De esta manera, esa cuenta tendrá denegado el acceso a la consola de administración, y si ya está conectada será expulsada de forma inmediata. También dejará de recibir alertas por correo en las direcciones de correo especificadas en su configuración.

Activar la verificación en dos pasos

Advanced EDR es compatible con el estándar 2FA (Two Factor Authentication), que añade una capa de seguridad adicional a la establecida en el esquema básico “usuario - contraseña”. De esta manera, cuando el administrador de la red accede a la consola web, se introduce un elemento nuevo en el sistema de autenticación básico: un código que solo posee el propietario de la cuenta. Este código es aleatorio y solo puede generarse en un dispositivo concreto, normalmente el teléfono móvil o tablet personal del administrador de Advanced EDR.

Requisitos para activar 2FA

- Acceso a un teléfono móvil o tablet personal con cámara de fotos integrada.
- Descarga la aplicación gratuita WatchGuard AuthPoint (o una aplicación equivalente) en:
 - iOS: <https://apps.apple.com/app/watchguard-authpoint/id1335115425>
 - Android: <https://play.google.com/store/apps/details?id=com.watchguard.authpoint>

Activar 2FA

- Haz clic en el icono situado en la parte superior derecha de la consola de administración. Se abrirá un menú desplegable.
- Haz clic en **Configurar mi perfil**.

Cytomic Central

- Se abrirá la ventana **Cytomic cuenta**.
- Haz clic en el panel izquierdo **Inicio de sesión** y en el enlace **Activar** de la sección **Verificación en dos pasos**. Se abrirá la ventana **Sincronización con la app de autenticación**.

- Si es la primera vez que utilizas la aplicación WatchGuard AuthPoint en tu dispositivo móvil, pulsa el botón **Activar**. Si ya la has utilizado anteriormente, pulsa en el icono del QR situado en la esquina superior derecha. Se abrirá la cámara de fotos del dispositivo móvil.



Figura 4.2: Escaneo del código QR con WatchGuard Authpoint

- Enfoca con la cámara el código QR que se muestra en la consola de Advanced EDR. Se añadirá una nueva entrada en WatchGuard AuthPoint y se empezarán a generar tokens cada 30 segundos.
- Escribe el código generado por WatchGuard AuthPoint en la consola de Advanced EDR para enlazar el dispositivo con la cuenta de usuario, y haz clic en el botón **Verificar**. Se abrirá una ventana con el mensaje **Se ha activado la verificación en dos pasos**.
- Haz clic en el botón **Aceptar**.

Acceder a la consola Web mediante una cuenta con 2FA activado desde Cytomic Central

- Accede a <https://www.pandacloudsecurity.com/PandaLogin/> escribe el usuario y la contraseña y haz clic en el botón **Iniciar sesión**.
- Introduce el código de verificación generado por WatchGuard AuthPoint en tu dispositivo móvil y haz clic en el botón **Verificar**. Se abrirá la ventana **Cytomic Central**.

Forzar la activación de 2FA a todos los usuarios de la consola

Es necesario que la cuenta de usuario que forzará el uso de 2FA tenga el permiso **Gestionar usuarios y roles** y visibilidad completa sobre el parque informático. Consulta [Gestión de roles y permisos](#)

- En el menú superior **Configuración** haz clic en la pestaña **Seguridad**.
- Activa la opción **Exigir tener activada la verificación en dos pasos para acceder a esta cuenta**.
- Si la cuenta de usuario que activa la funcionalidad 2FA para todos los usuarios de la consola no tiene activada la verificación en dos pasos para su propia cuenta, se mostrará una ventana de aviso que le permitirá acceder a la **Cuenta Cytomic** para activarlo. Consulta [Activar 2FA](#).

Listado de usuarios

Permisos requeridos

Todos los usuarios de la consola pueden ver el listado de usuarios.

Acceso al listado

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**.
- Haz clic en la pestaña **Usuarios**. Se mostrará un listado con todas las cuentas de usuario creadas en Advanced EDR con la información mostrada a continuación:

Campo	Descripción
Nombre de la cuenta	Nombre de la cuenta de usuario.
Rol	Rol asignado a la cuenta de usuario.
Cuenta de correo	Cuenta de correo asignada al usuario.
Candado	Indica si la cuenta tiene activada la funcionalidad de 2FA (Verificación en dos pasos / factores, Two Factor Authentication).
Estado	Indica si la cuenta de usuario esta activada o bloqueada.

Tabla 4.1: Campos del listado de usuarios

Organizar y buscar en el listado de usuarios: haz clic en el icono  para organizar el listado de usuarios de manera ascendente / descendente, por nombre o por fecha creación. Para buscar un usuario, escribe el texto en el cuadro de búsqueda y haz clic en el icono .

Campos mostrados en fichero exportado

Campo	Definición	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Nombre	Nombre del perfil de usuario.	Cadena de caracteres
Email de acceso	Email con el que se ha accedido a la consola.	Cadena de caracteres
Rol	Rol asignado al usuario.	Cadena de caracteres

Campo	Definición	Valores
Descripción	Descripción añadida al perfil de usuario.	Cadena de caracteres
Verificación en dos pasos	Indica si la cuenta tiene activada o desactivada la verificación en dos pasos.	Booleano
Bloqueado	Indica si la cuenta de usuario esta activada o bloqueada.	Booleano

Tabla 4.2: Campos de fichero exportado Listado de usuarios

Herramientas de filtrado

Campo	Comentario	Valores
Buscar usuario	Busca por el nombre y la cuenta de correo del usuario. Permite búsquedas parciales de cadenas.	Cadena de caracteres
Bloqueados	Filtra las cuentas de usuario bloqueadas del listado.	• Todos • Si • No
Verificación en dos pasos	Filtra las cuentas de usuario que tienen activado el sistema de verificación en dos pasos.	• Todos • Activado • Desactivado

Tabla 4.3: Campos de filtrado para el listado Estado de Cytomic Data Watch

Herramientas de ordenación

Para mostrar los criterios de ordenación disponibles, haz clic en el icono .

Gestión de roles y permisos

Conceptos básicos

Roles

Un rol es una configuración específica de permisos que se aplica a una o más cuentas de usuario. Una cuenta de usuario estará autorizada a ver o modificar determinados recursos de la consola, dependiendo de rol que tenga asignado.

Una cuenta de usuario solo puede tener un único rol asignado, aunque un mismo rol puede estar asignado a una o más cuentas de usuario.

Un rol está formado por los siguientes elementos:

- **Nombre del rol:** designado en el momento de la creación del rol, su objetivo es meramente identificativo.
- **Visibilidad:** restringe el acceso a determinados equipos de la red.
- **Juego de permisos:** determina las acciones concretas que las cuentas de usuario pueden ejecutar sobre los equipos que pertenecen a los grupos definidos con accesibles.

Roles predefinidos

Una licencia de Advanced EDR siempre incluye dos roles predefinidos. Estos roles no se pueden editar ni borrar y cualquier cuenta de usuario puede pertenecer a estos roles previa asignación en la consola Web:

El rol Control total

La primera cuenta de usuario que se crea siempre tiene el rol Control total asignado, y permite ejecutar todas las acciones disponibles en la consola sobre todos los equipos integrados en Advanced EDR.

El rol Solo lectura

Este rol permite el acceso a todas las secciones de la consola, pero no permite crear, modificar o borrar configuraciones, tareas, etc, por lo que permite una visión total del entorno pero sin ninguna modificación. Está especialmente indicado para aquellos administradores de red encargados de la vigilancia del parque informático, pero que no poseen los permisos suficientes para realizar modificaciones, como por ejemplo editar configuraciones o lanzar análisis bajo demanda.

Permiso

Un permiso regula el acceso a una sección concreta de la consola de administración. Existen varios permisos que establecen el acceso a otros tantos aspectos de la consola de Advanced EDR. Una configuración particular de todos los permisos disponibles forma un rol, que puede ser asignado a una o más cuentas de usuario.

Visibilidad

Cada cuenta de usuario puede configurar la seguridad de un subconjunto de equipos determinado por su visibilidad, de entre todos los equipos integrados en la consola de Advanced EDR.

Crear un rol

Figura 4.3: Ventana Cytomic Central

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**. Se abrirá una ventana con el listado de usuarios creados.
- Haz clic en la pestaña **Roles** y en el botón **Añadir**. Se abrirá la ventana **Añadir rol**.
- Escribe el nombre del rol (1) y una descripción opcional (2).
- Indica la visibilidad del rol (3).
- Activa o desactiva los permisos (4).
- Haz clic en el botón **Guardar** (5).

Limitaciones en la creación de usuarios y roles

Para evitar una situación de escalado de permisos, los usuarios con el permiso **Gestionar usuarios y roles** activo tienen las siguientes limitaciones a la hora de crear roles o asignarlos a otros usuarios ya creados:

- Una cuenta de usuario solo puede crear roles nuevos con los mismos permisos o menos de los que tiene asignada.
- Una cuenta de usuario sólo puede editar los permisos que tenga activos en los roles ya existentes. El resto permanecerán desactivados.
- Una cuenta de usuario no puede asignar un rol a un usuario si ese rol tiene más permisos asignados que la cuenta de usuario.

- Una cuenta de usuario no puede copiar un rol si ese rol tiene más permisos asignados que la cuenta de usuario.

Borrar un rol

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**.
- Haz clic en la pestaña **Roles**. Se mostrará el listado de roles creados.
- Haz clic sobre el icono  de un rol para borrarlo. Si al borrar un rol éste ya tiene cuentas de usuario asignadas, se cancela el proceso de borrado.

Copiar un rol

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**.
- Haz clic en la pestaña **Roles**. Se mostrará el listado de roles creados.
- Haz clic sobre el icono  de un rol para copiarlo. Se abrirá la ventana **Copiar rol** con la configuración del rol copiado.
- Modifica la configuración del rol copiado y haz clic en el botón **Guardar**.

Modificar un rol

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**.
- Haz clic en la pestaña **Roles**. Se mostrará el listado de roles creados.
- Haz clic en el rol a editar. Se abrirá la ventana **Editar rol**.
- Modifica la configuración del rol y haz clic en el botón **Guardar**.

Descripción de los permisos implementados

Gestionar usuarios y roles

- **Al activar:** el usuario de la cuenta puede crear, borrar y editar cuentas de usuario y roles.
- **Al desactivar:** el usuario de la cuenta deja de poder crear, borrar y editar cuentas de usuario y roles. Se permite ver el listado de usuarios dados de alta y los detalles de las cuentas, pero no el listado de roles creados.

Asignar licencias

- **Al activar:** el usuario de la cuenta puede asignar y retirar licencias de los equipos gestionados.
- **Al desactivar:** el usuario de la cuenta no puede asignar y retirar licencias, pero puede ver si los equipos tienen licencias asignadas.

Modificar el árbol de equipos

- **Al activar:** el usuario de la cuenta tiene pleno acceso al árbol de grupos y puede crear y eliminar grupos, y mover equipos a grupos ya creados.
- **Al activar con conflicto de permisos:** debido a los mecanismos de herencia que se aplican en el árbol de equipos, cualquier modificación en la estructura del mismo puede implicar un cambio de asignación de configuración para los dispositivos. Por ejemplo, en los casos en los que el administrador no tiene permisos para asignar configuraciones, y mueve un equipo de un grupo a otro, la consola web mostrará una advertencia indicando que debido al movimiento de equipos efectuado y a los mecanismos de herencia que se aplican la asignación de configuraciones de los equipos que se han movido podría cambiar (aunque el administrador no tenga permisos para asignar configuraciones). Consulta el apartado [Asignación manual y automática de configuraciones](#) en la página 261.
- **Al desactivar:** el usuario de la cuenta puede visualizar el árbol de carpetas y las configuraciones asignadas a cada grupo, pero no puede crear nuevos grupos ni mover equipos.

Añadir, descubrir y eliminar equipos

- **Al activar:** el usuario de la cuenta puede distribuir el instalador entre los equipos de la red e integrarlos en la consola, eliminarlos y configurar toda la funcionalidad relativa al descubrimiento de puestos no gestionados: asignar y retirar el rol de descubridor a los equipos, editar las opciones de descubrimiento, lanzar descubrimientos inmediatos e instalar el agente de Cytomic de forma remota desde los listados de equipos descubiertos.
- **Al desactivar:** el usuario de la cuenta no puede descargar el instalador, ni por lo tanto distribuirlo entre los equipos de la red. Tampoco puede eliminar equipos previamente integrados ni gestionar la funcionalidad relativa al descubrimiento de equipos no gestionados.

Modificar configuración de red (proxys y caché)

- **Al activar:** el usuario de la cuenta puede crear nuevas configuraciones de tipo **Configuración de red**, editar o borrar las existentes y asignarlas a los equipos integrados en la consola.
- **Al desactivar:** el usuario de la cuenta deja de poder crear nuevas configuraciones de tipo **Configuración de red**, borrar las existentes o cambiar la asignación de los equipos integrados a la consola.

Configurar ajustes por equipo (actualizaciones, contraseñas, etc.)

- **Al activar:** el usuario de la cuenta puede crear nuevas configuraciones de tipo **Ajustes por equipo**, editar y borrar las ya creadas y asignar a los equipos integrados en la consola.
- **Al desactivar:** el usuario de la cuenta deja de poder crear nuevas configuraciones de tipo **Ajustes por equipo**, borrar las existentes o cambiar la asignación de los equipos integrados a la consola.

Configurar control remoto

- **Al activar:** el usuario de la cuenta puede crear, editar, borrar y asignar configuraciones de acceso remoto a equipos de la red con sistema operativo Windows instalado.
- **Al desactivar:** el usuario de la cuenta no puede crear, editar, borrar y asignar configuraciones de acceso remoto a los equipos de la red.

Control remoto de equipos

- **Al activar:** el usuario de la cuenta puede acceder remotamente a los equipos de la red con sistema operativo Windows instalado y sobre los que tenga visibilidad.
- **Al desactivar:** el usuario de la cuenta no puede acceder remotamente a los equipos de la red.

Reiniciar y reparar equipos

- **Al activar:** el usuario de la cuenta puede reiniciar equipos desde los listados de equipos en estaciones y servidores. También puede iniciar la reinstalación remota del software Advanced EDR en equipos Windows.
- **Al desactivar:** el usuario de la cuenta deja de poder reiniciar equipos y de reinstalar remotamente el software Advanced EDR.

Aislar equipos

- **Al activar:** el usuario de la cuenta puede aislar y dejar de aislar equipos Windows y macOS.
- **Al desactivar:** el usuario de la cuenta deja de poder aislar equipos.

Configurar seguridad para estaciones y servidores

- **Al activar:** el usuario de la cuenta puede crear, editar, borrar y asignar configuraciones de seguridad para estaciones y servidores.
- **Al desactivar:** el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de seguridad para estaciones y servidores.

Al desactivar este permiso se mostrará el permiso **Ver configuraciones de seguridad para estaciones y servidores**.

Ver configuraciones de seguridad para estaciones y servidores



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar la seguridad para estaciones y servidores.

- **Al activar:** el usuario de la cuenta puede únicamente visualizar las configuraciones de seguridad creadas, así como ver la configuración de un equipo o de un grupo.
- **Al desactivar:** el usuario de la cuenta deja de poder ver las configuraciones de seguridad creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Visualizar detecciones y amenazas

- **Al activar:** el usuario de la cuenta puede acceder a los paneles y listados de la sección **Seguridad** en el menú superior **Estado**, y crear nuevos listados con filtros personalizados.
- **Al desactivar:** el usuario de la cuenta no puede visualizar ni acceder a los paneles y listados de la sección **Seguridad** en el menú superior **Estado**, ni crear nuevos listados con filtros personalizados.



*El acceso a la funcionalidad relativa a la exclusión y desbloqueo de amenazas y elementos desconocidos se establece mediante el permiso **Excluir temporalmente amenazas Malware, PUP y Bloqueados**.*

Desinfectar

- **Al activar:** el usuario de la cuenta puede crear, editar, modificar y borrar tareas de tipo análisis y desinfección.
- **Al desactivar:** el usuario de la cuenta no puede crear, editar, modificar ni borrar las tareas ya creadas de tipo análisis. Únicamente podrá listar las tareas y visualizar su configuración.

Buscar y administrar IOCs

- **Al activar:** el usuario de la cuenta puede acceder a todas las operaciones con IOCs: realizar búsquedas, gestión de la galería de IOCs, consultas del panel de control, acceso a las tareas de IOCs, visualizar los listados de IOCs, etc.
- **Al desactivar:** el usuario de la cuenta no puede acceder a ninguna de las operaciones que involucren IOCs.

Excluir temporalmente amenazas Malware, PUP y Bloqueados

- **Al activar:** el usuario de la cuenta puede desbloquear, no volver a detectar, bloquear, dejar de permitir y cambiar el comportamiento ante reclasificaciones de malware, PUP y desconocidos en clasificación.
- **Al desactivar:** el usuario de la cuenta no podrá desbloquear, no volver a detectar, bloquear, dejar de permitir y cambiar el comportamiento ante reclasificaciones de malware, PUP y desconocidos en clasificación.



Es necesario activar Visualizar detecciones y amenazas para poder ejercer completamente Excluir temporalmente amenazas Malware, PUP y Bloqueados.

Configurar gestión de parches

- **Al activar:** el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de gestión de parches para equipos Windows, macOS y Linux.
- **Al desactivar:** el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de gestión de parches para equipos Windows, macOS y Linux.

Al desactivar este permiso se mostrará el permiso **Visualizar configuraciones de gestión de parches**.

Visualizar configuraciones de gestión de parches



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar gestión de parches.

- **Al activar:** el usuario de la cuenta podrá únicamente visualizar las configuraciones de gestión de parches creadas, así como ver la configuración asignadas a un equipo o a un grupo.
- **Al desactivar:** el usuario de la cuenta dejará de poder ver las configuraciones Gestión de parches creadas, y tampoco podrá acceder a las configuraciones asignadas a cada equipo.

Instalar / desinstalar y excluir parches

- **Al activar:** el usuario de la cuenta podrá crear tareas de parcheo, desinstalación y exclusión de parches, así como acceder a los listados **Parches disponibles**, **Programas "End of life"**, **Historial de instalaciones** y **Parches excluidos**.
- **Al desactivar:** el usuario de la cuenta dejará de poder crear tareas de parcheo, desinstalación y exclusión de parches.

Visualizar parches disponibles



Este permiso solo es accesible cuando se ha deshabilitado el permiso Instalar / desinstalar y excluir parches

- **Al activar:** el usuario de la cuenta podrá acceder a los listados **Estado de gestión de parches**, **Parches disponibles**, **Programas “End of life”** e **Historial de instalaciones**.
- **Al desactivar:** el usuario de la cuenta dejará de poder acceder a los listados **Parches disponibles**, **Programas “End of life”** e **Historial de instalaciones**.

Configurar Evaluación de vulnerabilidades

- **Al activar:** el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de evaluación de vulnerabilidades para equipos Windows, macOS y Linux.
- **Al desactivar:** el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de evaluación de vulnerabilidades para equipos Windows, macOS y Linux.

Al desactivar este permiso se mostrará el permiso **Visualizar configuraciones de evaluación de vulnerabilidades**.

Visualizar configuraciones de evaluación de vulnerabilidades



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar evaluación de vulnerabilidades.

- **Al activar:** el usuario de la cuenta podrá únicamente visualizar las configuraciones de evaluación de vulnerabilidades creadas, así como ver la configuración asignadas a un equipo o a un grupo.
- **Al desactivar:** el usuario de la cuenta dejará de poder ver las configuraciones de evaluación de vulnerabilidades, y tampoco podrá acceder a las configuraciones asignadas a cada equipo.

Visualizar parches disponibles



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar gestión de parches.

- **Al activar:** el usuario de la cuenta podrá acceder a los listados **Estado de la evaluación de vulnerabilidades**, **Parches disponibles por equipos** y **Programas “End of life”**.
- **Al desactivar:** el usuario de la cuenta dejará de poder acceder a los listados **Estado de la evaluación de vulnerabilidades**, **Parches disponibles por equipos** y **Programas “End of life”**.

Configurar bloqueo de programas

- **Al activar:** el usuario de la cuenta puede crear, editar, borrar y asignar configuraciones de bloqueo de programas para estaciones y servidores Windows.
- **Al desactivar:** el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de bloqueo de programas para estaciones y servidores Windows.

Al desactivar este permiso se mostrará el permiso **Ver configuraciones de bloqueo de programas**.

Ver configuraciones de bloqueo de programas



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar bloqueo de programas.

- **Al activar:** el usuario de la cuenta puede únicamente visualizar las configuraciones de bloqueo de programas, así como ver la configuración de un equipo o de un grupo.
- **Al desactivar:** el usuario de la cuenta deja de poder ver las configuraciones de bloqueo de programas creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Configurar software autorizado

- **Al activar:** el usuario de la cuenta puede crear, editar, borrar y asignar configuraciones de software autorizado para estaciones y servidores Windows.
- **Al desactivar:** el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de software autorizado para estaciones y servidores Windows.

Al desactivar este permiso se mostrará el permiso **Ver configuración de software autorizado**.

Ver configuración de software autorizado



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar software autorizado.

- **Al activar:** el usuario de la cuenta puede únicamente visualizar las configuraciones de software autorizado, así como ver la configuración de un equipo o de un grupo.
- **Al desactivar:** el usuario de la cuenta deja de poder ver las configuraciones de software autorizado creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Configurar indicadores de ataque (IOA)

Al activar: el usuario de la cuenta puede crear, editar, borrar y asignar configuraciones de indicadores de ataque (IOA).

- **Al desactivar:** el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de indicadores de ataque (IOA).
- Al desactivar este permiso se mostrará el permiso Ver configuración de indicadores de ataque (IOA).

Ver configuración de indicadores de ataque (IOA)



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar indicadores de ataque (IOA).

- **Al activar:** el usuario de la cuenta puede únicamente visualizar las configuraciones de indicadores de ataque (IOA) creadas, así como ver la configuración de un equipo o de un grupo.
- **Al desactivar:** el usuario de la cuenta deja de poder ver las configuraciones de indicadores de ataque (IOA) creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Configurar Cytomic Data Watch

- **Al activar:** el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de Cytomic Data Watch en equipos Windows.
- **Al desactivar:** el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de Cytomic Data Watch en equipos Windows.

Ver configuraciones de Cytomic Data Watch



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar inventario, seguimiento y búsqueda de información sensible.

- **Al activar:** el usuario de la cuenta podrá únicamente visualizar las configuraciones de Cytomic Data Watch, así como ver la configuración de un equipo o de un grupo.
- **Al desactivar:** el usuario de la cuenta dejará de poder ver las configuraciones de Cytomic Data Watch creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Buscar información en los equipos

- **Al activar:** el usuario de la cuenta podrá acceder al widget de **Búsquedas** para localizar ficheros por nombre y contenido almacenados en los equipos de los usuarios.
- **Al desactivar:** el usuario de la cuenta dejará de poder acceder al widget Búsquedas.

Visualizar inventario de información personal

- **Al activar:** el usuario de la cuenta podrá acceder a los listados **Archivos con información personal** y **Equipos con información personal**, así como a los widgets **Archivos con información personal**, **Equipos con información personal** y **Archivos por tipo de información personal**.
- **Al desactivar:** el usuario de la cuenta dejará de tener acceso a los listados **Archivos con información personal** y **Equipos con información personal**, así como a los widgets **Archivos con información personal**, **Equipos con información personal** y **Archivos por tipo de información personal**.

Eliminar y restaurar archivos

- **Al activar:** el usuario de la cuenta puede acceder a la opción **Eliminar** del menú de contexto en el listado **Archivos con información personal** para borrar y restaurar ficheros.
- **Al desactivar:** el usuario de la cuenta no puede acceder a la opción **Eliminar** del menú de contexto en el listado **Archivos con información personal** y por lo tanto no puede borrar ni restaurar ficheros.

Configurar cifrado de equipos

- **Al activar:** el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de cifrado.
- **Al desactivar:** el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de cifrado.

Ver configuraciones de cifrado de equipos



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar cifrado de equipos.

- **Al activar:** el usuario de la cuenta podrá únicamente visualizar las configuraciones de cifrado de equipos, así como ver la configuración asignadas a un equipo o a un grupo.
- **Al desactivar:** el usuario de la cuenta dejará de poder ver las configuraciones de cifrado creadas, y tampoco podrá acceder a las configuraciones asignadas a cada equipo.

Acceder a las claves de recuperación de unidades cifradas

- **Al activar:** el usuario de la cuenta podrá visualizar las claves de recuperación para los equipos con dispositivos de almacenamiento cifrados y administrados por Advanced EDR.
- **Al desactivar:** el usuario de la cuenta no podrá visualizar las claves de recuperación para los equipos con dispositivos de almacenamiento cifrados.

Acceder a información avanzada de seguridad

- **Al activar:** el usuario de la cuenta podrá acceder a la herramienta Cytomic Insights desde el menú superior **Estado**, panel izquierdo Cytomic Insights pero la aplicación Data Access Control no es visible con este permiso.
- **Al desactivar:** se impide el acceso a la herramienta Cytomic Insights.

Acceder a información de acceso a archivos

- **Al activar:** el usuario de la cuenta podrá acceder a la herramienta Cytomic Insights desde el menú superior **Estado**, panel izquierdo **Cytomic Insights**. La aplicación Data Access Control es accesible con este permiso.
- **Al desactivar:** se impide el acceso a la herramienta Cytomic Insights.

Acceder a información avanzada de Cytomic Data Watch

- **Al activar:** el usuario de la cuenta podrá acceder a la consola extendida de Cytomic Data Watch desde el menú superior **Estado**, panel izquierdo **Cytomic Insights**.
- **Al desactivar:** el usuario de la cuenta no podrá acceder a la consola extendida de Cytomic Data Watch desde el menú superior **Estado**, panel izquierdo **Cytomic Insights**.

Configurar MDR

- **Al activar:** el usuario de la cuenta puede crear, editar o borrar la configuración de MDR para todos los equipos de la red.
- **Al desactivar:** el usuario de la cuenta dejará de poder crear, editar o borrar la configuración de MDR para todos los equipos de la red.

Al desactivar este permiso se mostrará el permiso **Ver configuración de MDR**.

Ver configuración de MDR



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar MDR.

- **Al activar:** el usuario de la cuenta puede únicamente visualizar la configuración de MDR.
- **Al desactivar:** el usuario de la cuenta deja de poder ver la configuración de MDR.

Registro de la actividad de las cuentas de usuario

Advanced EDR registra todas las acciones efectuadas por los administradores de red en la consola web de gestión para determinar quién realizó un cambio, en que momento y sobre qué objeto.

Para acceder a la sección de actividad haz clic en el menú superior **Configuración** y después en la pestaña **Actividad**.

Registro de sesiones

La sección de sesiones lista todos los accesos a la consola de administración, los exporta a formato csv y filtra la información.

Campos mostrados en el listado de sesiones

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se produce el acceso.	Fecha
Usuario	Cuenta de usuario que accede.	Cadena de caracteres
Actividad	Acción que ejecuta la cuenta.	• Iniciar sesión • Cerrar sesión
Dirección IP	Dirección IP desde donde se produce el acceso.	Cadena de caracteres

Tabla 4.4: Campos del listado sesiones

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se produce el acceso	Fecha
Usuario	Cuenta de usuario que accede.	Cadena de caracteres
Actividad	Acción que ejecuta la cuenta	• Iniciar sesión • Cerrar sesión

Campo	Descripción	Valores
Dirección IP	Dirección IP desde donde se produce el acceso.	Cadena de caracteres

Tabla 4.5: Campos del fichero exportado sesiones

Herramienta de búsqueda

Campo	Descripción	Valores
Desde	Establece el limite inferior del intervalo de búsqueda.	Fecha
Hasta	Establece el limite superior del intervalo de búsqueda.	Fecha
Usuarios	Nombre del usuario.	Listado de cuentas de usuario creados en la consola de administración.

Tabla 4.6: Campos de filtrado para el listado de sesiones

Registro de acciones de usuario

La sección de **Acciones de usuario** lista todas las acciones ejecutadas por las cuentas de usuario, exporta las acciones a formato csv y filtra la información.

Campos mostrados en el listado de acciones

Campo	Descripción	Valores
Fecha	Fecha y hora en la que ha producido la acción.	Fecha
Usuario	Cuenta de usuario que ejecutó la acción.	Cadena de caracteres.
Acción	Tipo de operación ejecutada.	Consulta la tabla Tipos de elementos y acciones .
Tipo de elemento	Tipo del objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla Tipos de elementos y acciones .

Campo	Descripción	Valores
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla Tipos de elementos y acciones .

Tabla 4.7: Campos del Registro de acciones

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se ha producido la acción.	Fecha
Usuario	Cuenta de usuario que ejecutó la acción.	Cadena de caracteres
Acciones	Tipo de operación realizada.	Consulta la tabla Tipos de elementos y acciones .
Tipo de elemento	Tipo del objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla Tipos de elementos y acciones .
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla Tipos de elementos y acciones .

Tabla 4.8: Campos del fichero exportado Registro de acciones

Herramienta de búsqueda

Campo	Descripción	Valores
Desde	Establece el límite inferior del intervalo de búsqueda.	Fecha
Hasta	Establece el límite superior del intervalo de búsqueda.	Fecha
Usuarios	Nombre del usuario encontrado.	Listado de cuentas de usuario creados en la consola de administración.

Tabla 4.9: Campos de filtrado para el Registro de acciones

Tipos de elementos y acciones

Tipo de elemento	Acción	Elemento
Acuerdo de licencia	Aceptar	Número de versión del EULA aceptado.
Amenaza	Permitir	Nombre de la amenaza sobre la que el usuario realizó la acción.
	Dejar de permitir	Nombre de la amenaza sobre la que el usuario realizó la acción.
Búsqueda de información	Lanzar	Nombre de la búsqueda sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la búsqueda sobre la que el usuario realizó la acción.
	Cancelar	Nombre de la búsqueda sobre la que el usuario realizó la acción.
Cuenta	Actualizar consola	De Versión origen a Versión destino.
	Cancelar actualización de consola	De Versión origen a Versión destino.
Configuración - 'Control remoto'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Configuración de red'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Indicadores de ataque (IOA)'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Ajustes por equipo'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Bloqueo de programas'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Estaciones y servidores'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
Configuración - 'Información personal'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Cytomic Patch'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración Control de Acceso a Endpoints	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Cytomic Encryption'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - Evaluación de vulnerabilidades	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Software autorizado'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Envío programado	Crear	Nombre del envío programado sobre el que el usuario realizó la acción.
	Editar	Nombre del envío programado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del envío programado sobre el que el usuario realizó la acción.
Equipo	Eliminar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Editar nombre	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Editar descripción	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Cambiar Grupo	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Control remoto	Nombre del dispositivo sobre el que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Intento de control remoto	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Proxy e idioma'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Proxy e idioma'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Ajustes por equipo'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Ajustes por equipo'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Estaciones y servidores'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Estaciones y servidores'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Información sensible'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Información sensible'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar licencia	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Desasignar licencia	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reiniciar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Bloquear	Nombre del dispositivo sobre el que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Designar Proxy Cytomic	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar Proxy Cytomic	Nombre del equipo sobre el que el usuario realizó la acción.
	Designar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Configurar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Designar equipo descubridor	Nombre del equipo sobre el que el usuario realizó la acción.
	Configurar descubrimiento	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar equipo descubridor	Nombre del equipo sobre el que el usuario realizó la acción.
	Descubrir ahora	Nombre del equipo sobre el que el usuario realizó la acción.
	Mover a su ruta de Active Directory	Nombre del equipo sobre el que el usuario realizó la acción.
	Activar modo Detallado	Nombre del equipo sobre el que el usuario realizó la acción.
	Desactivar modo Detallado	Nombre del equipo sobre el que el usuario realizó la acción.
	Aislar	Nombre del dispositivo sobre el que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Dejar de aislar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Desinstalar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reinstalar agente	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reinstalar protección	Nombre del dispositivo sobre el que el usuario realizó la acción
	Finalizar el modo “Contención de ataque RDP” en el equipo.	Nombre del dispositivo sobre el que el usuario realizó la acción.
Equipo no administrado	Ocultar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Visibilizar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Editar descripción	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Instalar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
Filtro	Crear	Nombre del filtro sobre el que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Editar	Nombre del filtro sobre el que el usuario realizó la acción.
	Eliminar	Nombre del filtro sobre el que el usuario realizó la acción.
Grupo	Crear	Nombre del grupo sobre el que el usuario realizó la acción.
	Editar	Nombre del grupo sobre el que el usuario realizó la acción.
	Eliminar	Nombre del grupo sobre el que el usuario realizó la acción.
	Cambiar Grupo-Padre	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de Proxy e idioma	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de Proxy e idioma	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Ajustes por Equipo'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Ajustes por Equipo'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Estaciones y servidores'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Estaciones y servidores'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Información sensible'	Nombre del grupo sobre el que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Heredar configuración de 'Información sensible'	Nombre del grupo sobre el que el usuario realizó la acción.
	Sincronizar grupo	Nombre del grupo sobre el que el usuario realizó la acción.
	Mover equipos a su ruta de Active Directory	Nombre del grupo sobre el que el usuario realizó la acción.
Informes avanzados	Acceder	
IOA	Archivar para un equipo	Nombre del IOA (Nombre del equipo).
	Marcar como pendiente para un equipo	Nombre del IOA (Nombre del equipo).
IOC	Crear (mediante importación)	Nombre del IOC sobre el que el usuario realizó la acción
	Eliminar	Nombre del IOC sobre el que el usuario realizó la acción
	Crear (mediante asistente)	Nombre del IOC sobre el que el usuario realizó la acción
	Editar	Nombre del IOC sobre el que el usuario realizó la acción.
Listado	Crear	Nombre del listado sobre el que el usuario realizó la acción.
	Editar	Nombre del listado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del listado sobre el que el usuario realizó la acción.
Control de acceso a redes	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
Parche	Excluir para un equipo	Nombre del parche sobre el que el usuario realizó la acción.
	Excluir para todos los equipos	Nombre del parche sobre el que el usuario realizó la acción.
	Dejar de excluir para un equipo	Nombre del parche sobre el que el usuario realizó la acción.
	Dejar de excluir para todos los equipos	Nombre del parche sobre el que el usuario realizó la acción.
	Marcar como “Descargado manualmente”	Nombre del parche sobre el que el usuario realizó la acción.
	Marcar como “Requiere descarga manual”	Nombre del parche sobre el que el usuario realizó la acción.
Preferencia ante reclasificación de amenaza	Editar	
Preferencia para envío emails	Editar	
Preferencia para eliminación automática de equipos	Editar	
Preferencia para entornos VDI	Editar	
Preferencia para evaluación de riesgos	Editar	
Preferencia para MDR	Editar	
Preferencia de acceso de equipo de Cytomic S.L.	Editar	

Tipo de elemento	Acción	Elemento
Preferencia de acceso del distribuidor	Editar	
Preferencia para envío emails distribuidor	Editar	
Preferencia de verificación en dos pasos	Editar	
Programa bloqueado en clasificación	Eliminar del listado	Nombre del programa bloqueado sobre el que el usuario realizó la acción.
	Permitir	Nombre del programa bloqueado sobre el que el usuario realizó la acción.
	Dejar de permitir	Nombre del programa bloqueado sobre el que el usuario realizó la acción.
Rol	Crear	Nombre del rol sobre el que el usuario realizó la acción.
	Editar	Nombre del rol sobre el que el usuario realizó la acción.
	Eliminar	Nombre del rol sobre el que el usuario realizó la acción.
Tarea- Detección de IOCs	Crear	Nombre de la tarea sobre la que el usuario realizó la acción.
	Editar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la tarea sobre la que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Cancelar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Publicar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Crear y publicar	Nombre de la tarea sobre la que el usuario realizó la acción.
Tarea - Instalación de parches	Crear	Nombre de la tarea sobre la que el usuario realizó la acción.
	Editar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Cancelar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Publicar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Crear y publicar	Nombre de la tarea sobre la que el usuario realizó la acción.
Usuario	Crear	Nombre del usuario sobre la que el usuario realizó la acción.
	Editar	Nombre del usuario sobre la que el usuario realizó la acción.
	Eliminar	Nombre del usuario sobre la que el usuario realizó la acción.
	Bloquear	Nombre del usuario sobre la que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Desbloquear	Nombre del usuario sobre la que el usuario realizó la acción.
Tarea - Desinstalación de parches	Crear	Nombre de la tarea sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Cancelar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Publicar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Crear y publicar	Nombre de la tarea sobre la que el usuario realizó la acción.

Tabla 4.10: Tipos de elemento y acciones

Eventos de control remoto

Al hacer clic en la acción **Control remoto** se abrirá la ventana **Detalles de la sesión de control remoto** con la información siguiente:

Campo	Descripción
Fecha	Fecha y hora en la que se ha producido el evento de control remoto.
Categoría	• Archivos: operación relacionada con la herramienta de transferencia de archivos. • Procesos: operación relacionada con la herramienta de gestión de procesos. • Servicios: operación relacionada con la herramienta de gestión de servicios. • Terminal: operación relacionada con la herramienta de línea de comandos remota. • Conexión: operación de conexión de la consola de Advanced EDR con el equipo.

Campo	Descripción
Acción	Descripción de la categoría de la acción registrada. En el caso de la categoría Terminal , se registran los comandos que el administrador ejecutó remotamente en el equipo conectado.

Tabla 4.11: Campos del listado Detalles de la sesión de control remoto

Eventos del sistema

Lista los eventos que se producen en Advanced EDR y que no tienen una cuenta de usuario como origen, sino que son desencadenados por el propio sistema como respuesta las situaciones mostradas en [Tipos de elementos y acciones](#).

Campos mostrados en el listado de eventos del sistema

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se ha producido el acceso.	Fecha
Evento	Acción que ejecutó Advanced EDR.	Consulta Tipos de elementos y acciones .
Tipo	Tipo del objeto sobre el cual se ejecutó la acción.	Consulta Tipos de elementos y acciones .
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta Tipos de elementos y acciones .

Tabla 4.12: Campos del listado Eventos del sistema

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se ha producido el acceso.	Fecha
Evento	Acción que ejecutó Advanced EDR.	Consulta Tipos de elementos y acciones .
Tipo	Tipo del objeto sobre el cual se ejecutó la acción.	Consulta Tipos de elementos y acciones .

Campo	Descripción	Valores
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta Tipos de elementos y acciones .

Tabla 4.13: Campos del listado Eventos del sistema

Herramienta de búsqueda

Campo	Descripción	Valores
Desde	Establece el límite inferior del intervalo de búsqueda.	Fecha
Hasta	Establece el límite superior del intervalo de búsqueda.	Fecha

Tabla 4.14: Campos del listado Eventos del sistema

Tipos de elementos y acciones

Tipo de elemento	Acción	Elemento
Equipo no-persistente	Eliminar automáticamente	Nombre del equipo sobre el que se realizó la acción.
Equipo	Registrar en servidor por primera vez.	Nombre del equipo sobre el que se realizó la acción.
	Registrar en servidor tras eliminación de equipo.	Nombre del equipo sobre el que se realizó la acción.
	Registrar en servidor tras reinstalación de agente.	Nombre del equipo sobre el que se realizó la acción.
	Desinstalar el agente	Nombre del equipo sobre el que se realizó la acción.
	Desinstalar el agente y eliminar automáticamente	Nombre del equipo sobre el que se realizó la acción.
	Eliminar automáticamente	Nombre del equipo sobre el que se realizó la acción.

Tipo de elemento	Acción	Elemento
Envío programado	Desactivar automáticamente	Nombre del envío programado sobre el que se realizó la acción.

Tabla 4.15: Tipos de elementos y acciones

Instalación del software cliente

La instalación del software de seguridad comprende un conjunto de procesos que tienen como objetivo integrar en los dispositivos de los clientes los componentes software necesarios para protegerlos de las amenazas informáticas. En líneas generales, se compone de las etapas siguientes:

- **Despliegue:** crea el paquete de instalación con los componentes que forman la solución de seguridad y lo envía a cada uno de los dispositivos de los usuarios de la red.
- **Instalación:** descomprime el paquete de instalación e integra en el sistema operativo del dispositivo los ficheros que forman el software de seguridad.
- **Configuración:** el software de seguridad instalado en el dispositivo recibe las configuraciones necesarias para protegerlo desde el momento de su instalación, sin necesidad de acciones por parte del usuario.
- **Integración en la consola:** la consola de Advanced EDR muestra el dispositivo y el administrador puede ejecutar acciones sobre el mismo.

Contenido del capítulo

Instalación en sistemas Windows	100
Visión general del despliegue de la protección	100
Requisitos de instalación	103
Generar el paquete de instalación y despliegue manual	104
Instalación del paquete descargado	106
Integración de equipos según su dirección IP	107
Instalar con herramientas centralizadas	108
Instalar mediante generación de imágenes gold	110
Descubrimiento de equipos e instalación remota del software cliente	117
Visualizar equipos descubiertos	121

Detalle de los equipos descubiertos	125
Borrar y ocultar equipos	129
Instalación remota del software cliente	130
Instalación en sistemas Linux	133
Visión general del despliegue de la protección	133
Requisitos de instalación	134
Generar el paquete de instalación y despliegue manual	136
Instalación en plataformas Linux	137
Instalación en sistemas macOS	141
Visión general del despliegue de la protección	141
Requisitos de instalación	143
Despliegue manual del agente macOS	144
Instalación del paquete descargado	145
Comprobar el despliegue	145
Eliminación automática de equipos	148
Desinstalar el software	150
Desinstalación manual	150
Desinstalación desde la consola de administración	152
Reinstalación remota	153

Instalación en sistemas Windows

Visión general del despliegue de la protección

El proceso de instalación en equipos Windows comprende varios pasos, dependiendo del estado de la red en el momento del despliegue y del número de equipos a proteger:

- Localizar los equipos desprotegidos en la red.
- Satisfacer los requisitos mínimos.
- Desinstalar productos de la competencia y reinicio de equipos.
- Establecer la configuración por defecto de los equipos.
- Establecer el procedimiento de despliegue.
- Comprobar que el software de seguridad se instaló correctamente.

Localizar los equipos desprotegidos en la red

- Localiza los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con Advanced EDR. En redes de tamaño grande, es posible acelerar esta tarea mediante las funcionalidades de descubrimiento (consulta [Visualizar equipos descubiertos](#)).

- Comprueba que el número de licencias libres contratadas es suficiente (consulta [Licencias](#) en la página 157).



Advanced EDR permite la instalación del software sin tener contratadas licencias suficientes. Estos equipos serán visibles en la consola de administración y mostrarán el software instalado, hardware y otras características, pero no estarán protegidos frente al malware.

Satisfacer los requisitos mínimos

Para conocer los requisitos mínimos consulta [Requisitos de instalación](#).

Desinstalar productos de la competencia y reinicio de equipos

Los servicios de protección de Advanced EDR funcionan sin reiniciar el equipo en el caso de no tener un antivirus previamente instalado.



Algunas versiones anteriores de Citrix pueden requerir un reinicio del equipo o producir pequeños microcortes en las conexiones.

Por defecto, Advanced EDR convive con otras soluciones de seguridad instaladas en el equipo.

La desinstalación de otros productos aplica a versiones trial y comerciales. Para ello asigna una configuración de **Estaciones y servidores** con la opción **Desinstalar otros productos de seguridad** habilitada (consulta [Desinstalar otros productos de seguridad](#) en la página 294). Coincidiendo con la búsqueda de actualizaciones, Advanced EDR comprueba una vez al día la configuración establecida. Para obtener un listado de los productos de seguridad de terceros que Advanced EDR desinstala de forma automática, consulta el recurso web <https://www.pandasecurity.com/es/support/card?id=50021>.

Establecer la configuración por defecto de los equipos

Con el objeto de proteger a los equipos de la red desde el primer momento, Advanced EDR establece las configuraciones por defecto asignadas al grupo **Todos**. En el proceso de despliegue, es posible cambiar el grupo al que pertenecerá el equipo para asignarle otras configuraciones. Consulta [Gestión de configuraciones](#) en la página 251.

Una vez instalado el software en el equipo, Advanced EDR aplica las configuraciones establecidas en el grupo al que pertenece el equipo. Posteriormente, si la configuración de red del grupo seleccionado difiere de la indicada al generar el instalador, se genera una asignación manual. De esta forma, la configuración de red seleccionada en la instalación prevalece por encima de la asignada en el árbol de grupos. Consulta [Generar el paquete de instalación y despliegue manual](#).

Establecer el procedimiento de despliegue

Dependiendo del número total de equipos Windows a proteger, los puestos y servidores con un agente Cytomic ya instalado y la arquitectura de red de la empresa, es preferible utilizar un procedimiento u otro de los disponibles:

- Despliegue manual. Consulta [Generar el paquete de instalación y despliegue manual](#).
- Herramienta de despliegue centralizado. Consulta [Instalar mediante generación de imágenes gold](#).
- Despliegue remoto desde la consola de administración. Consulta [Descubrimiento de equipos e instalación remota del software cliente](#).
- Despliegue mediante generación de imágenes gold. Consulta [Instalar mediante generación de imágenes gold](#).

Comprobar que el software de protección se instaló correctamente

- Selecciona el menú superior **Equipos** y localiza el equipo instalado. Para obtener más información sobre buscar equipos consulta [Gestión de equipos y dispositivos](#) en la página 177.
- Haz clic en el equipo en el que has instalado el software de seguridad. Se abrirá la ventana de detalles del equipo.
- Haz clic en la pestaña **Detalles**. Se mostrará toda la información recogida del equipo y el estado de la instalación.
- En la sección **Seguridad** comprueba el estado de los distintos módulos:
 - **Instalando...**: el proceso de instalación no se ha completado o ha terminado en error. Espera unos minutos.
 - **Activado / desactivado**: transcurridos unos minutos, si la instalación terminó correctamente se mostrará el estado de los módulos de protección.

Detectar y solucionar fallos de instalación

Si transcurridos unos minutos la sección **Seguridad** desaparece del detalle del equipo, esto indica que el software de seguridad no se instaló correctamente. Comprueba los siguientes puntos:

- Si la instalación se realizó de forma manual comprueba que en el equipo del usuario no se muestran mensajes de error.
- Comprueba si el equipo se muestra en los listados. Consulta [Comprobar el despliegue](#).
- Comprueba en el equipo del usuario el visor de sucesos. Consulta [Comprobar el despliegue](#).
- Consulta que el equipo del usuario cumple con los requisitos indicados en [Requisitos de instalación](#) y actualiza la versión del producto o la versión del sistema operativo. Consulta [Actualización del producto](#) en la página 171.

Requisitos de instalación

Comprueba que el equipo donde vas a instalar el software de seguridad cumple con la lista de requisitos mostrada a continuación, y que los recursos de red necesarios se encuentran disponibles.



A partir de la fecha 30/09/2024 no será posible añadir a la consola de administración nuevos equipos que utilicen los siguientes sistemas operativos: Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008 (no afecta a Windows Server 2008 R2). Los equipos instalados en una fecha anterior seguirán protegidos. Consulta <https://www.watchguard.com/wgrd-trust-center/end-of-life-policy>.

Versiones del sistema operativo compatibles

Advanced EDR es compatible con microprocesadores x86 de 32 y 64 bits, así como ARM. Para una lista detallada consulta **Sistemas operativos soportados** en la página **852**.



Advanced EDR es compatible con Windows XP Embedded y superiores. Los sistemas embedded pueden instalarse de forma personalizada, por lo que el funcionamiento del software de seguridad instalado y de algunos de sus módulos puede variar.

Hardware

Consulta **Requisitos hardware** en la página **853**.

Certificados raíz

Advanced EDR requiere que los certificados raíz instalados en el equipo estén actualizados para utilizar el módulo Cytomic Patch y las comunicaciones en tiempo real con la consola de administración. Consulta **Actualizar los certificados raíz** en la página **854**.

Compatibilidad con SHA-256

Es necesario que el equipo del usuario o servidor sea compatible con las firmas de drivers SHA-256. Para obtener más información sobre los sistemas operativos afectados y cómo actualizarlos, consulta **Compatibilidad con firma de drivers SHA-256** en la página **855**. Para localizar los equipos que no admiten el firmado de drivers SHA-256, consulta **Equipos no compatibles con firma de drivers SHA-256** en la página **187**.

Requisitos de red

En su funcionamiento normal, Advanced EDR accede a varios recursos alojados en Internet. De forma general, se requiere acceso a los puertos 80 y 443.

El agente Advanced EDR requiere acceso al puerto 33000 para la comunicación entre equipos protegidos de la red (consulta **Configuración de Control de Acceso a Endpoints** en la página **458** y con dispositivos Firebox o Access Point (consulta **Control de acceso a redes** en la página **282**

Para un listado completo de las URLs que se acceden desde los equipos con el software Advanced EDR instalado, consulta [Puertos locales y acceso a URLs](#) en la página **862**.

Sincronización horaria de los equipos (NTP)

Aunque no es un requisito indispensable, es muy recomendable que el reloj de los equipos protegidos con Advanced EDR esté sincronizado. La mayoría de las veces, la sincronización se establece mediante el uso de un servidor NTP. Consulta [Sincronización horaria de los equipos \(NTP\)](#) en la página **854**.

Internet Explorer 7

Para que la protección avanzada funcione correctamente en sistemas operativos Windows XP y Windows 2003 es necesario instalar Internet Explorer 7 previamente o una versión superior.

En el caso de Windows XP, no es posible instalar o actualizar la protección de manera directa, por lo que es necesario utilizar un equipo caché para ello. Para más información, consulta [Configuración de las descargas mediante equipos caché](#) en la página **279**

La instalación o actualización de la protección en Windows 2003 solo es posible siempre y cuando el sistema operativo esté debidamente actualizado y con todos los parches necesarios instalados. En caso contrario, será necesario utilizar un equipo caché. Para más información consulta [Cytomic Patch \(Actualización de programas vulnerables\)](#) en la página **375**

Generar el paquete de instalación y despliegue manual

- En el menú superior **Equipos** de la consola de administración, haz clic en el botón **Añadir equipos** situado en la parte superior derecha de la pantalla. Se abrirá una ventana con las plataformas compatibles con Advanced EDR.
- Haz clic en el icono Windows, tanto para equipos con procesador x86 como ARM. Se abrirá la ventana **Windows**.

Figura 5.1: Configuración del paquete de descarga

- Selecciona el grupo donde se integrará el equipo en el árbol de carpetas (para más información sobre los diferentes tipos de grupos y sus particularidades, consulta [Tipos de grupos](#) en la página 188:
 - Para integrar el equipo en un grupo nativo, haz clic en **Añadir los equipos al siguiente grupo (1)** y selecciona el destino en el árbol de carpetas mostrado.
 - Para integrar el equipo en un grupo Directorio Activo, haz clic en **Añadir los equipos en su ruta de Directorio Activo (2)**.



*Las políticas de seguridad asignadas a un equipo dependen del grupo al que pertenece. Si has elegido **Añadir los equipos en su ruta de Directorio Activo** y el administrador del directorio activo de la empresa mueve el equipo de una unidad organizativa a otra, este cambio se replicará en la consola de Advanced EDR como un cambio de grupo. Por esta razón, las políticas de seguridad asignadas a ese equipo también podrían cambiar sin ser advertido por el administrador de la consola Web.*

- Para integrar el equipo en un grupo u otro en función de su dirección IP, haz clic en la opción **Seleccionar el grupo en función de la IP del equipo (3)** y elige el grupo a partir del cual se buscará un destino que coincida con la IP del equipo. Consulta [Integración de equipos según su dirección IP](#).

- Para establecer una configuración de red alternativa al grupo donde se integrará el equipo, haz clic en **Selecciona la configuración de red para los equipos (4)** y elige una configuración de red en el desplegable: inicialmente, todas las configuraciones que se aplican al equipo en el momento de la integración son las que están asignadas al grupo de la consola al que pertenecerá. Sin embargo, para prevenir fallos de conectividad y evitar que el equipo quede inaccesible desde la consola de administración por una configuración de red no apropiada, es posible establecer una configuración de red alternativa. Para más información sobre crear configuraciones de red consulta [Configuración remota del agente](#) en la página 271.
- **Grupos nativos y grupos IP:** el desplegable **Selecciona la configuración de red para los equipos (4)** muestra la configuración de red asignada al grupo elegido en **Añadir los equipos al siguiente grupo (1)**.
- **Grupos Active Directory:** el desplegable **Selecciona la configuración de red para los equipos (4)** muestra la configuración de red asignada al grupo de Active Directory seleccionado en el árbol de grupos. Si no estaba seleccionado ningún grupo de directorio activo antes de hacer clic en el botón **Añadir equipo**, será necesario establecer una configuración de red.
- Para evitar que el instalador pueda utilizarse más allá de una fecha determinada, haz clic en la caja de texto **Indica si quieres que el instalador no se pueda utilizar a partir de una fecha** y selecciona la fecha en el calendario.
- Para enviar el instalador al usuario por correo electrónico:
 - Haz clic en el botón **Enviar URL por email (6)**. Se mostrará la aplicación de correo instalada por defecto en el equipo del administrador con un mensaje ya generado que contiene la URL de descarga.
 - Añade al mensaje los destinatarios de correo y haz clic en el botón **Enviar**.
 - El usuario que reciba el correo deberá hacer clic en la URL desde el dispositivo para iniciar la descarga del instalador.
- Para descargar el paquete de instalación y compartirlo con los usuarios de la red, haz clic en el botón **Descargar instalador (7)**.

Instalación del paquete descargado

- Haz doble clic en el paquete y sigue el asistente de instalación. Durante todo el proceso se muestra una ventana que indica el progreso de la tarea.
- Si el número de licencias libres no es suficiente para asignar una al equipo en proceso de instalación, se mostrará un aviso en pantalla. Independientemente de este hecho, el equipo se integrará en la consola de administración pero no estará protegido hasta que no haya licencias disponibles.

Una vez instalado el agente, éste realiza una serie de comprobaciones automáticas:

- **Integración del agente en Cytomic:** el agente envía la información del equipo a la nube de Cytomic para integrarlo en la plataforma.
- **Descarga del instalador del módulo de la protección:** el agente descarga e instala el módulo de protección.
- **Descarga del fichero de firmas:** el agente descarga el fichero de firmas con el malware conocido.
- **Descarga de configuraciones:** se descargan y aplican las configuraciones predeterminadas y creadas por el administrador.
- **Comprobar la conectividad con la nube de Cytomic:** en caso de error se reporta su tipo a los siguientes lugares:
 - **En la consola de instalación del agente:** se muestra un mensaje de error y las URLs que fallan. Haz clic en el botón **Reintentar** para realizar una nueva verificación.
 - **En el visor de sucesos de Windows (Eventlog):** se muestra un mensaje de error y las URLs que fallan.
 - **En la consola web:** se muestra un mensaje de error y las URLs que fallan.

Integración de equipos según su dirección IP

Advanced EDR permite asignar rangos de direcciones IPs e IPs individuales a grupos. Los equipos con una IP que pertenezca al rango del grupo, se moverán automáticamente a éste en el momento de su instalación. Consulta [Crear y organizar grupos](#) en la página 190.

El objetivo de esta funcionalidad consiste en ahorrar tiempo al administrador organizando de forma automática los equipos recién integrados en el producto. Cuando un equipo nuevo se integra en Advanced EDR se siguen los pasos mostrados a continuación:

- Si la opción elegida en la integración es **Seleccionar el grupo en función de la IP del equipo**, Advanced EDR ejecutará una búsqueda en profundidad para recuperar las IPs asociadas al grupo indicado en el campo **Seleccionar a partir de qué grupo se añadirán los equipos** y las de todos sus hijos.
- Si se encuentra una única IP coincidente con el equipo, éste se moverá al grupo pertinente.
- Si hay varios grupos de IPs que coinciden con la IP del equipo, se tomará siempre el grupo de mayor profundidad. Si existen varios grupos que coinciden con la IP con un mismo nivel de profundidad se elegirá el último de ellos.
- Si no existe ninguna coincidencia, el equipo se moverá al grupo indicado en el campo **Seleccionar a partir de qué grupo se añadirán los equipos**, y si este grupo no existe en el momento de la integración, el equipo se moverá al grupo **Todos**.

Una vez movido el equipo al grupo correspondiente, el equipo no se volverá a mover automáticamente al cambiar su IP, ni tampoco se reorganizarán los equipos ya integrados al cambiar las IPs asignadas a los grupos de IPs.

Instalar con herramientas centralizadas

En redes de tamaño medio o grande es conveniente instalar el software cliente para equipos Windows de forma centralizada con la ayuda de herramientas de terceros.

Línea de comandos del paquete de instalación

Para automatizar la instalación e integración del software de seguridad en la consola de administración se implementan los parámetros siguientes de línea de comandos:

- **GROUPPATH="grupo1\grupo2"**: ruta dentro del árbol de grupos y sin indicar el nodo raíz **Todos** donde se integrará el equipo. Si el grupo no existe, el equipo se integra en el nodo raíz **Todos**.
- **PRX_SERVER**: dirección IP o nombre del servidor proxy corporativo.
- **PRX_PORT**: puerto del servidor proxy corporativo.
- **PRX_USER**: usuario del servidor proxy corporativo.
- **PRX_PASS**: contraseña del servidor proxy corporativo.

A continuación, se muestra un ejemplo de instalación con parámetros:

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

Para realizar la instalación de modo silencioso, añade el parametro /qn:

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

Despliegue desde Panda Systems Management

- Panda Endpoint Protection Installer on Aether for Linux: 3 Kbytes

Despliegue con Microsoft Active Directory

Limitaciones de Microsoft Active Directory al desplegar el software de seguridad

- El método de despliegue con Microsoft Active Directory instala el software de seguridad en un equipo por primera vez. No se soporta la actualización del software de seguridad ya instalado.
- El equipo donde se define la GPO (Group Policy Object) no puede tener instalado el software de seguridad. En caso contrario, el proceso mostrará el error "The process of adding failed. The deployment information could not be retrieved from the package. Make sure that the package is correct".

Pasos para preparar una GPO (Group Policy Object) de instalación

1. Descarga el paquete Advanced EDR y comparte el instalador en la red.
 - Coloca el instalador Advanced EDR en una carpeta compartida que sea accesible por todos los equipos que vayan a recibir el software.
2. Crea una nueva UO (Unidad Organizativa) de nombre “Despliegue Cytomic”.
 - Abre la mmc y agrega el snap-in Administrador de políticas de grupo.
 - Con el botón de la derecha en el nodo del dominio, haz clic en **Nuevo y Unidad Organizativa** para crear una unidad organizativa de nombre “Despliegue Cytomic”.
 - Haz clic con el botón de la derecha del ratón en la unidad organizativa recién creada y selecciona en el menú **Bloquear herencia**.

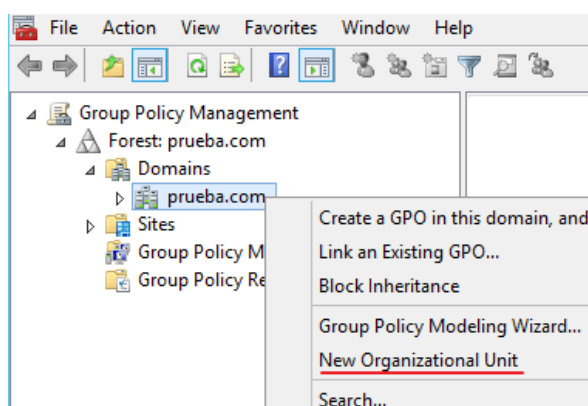


Figura 5.2: Nueva unidad organizativa

3. Crea una nueva GPO con el paquete de instalación

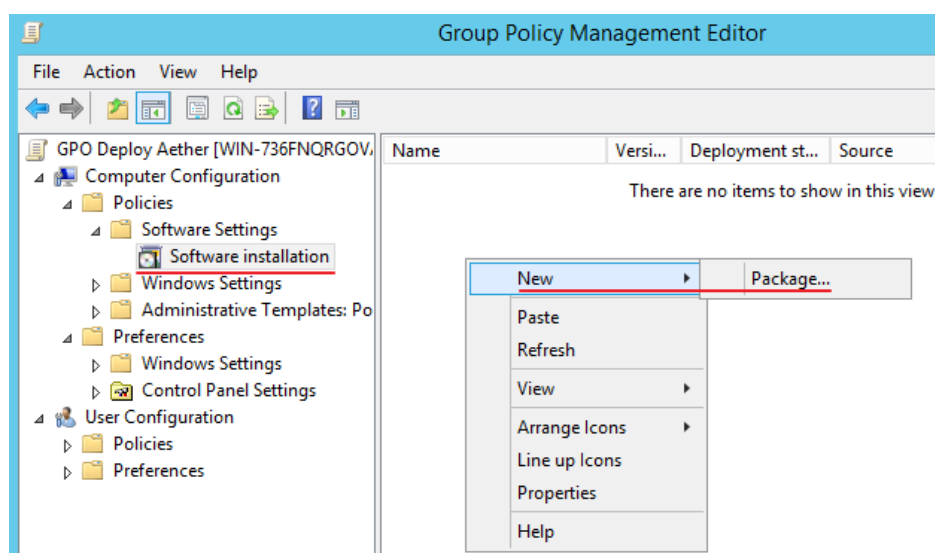


Figura 5.3: Nuevo paquete de instalación

- Haz clic con el botón de la derecha del ratón en la Unidad Organizativa recién creada y selecciona **Crear una GPO** de nombre “GPO Despliegue Cytomic”.
 - Edita la GPO recién creada y añade el paquete de instalación que contiene el software Advanced EDR en la rama **Configuración del equipo, Políticas, Configuración de software, Instalación del software**.
 - Con el botón de la derecha en el panel de la derecha, haz clic en **Nuevo, Paquete**.
 - Añade el fichero de instalación .msi de Advanced EDR.
4. Edita las propiedades del paquete

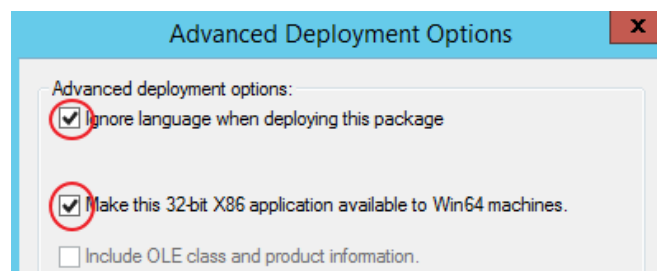


Figura 5.4: Configuración del despliegue

- Haz clic con el botón derecho sobre el paquete agregado y selecciona **Propiedades**, pestaña **Despliegue** y **Avanzado**. Selecciona las casillas que evitan las comprobaciones de idioma y de plataforma entre el sistema operativo de destino y el definido en el instalador.
- Añade a la OU “Despliegue Cytomic” todos los equipos de la red que recibirán el agente.

Instalar mediante generación de imágenes gold



Sigue los pasos exactos que se muestran en este apartado para generar y desplegar imágenes Windows con Advanced EDR instalado. De no seguir el procedimiento tal y como se indica, las capacidades de gestión y de protección de tu producto de seguridad se verán reducidas, y se dejarán de monitorizar las acciones ejecutadas por los procesos en los equipos clonados.

En redes grandes formadas por muchos equipos homogéneos, el procedimiento de instalación del sistema operativo y del software que lo acompaña puede automatizarse generando una imagen gold (también conocida como imagen “master”, “base”, “maqueta” o imagen “plataforma”). Posteriormente, esta imagen se distribuye a todos los equipos de la red, lo que evita gran parte del proceso manual de instalación desde cero.

Para generar una imagen gold, es necesario instalar en un equipo de la red el sistema operativo ya actualizado junto a todo el software que el usuario vaya a necesitar, incluyendo las herramientas de seguridad. Una vez listo el equipo, es necesario utilizar un software de virtualización para “sellar” o “cerrar”

la instalación y distribuirla en los equipos de la red. Para obtener información específica de tu solución de virtualización, consulta la documentación de tu proveedor.

Plataformas de virtualización compatibles

- VMware Workstation
- VMware Server
- VMware ESX
- VMware ESXi
- Citrix XenDesktop
- XenApp
- XenServer
- MS Virtual Desktop
- MS Virtual Servers

Conceptos básicos y herramientas necesarias

Identificador de los equipos VDI

Advanced EDR genera un identificador único en el proceso de instalación, que se utiliza internamente para referenciar a cada equipo en la consola de administración.

Si Advanced EDR se instala una única vez en la imagen gold que posteriormente se copiará en los equipos de la red pero no se instala de forma individual en cada uno de los equipos, todos los equipos clonados heredarán el mismo identificador.

Compartir un mismo identificador en varios equipos tiene las siguientes consecuencias negativas:

- Se reducen las capacidades de gestión: la consola de administración solo muestra un equipo, generalmente el primero que se integró en ella. El resto de equipos clonados no serán accesibles desde la consola de Advanced EDR.
- Se reducen las capacidades de protección del software de seguridad.
- Se dejan de monitorizar las acciones ejecutadas por los procesos.

Para evitar compartir un mismo identificador en varios equipos, es necesario seguir un protocolo de preparación de la imagen muy estricto que tiene como fin generar una imagen gold sin identificador. Este protocolo incluye:

- Borrar el identificador de la imagen gold
- Desactivar el servicio de protección

Borrar el identificador de la imagen gold

Descarga la herramienta gratuita `Endpoint Agent Tool` en la página web de soporte de Cytomicen la siguiente URL (contraseña `panda`):

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

Desactivar el servicio de protección

Muchas soluciones de virtualización inician de forma transparente la imagen gold recién creada como parte del proceso de preparación y despliegue. Esto provoca que Advanced EDR se inicie, y al detectar que su identificador fue borrado, genera un identificador nuevo, e invalida a imagen generada. Para evitar este escenario, es necesario desactivar el servicio de protección antes de cerrar la imagen gold y programar su lanzamiento mediante métodos alternativos en el inicio de los equipos clonados.

Hay varias formas para ejecutar este paso; la más popular y tratada en este apartado es mediante una GPO si el equipo pertenece a un dominio Windows. Si éste no es el caso, existen otras soluciones alternativas:

- Las soluciones de virtualización pueden incorporar este tipo de herramientas, como por ejemplo Horizon en VMWare.
- RMMs como Panda Systems Management.
- Herramientas como PDQ Deploy, PSEXec de Sysinternals, PowerShell de Microsoft, o scripts que utilicen WMI, entre muchos otros.

Activar y desactivar la actualización de Advanced EDR

En entornos no persistentes donde el sistema de almacenamiento de los equipos clonados se borra cada cierto tiempo, es importante evitar la actualización del software de protección. Esta tarea se delega en el mantenimiento de la imagen gold, para evitar el consumo de red generado por los equipos clonados y un excesivo uso de la CPU en el sistema anfitrión.

Para seguir los procedimientos que permiten generar con éxito una imagen gold, es necesario asignar configuraciones que activan y/o desactivan la actualización de Advanced EDR en el equipo a clonar:

- Para activar o desactivar la actualización del agente, consulta [Actualización del agente de comunicaciones](#) en la página 174.
- Para activar o desactivar la actualización de la protección, consulta [Actualización del motor de protección](#) en la página 172.
- Para asignar configuraciones a equipos, consulta [Gestión de configuraciones](#) en la página 251.
- Para obtener más información acerca de los grupos en Advanced EDR, consulta [Árbol de grupos](#) en la página 188.

Ya que en algunos escenarios es necesario alternar entre un juego de configuraciones y otro, se recomienda crear dos grupos en la consola de administración: uno con las configuraciones asignadas que activan las actualizaciones de Advanced EDR y otro con las configuraciones que las desactivan. De esta forma, para activar o desactivar las actualizaciones solo será necesario mover el equipo que contiene la imagen gold de un grupo a otro en la consola.

Adicionalmente, siempre que se hable de un cambio de configuración en la consola de Advanced EDR, es recomendable seguir el procedimiento mostrado a continuación para asegurarse de que el cambio de configuración se recibe en el equipo utilizado para generar la imagen gold:

- Mover el equipo al grupo adecuado para que herede las configuraciones.
- En el área de notificaciones de la barra de tarea de Windows, haz clic con el botón derecho del ratón sobre el icono de Advanced EDR. Se mostrará un menú desplegable.
- Selecciona **Sincronizar**. Esto forzará la descarga en el equipo de las configuraciones de seguridad pendientes de recibir desde el servidor.

Crear y desplegar una imagen gold en entornos VDI persistentes

Pasos a ejecutar en el equipo que genera la imagen gold

- Instala el sistema operativo actualizado y los programas que necesitarán los usuarios.
- Comprueba que hay conexión a Internet y que la MAC de la tarjeta de red es estática.
- Instala Advanced EDR según los pasos mostrados en **Generar el paquete de instalación y despliegue manual en un grupo con las actualizaciones activadas**.
- Ejecuta la herramienta `Endpoint Agent Tool`, selecciona las opciones **Detections**, **Counters** y **Check commands**, y haz clic en el botón **Send**.
- Comprueba que la casilla de selección **Is a gold image** NO está marcada.
- Si el equipo está protegido por AntiTamper, escribe la contraseña en **AntiTamper password**; si no, deja este campo en blanco.
- Haz clic en el botón **Prepare image**.
- **Deshabilita el servicio Panda Endpoint Agent**.
- Apaga el equipo y genera la imagen con el software de administración de entornos virtuales que utilices.

Pasos a ejecutar para activar el servicio de protección

Este procedimiento activa el servicio Panda Endpoint Agent en los equipos clonados mediante una GPO:

- Dentro de la configuración de la GPO, navega la ruta **Computer Configuration, Policies, Windows Settings, Security Settings, System Services, Panda Endpoint Agent**.
- El servicio aparecerá como **Deshabilitado**. Cámbialo a **Automático**.



Para conocer más detalles sobre las GPOs, consulta la URL <https://www.microsoft.com/es-ES/download/details.aspx?id=21895>.

Crear, desplegar y mantener una imagen gold para entornos VDI no persistentes

Pasos a ejecutar en el equipo que genera la imagen gold

- Instala el sistema operativo actualizado y los programas que necesitarán los usuarios.
- Comprueba que el equipo tiene conexión a Internet .
- Instala Advanced EDR según los pasos mostrados en **Generar el paquete de instalación y despliegue manual en un grupo con las actualizaciones desactivadas**.
- **Mueve el equipo a un grupo con las actualizaciones activadas.**
- Si la persistencia de los equipos clonados será inferior a una semana, es recomendable, aunque no estrictamente necesario, precargar las cachés de Advanced EDR. Sigue uno de estos dos métodos:
 - En la herramienta `Endpoint Agent Tool` haz clic en el botón **Start cache scan** y espera a que el proceso termine.
 - o
 - Haz clic con el botón derecho del ratón en el icono de Advanced EDR en la barra de notificaciones de Windows.
 - Haz clic en **Protección avanzada**.
 - Haz clic en el botón **Analizar ahora** y espera a que el proceso termine.
- Ejecuta la herramienta `Endpoint Agent Tool`, selecciona las opciones **Detections**, **Counters** y **Check commands**, y haz clic en **Send**.
- **Comprueba que la casilla de selección *Is a gold image* **Sí** está marcada.**
- Si el equipo está protegido por AntiTamper, escribe la contraseña en **AntiTamper password**; si no, deja este campo en blanco.
- Haz clic en el botón **Prepare image**.
- **Deshabilita el servicio Panda Endpoint Agent.**
- Apaga el equipo para generar la imagen con el software de administración de entornos virtuales que utilices.

Pasos a ejecutar en la consola de administración de Advanced EDR

- Haz clic en el menú superior **Configuración** y en el panel lateral **Entornos VDI** .
- Define el máximo número de equipos VDI no persistentes que estarán activos simultáneamente.

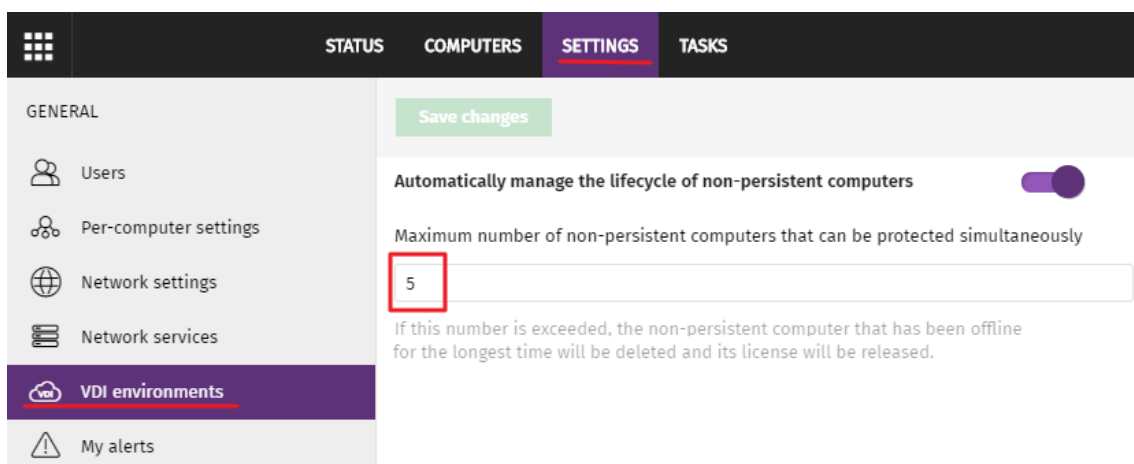


Figura 5.5: Configuración del numero de licencias asignadas a equipos VDI no persistentes

Pasos para activar el servicio de protección

Este procedimiento activa el servicio Panda Endpoint Agent en los equipos clonados mediante una GPO:

- Dentro de la configuración de la GPO, navega la ruta **Computer Configuration, Policies, Windows Settings, Security Settings, System Services, Panda Endpoint Agent**.
- El servicio aparecerá como **Deshabilitado**. Cámbialo a **Automático**.



Para conocer más detalles sobre las GPO, consulta la URL <https://www.microsoft.com/es-ES/download/details.aspx?id=21895>

Mantener la imagen gold en entornos VDI no persistentes

Dado que los equipos VDI tienen asignada una configuración de actualización deshabilitada, para que reciban la última versión de la protección y del fichero de firmas, es necesario actualizar la imagen gold de forma manual por lo menos una vez al mes. Para ello, accede al equipo que tiene instalada la imagen gold y sigue los pasos mostrados a continuación:

- Comprueba que el equipo tiene conexión a Internet.
- **Mueve el equipo a un grupo con las actualizaciones activadas.**
- Las actualizaciones se hacen en segundo plano, por lo que es necesario esperar varios minutos para completar el proceso. Si hay una versión nueva de la protección, se solicitará el reinicio del equipo. En este caso, tras el reinicio se recomienda volver a forzar una sincronización para asegurar que Advanced EDR está totalmente actualizado y con la configuración correcta.
- Precarga las cachés de Advanced EDR. Sigue uno de estos dos métodos:
 - En la herramienta `Endpoint Agent Tool` haz clic en el botón **Start cache scan** y espera a que el proceso termine.

o

- Haz clic con el botón derecho del ratón en el icono de Advanced EDR en la barra de notificaciones de Windows.
- Haz clic en **Protección avanzada**.
- Haz clic en el botón **Analizar ahora** y espera a que el proceso termine.
- En la herramienta `Endpoint Agent Tool` selecciona las opciones **Detections**, **Counters** y **Check commands**, y haz clic en **Send**.
- Comprueba que la casilla de selección **Is a gold image SI** está marcada.
- Si el equipo está protegido por AntiTamper, escribe la contraseña en **AntiTamper password**; de lo contrario, deja este campo en blanco.
- Haz clic en el botón **Prepare image**.
- Apaga el equipo para generar la imagen con el software de administración de entornos virtuales que utilices.
- Sustituye en el entorno VDI la imagen anterior por la nueva obtenida.
- Repite este proceso de mantenimiento una vez al mes por lo menos.

Comprobar que el proceso de clonación es correcto

No existe una fórmula única para comprobar que los equipos clonados son correctos en todos los escenarios posibles, pero a continuación se ofrece una lista de comprobación mínima.

Mostrar los equipos VDI persistentes y no persistentes

Un síntoma de no haber seguido correctamente el procedimiento de generación de imágenes gold, es la aparición de un número de equipos VDI en la consola de administración de Advanced EDR menor que el realmente instalado en el parque informático. En este caso, las capacidades de gestión y de protección de tu producto de seguridad se verán severamente reducidas.

Para obtener un listado de los equipos VDI no persistentes, sigue los pasos mostrados a continuación:

- En el menú superior **Configuración**, panel lateral **Entornos DVI** haz clic en el enlace **Mostrar los equipos no persistentes**.
- Se mostrará el listado de equipos con el filtro **Equipos no persistentes** configurado.

Para obtener un listado de los equipos VDI persistentes, sigue los pasos mostrados a continuación:

- En el menú superior **Equipos**, haz clic en el icono de carpeta  en el panel lateral. Se mostrará el árbol de grupos.
- Haz clic en el nodo raíz **Todos**. En el panel derecho se mostrarán todos los equipos integrados en la consola de Advanced EDR.
- Comprueba que todos los equipos persistentes están incluidos en el listado.

Comprobar el estado de las actualizaciones de Advanced EDR en los equipos clonados

- En el menú superior **Equipos**, haz clic en el icono de carpeta  en el panel lateral. Se mostrará el árbol de grupos.
- Localiza en el panel de la derecha los equipos persistentes y no persistentes.
- Por cada equipo clonado haz clic en su nombre. Se abrirá una ventana con el detalle.
- Haz clic en la pestaña **Configuración**. Se mostrarán las configuraciones aplicadas en el equipo.
- Comprueba que las configuraciones **Ajustes por equipo** y **Seguridad para estaciones y servidores** tienen los valores correctos:
 - Para equipos persistentes las actualizaciones deben estar activadas.
 - Para equipos no persistentes las actualizaciones deben estar desactivadas.

Descubrimiento de equipos e instalación remota del software cliente

Los productos basados en Cytomic Platform incorporan las herramientas necesarias para localizar los puestos de usuario y servidores Windows sin proteger, e iniciar una instalación remota y desatendida del software de seguridad desde la consola de administración.

Para instalar la el software de protección de forma remota en un equipo mediante la consola de administración, es necesario seguir los pasos mostrados a continuación:

- Asignar el rol de descubridor a uno o más equipos de la red. Consulta [Asignar el rol de descubridor a un equipo](#).
- Comprobar que los equipos de la red cumplen con los requisitos mínimos. Consulta [Requisitos de red y sistema operativo](#).
- Iniciar la instalación remota del software de seguridad. Consulta [Instalación remota del software cliente](#).

El descubrimiento de equipos se efectúa a través de un equipo con el rol de descubridor asignado. Todos los equipos que cumplan los requisitos se mostrarán en el listado **Equipos no administrados descubiertos**, independientemente de si el sistema operativo o el tipo de dispositivo admite la instalación de Advanced EDR.



El primer equipo Windows que se integre en Advanced EDR, tendrá asignado el rol descubridor de forma automática.

El equipo descubridor puede utilizar al mismo tiempo uno o los dos sistemas de descubrimiento existentes: descubrimiento mediante escaneo de red o descubrimiento mediante directorio activo. Consulta [Utilizar la](#)

red para descubrir equipos Utilizar el Directorio activo para descubrir equipos y Asignar el rol de descubridor a un equipo.

Asignar el rol de descubridor a un equipo

- Comprueba que el equipo descubridor tiene instalado Advanced EDR.
- Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red** y pestaña **Descubrimiento**.
- Haz clic en el botón **Añadir equipo descubridor** y selecciona en el listado los equipos que lanzarán procesos de descubrimiento en la red.

Una vez asignado el rol de descubridor a un equipo, éste se mostrará en la lista de equipos descubridores (menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**). Para cada equipo descubridor se muestra la siguiente información:

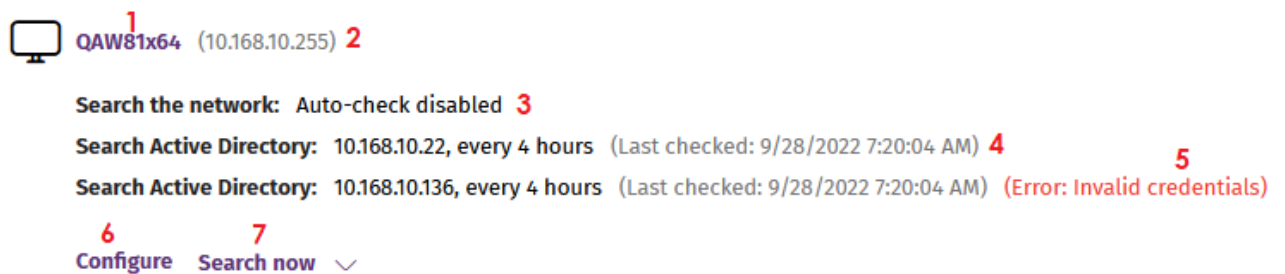


Figura 5.6: Información del equipo descubridor

Campo	Descripción
Nombre del equipo (1)	Nombre del equipo descubridor.
Dirección IP (2)	Dirección IP del equipo descubridor.
Configuración de las tareas de descubrimiento (3)	Descripción de la configuración de las tareas automáticas definidas en el equipo descubridor.
Última comprobación (4)	Fecha y hora de la última vez que se lanzó la tarea de descubrimiento.
Códigos de error (5)	• “El equipo está apagado o sin conexión”: el equipo descubridor no es accesible por el servidor de Advanced EDR. • Error: credenciales incorrectas.

Campo	Descripción
	- Error: servidor de directorio activo no encontrado. - Error (<código de error>): si se trata de un error desconocido.
Configurar (6)	Establece el alcance y tipo de descubrimiento (automático o manual). Si es automático, la tarea de descubrimiento se ejecutará una vez al día. Consulta Asignar el rol de descubridor a un equipo .
Buscar ahora (7)	Lanza la tarea de búsqueda de forma manual. Consulta Lanzar las tareas de descubrimiento manualmente .

Tabla 5.1: Campos del detalle de un equipo con el rol descubridor asignado

Utilizar la red para descubrir equipos

- En el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**, selecciona el equipo descubridor que quieres configurar y haz clic en el enlace **Configurar**. Se abrirá la ventana **Configurar descubrimiento en <nombre de equipo>**
- Para activar el descubrimiento, desplaza el control deslizante en la sección **Descubrir equipos de la red**.
- En la sección **Limitar alcance del descubrimiento** selecciona un criterio:
 - Buscar en toda la red:** el equipo descubridor utiliza la máscara configurada en la interface para efectuar un barrido completo de la subred a la que pertenece. La búsqueda se realiza solo sobre rangos de IPs privadas.
 - Buscar solo en los siguientes rangos de direcciones IPs:** define varios rangos de búsqueda en la red separados por comas. Separa el inicio y el final del rango mediante el carácter guion '-'. Solo se admite especificar rangos de IPs privadas.
 - Buscar sólo equipos de los siguientes dominios:** la búsqueda queda limitada a los dominios Windows indicados separados por comas.



Todas las configuraciones de alcance de descubrimiento están limitadas al segmento de red donde está conectado el equipo descubridor. Para buscar dispositivos en todos los segmentos de red, asigna el rol de descubridor a por lo menos un equipo en cada segmento de red.

Utilizar el Directorio activo para descubrir equipos

El equipo descubridor se conecta al Directorio Activo de la empresa para buscar los equipos de la red. Cada equipo descubridor puede conectarse a más de un servidor para lanzar las consultas en los directorios, siendo el máximo 3 servidores.

- En el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**, selecciona el equipo descubridor cuyo alcance quieres configurar y haz clic en el enlace **Configurar**. Se abrirá la ventana **Configurar descubrimiento**.
- Para activar el descubrimiento, desplaza el control deslizante en la sección **Descubrir equipos en el directorio activo**.
- Haz clic en el enlace **Añadir servidor de directorio activo**. Se abrirá la ventana **Añadir servidor de Directorio Activo**.
- En la ventana que se muestra, escribe el nombre o dirección IP del servidor (campo obligatorio) en el que quieres hacer la búsqueda, y las credenciales si fueran necesarias (pueden ser datos opcionales).
- Para finalizar la configuración, haz clic en el botón **Guardar**. El equipo descubridor preguntará al directorio activo por los equipos de la red cada 4 horas.

Programar las tareas de descubrimiento

Las tareas de descubrimiento de equipos se pueden lanzar de forma programada cada cierto tiempo por los equipos descubridores.

Descubrimiento de red

- En el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**, haz clic en el enlace **Configurar** del equipo descubridor a configurar.
- En el desplegable **Ejecutar automáticamente** elige **Todos los días**.
- Elige la hora a la que se ejecutará la tarea.
- Si quieres que la tarea se rija por la hora local del equipo en lugar de por la del servidor de Advanced EDR, selecciona la casilla **Hora local del dispositivo**.
- Haz clic en **Guardar**. El equipo descubridor mostrará en su descripción la programación configurada.

Descubrimiento mediante Directorio activo

- En el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**, selecciona el equipo que quieres configurar y haz clic en el enlace **Configurar**. Se abrirá la ventana **Configurar descubrimiento**.
- Haz clic en el directorio activo a configurar. Se abrirá la ventana **Editar servidor de Directorio Activo**.
- En el desplegable **Periodicidad**, selecciona cada cuántas horas se lanzarán las búsquedas.

Lanzar las tareas de descubrimiento manualmente

Para lanzar una tarea de descubrimiento manual, es necesario que el equipo descubridor esté en funcionamiento y tenga conexión con el servidor de Advanced EDR.

- Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**.
- Haz clic en el enlace **Comprobar ahora** del equipo descubridor de tu elección. Si el equipo descubridor solo tiene un método de descubrimiento configurado, se mostrará el mensaje **Búsqueda de equipos no administrados en curso** y se lanzará la tarea de descubrimiento en segundo plano.
- Si el equipo descubridor tiene configurados varios métodos de descubrimiento, se mostrará un menú de contexto al hacer clic en el enlace **Comprobar ahora**:
 - **Buscar en todos los sitios**: el equipo descubridor realizará un escaneo de la red y de todos los servidores con directorio activo que se hayan configurado.
 - **Buscar en la red**: el equipo descubridor realizará un escaneo de red.
 - **Buscar en <nombre_servidor>**: el equipo descubridor buscará solo en el servidor seleccionado.

Visualizar equipos descubiertos

Los equipos descubiertos mediante el escaneo de red o mediante directorio activo se muestran en el listado **Equipos no administrados descubiertos**.



Para mas información sobre los métodos de descubrimiento de equipos, consulta **Utilizar la red para descubrir equipos** y **Utilizar el Directorio activo para descubrir equipos**

Existen dos formas de acceder al listado de **Equipos no administrados descubiertos**:

- **Widget Estado de protección**: desde el menú superior **Estado** accede al panel de control de Advanced EDR donde se encuentra el widget **Estado de la protección**. En su parte inferior se mostrará el enlace **Se han descubierto x equipos que no están siendo administrados desde Advanced EDR**. Haz clic en el enlace para abrir el listado **Equipos no administrados descubiertos**.
- Accede a la sección **Mis listados** desde el panel lateral y haz clic en el enlace **Añadir**. Selecciona en el desplegable el listado **Equipos no administrados descubiertos**.

Listado Equipos no administrados descubiertos

Este listado contiene los equipos descubiertos en la red del cliente que no tienen instalado Advanced EDR o que, habiéndose instalado correctamente, su funcionamiento no es el adecuado.

Campo	Descripción	Valores
Equipo	Nombre del equipo descubierto.	Cadena de caracteres
Estado	Estado en el que se encuentra el equipo con respecto al proceso de instalación.	— No administrado: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. 📶 Instalando: el proceso de instalación se ha iniciado. 🔴 Error instalando: mensaje con el tipo de error producido en la instalación. Para una relación de mensajes de error y la explicación de cada uno de ellos, consulta Sección alertas de equipo (2) en la página 220. Si el error es de origen desconocido, se mostrará su código de error asociado.
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor.	Cadena de caracteres
Ruta de directorio activo	Ruta del directorio activo donde el equipo ha sido descubierto por última vez.	Cadena de caracteres
Último descubridor	Nombre del dispositivo que descubrió más recientemente el puesto de trabajo o servidor.	Cadena de caracteres
Última vez visto	Fecha en la que el equipo fue descubierto por	Fecha

Campo	Descripción	Valores
	última vez.	

Tabla 5.2: Campos del listado de equipos no administrados descubiertos

Cuando el campo **Estado** muestra **Error instalando** y es un error de origen conocido, se añade una cadena de texto que lo describe. Para obtener un listado de los errores de instalación reportados por Advanced EDR, consulta [Sección alertas de equipo \(2\)](#) en la página 220 .

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Nombre	Nombre del equipo descubierto.	Cadena de caracteres
IP	Dirección IP principal del equipo.	Cadena de caracteres
Dirección MAC	Dirección física del equipo.	Cadena de caracteres
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Directorio activo	Ruta del directorio activo donde el equipo ha sido descubierto por última vez.	Cadena de caracteres
Primera vez visto	Fecha en la que el equipo fue	Cadena de caracteres

Campo	Descripción	Valores
	descubierto por primera vez.	
Primera vez visto por	Nombre del equipo descubridor que vio por primera vez al equipo de usuario.	Cadena de caracteres
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha
Última vez visto por	Nombre del equipo descubridor que vio por última vez al equipo de usuario.	Cadena de caracteres
Descripción	Descripción del equipo descubierto.	Cadena de caracteres
Estado	Estado en el que se encuentra el equipo con respecto al proceso de instalación.	• No administrado: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. • Instalando: el proceso de instalación se ha iniciado. • Error instalando: mensaje con el tipo de error producido en la instalación. Para una relación de mensajes de error y la explicación de cada uno de ellos, consulta Sección alertas de equipo (2) en la página 220.
Error	Descripción del error encontrado.	Para más información, consulta Sección alertas de equipo (2) en la página 220.
Fecha error instalación	Fecha y hora en la que se produjo el error.	Fecha

Tabla 5.3: Campos del fichero exportado del listado de equipos no administrados descubiertos

Herramienta de búsqueda

Campo	Descripción	Valores
Buscar	Búsqueda por el nombre del equipo, IP, fabricante de la tarjeta de red o equipo descubridor.	Cadena de caracteres
Estado	Estado de la instalación de Advanced EDR.	• No administrado: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. • Instalando: el proceso de instalación se ha iniciado. • Error instalando: mensaje con el tipo de error producido en la instalación.
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	• Últimas 24 horas • Últimos 7 días • Último mes
Método de descubrimiento	Método empleado para descubrir al equipo	• Todos • Escaneo de red. Consulta Descubrimiento de equipos e instalación remota del software cliente • Directorio activo. Consulta Descubrimiento de equipos e instalación remota del software cliente

Tabla 5.4: Campos de filtrado para el listado de equipos no administrados descubiertos

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo.

Detalle de los equipos descubiertos

En el listado de **Equipos no administrados descubiertos**, haz clic en un equipo descubierto para ver su ventana de detalle dividida en tres secciones:

- **Alertas de equipo (1):** muestra potenciales problemas asociados a la instalación del equipo.
- **Detalles del equipo (2):** muestra un resumen ampliado del hardware, software y seguridad configurada en el equipo.
- **Último descubridor (3):** muestra los equipos descubridores que vieron el equipo no administrado.

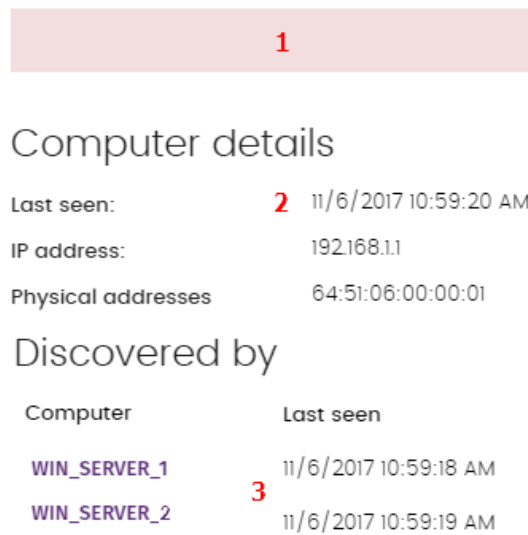


Figura 5.7: Distribución de la información en un equipo descubierto

Alertas de equipo (1)

Estado	Tipo	Resolución
Error instalando el agente de Cytomic	Indica el motivo del error en la instalación del agente.	
	Credenciales incorrectas	Lanza de nuevo la instalación con unas credenciales que tengan suficientes privilegios para realizar la instalación.
	No es posible conectar con el equipo	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible descargar el instalador del agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible copiar el instalador del agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible instalar el agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible registrar el agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.

Estado	Tipo		Resolución
Error instalando la protección de Advanced EDR	Indica el motivo del error en la instalación de la protección.		
	No hay suficiente espacio libre en el disco para realizar la instalación	Para ver los requisitos de espacio necesarios para instalar Advanced EDR, consulta Requisitos hardware en la página 853 .	
	El servicio de Windows Installer no está operativo	Comprueba que el servicio Windows Installer se esté ejecutando. Detiene y pone en marcha el servicio.	
	El usuario canceló la desinstalación de la protección de otro fabricante	Acepta la desinstalación del antivirus de terceros.	
	Hay otra instalación en curso	Espera a que finalice la instalación previa.	
	Error desinstalando automáticamente protecciones de otros fabricantes	Para ver una lista de fabricantes con desinstalador compatible con Cytomic, consulta Desinstaladores compatibles .	
	Desinstalador no disponible para protección de otro fabricante	Contacta con el departamento de soporte para pedir un desinstalador.	
Instalando agente de Cytomic	Una vez terminado el proceso de instalación, el equipo dejará de aparecer en el listado de Equipos no administrados descubiertos.		
Equipo no administrado	El equipo no tiene el agente Cytomic instalado. Comprueba que se trata de un equipo compatible con Advanced EDR y que cumple con los requisitos indicados en Funcionalidades del producto y requisitos en la página 847 .		

Tabla 5.5: Campos del listado Equipos protegidos

Detalles del equipo (2)

Campo	Descripción
Nombre del equipo	Nombre del equipo descubierto.

Campo	Descripción
Descripción	Permite asignar una descripción al equipo, aunque no esté administrado todavía.
Primera vez visto	Fecha y hora de la primera vez que el equipo fue descubierto.
Última vez visto	Fecha y hora de la última vez que el equipo fue descubierto.
Ruta de directorio activo	En el caso de ser un equipo no administrado descubierto mediante directorio activo, indica la ruta en la que fue descubierto.
Dirección IP	Dirección IP de la tarjeta de red del equipo descubierto.
Direcciones físicas (MAC)	Dirección física de la tarjeta de red del equipo descubierto.
Dominio	Dominio Windows al que pertenece el equipo.
Fabricante NIC	Fabricante de la tarjeta de red instalada en el equipo.

Tabla 5.6: Detalles de los equipos descubiertos

Último descubridor (3)

Campo	Descripción
Equipo	Nombre del equipo descubridor que vio al equipo no administrado.
Última vez visto	Fecha y hora de la última vez que el equipo fue visto por el equipo descubridor.
Método de descubrimiento	Indica si el equipo fue descubierto mediante directorio activo o a través del escaneo de red.

Tabla 5.7: Último descubridor

Borrar y ocultar equipos

Borrar equipos

Advanced EDR no elimina de la lista **Equipos no administrados descubiertos** los equipos que una vez fueron detectados pero ya no están accesibles por haberse retirado (avería, robo o cualquier otra razón).

Para eliminar de forma manual estos equipos nunca más accesibles, sigue los pasos mostrados a continuación:

- En **Equipos no administrados descubiertos** haz clic en **Descubiertos** u **Ocultos** en la parte superior derecha del listado.
- Selecciona las casillas correspondientes de los equipos a borrar.
 - Para borrar varios equipos, haz clic en el menú de contexto general y en **Eliminar**.
 - Para borrar un único equipo, haz clic en el menú de contexto del equipo y en **Eliminar**.



Un equipo que se elimina de la consola sin desinstalar el software Advanced EDR, y sin retirarse físicamente de la red, volverá a aparecer en la siguiente tarea de descubrimiento. Borra únicamente los equipos que nunca más vayan a ser accesibles.

Equipos ocultos

Para evitar generar listados muy extensos de equipos no administrados descubiertos que incluyan dispositivos sin interés para la instalación de Advanced EDR, es posible ocultarlos de forma selectiva:

- En **Equipos no administrados descubiertos** haz clic en **Descubiertos** en la parte superior derecha del listado.
- Selecciona las casillas correspondientes de los equipos a ocultar.
- Para ocultar varios equipos, haz clic en el menú de contexto general y en **Ocultar y no volver a descubrir**.
- Para ocultar un único equipo, haz clic en el menú de contexto del equipo y en **Ocultar y no volver a descubrir**.

Instalación remota del software cliente

El administrador de la red puede instalar de forma remota el software de seguridad en los equipos sin proteger descubiertos. Para ello, es necesario disponer de un equipo descubridor configurado que pueda establecer una conexión con el equipo a instalar.



La instalación remota es compatible con plataformas Windows.

Requisitos de red y sistema operativo

Para poder instalar Advanced EDR de forma remota, es necesario que los equipos cumplan con los requisitos indicados a continuación:

- Abrir los puertos UDP 21226 y 137 para el proceso `System`.
- Abrir el puerto TCP 445 para el proceso `System`.
- Habilitar el protocolo NetBIOS sobre TCP.
- Permitir las resoluciones DNS.
- Acceso al recurso de administración `Admin$`. En las ediciones "Home" de Windows es necesario habilitar este recurso de forma explícita.
- Credenciales de administrador de dominio o de la cuenta de administrador local generada por defecto en la instalación del sistema operativo.
- Activar la Administración remota.



*Para cumplir con estos requisitos de forma rápida sin necesidad de añadir reglas de forma manual en el firewall de Windows, selecciona **Activar la detección de redes y Activar el uso compartido de archivos e impresoras** en Centro de redes y recursos compartidos, Configuración de uso compartido avanzado.*

- Adicionalmente, para que un equipo de la red con Advanced EDR instalado pueda descubrir a otros equipos es necesario que:
 - No estén ocultos por el administrador.
 - No estén siendo ya administrados por Advanced EDR sobre Cytomic Platform.
 - Se encuentren en el mismo segmento de subred al que pertenece el equipo descubridor.

Instalación remota desde el listado de Equipos no administrados descubiertos

- Accede al listado de **Equipos no administrados descubiertos**.
 - Desde el panel lateral **Mis listados, Añadir**, selecciona el listado **Equipos no administrados descubiertos**.
 - Desde el menú superior **Estado** en el widget **Estado de la protección**, haz clic en el enlace **Se han descubierto x equipos que no están siendo administrados desde Advanced EDR**.
 - Desde el menú superior **Equipos** haz clic en **Añadir equipos** y selecciona **Descubrimiento e instalación remota**. Se mostrará una ventana con un asistente. Haz clic en el enlace **Ver equipos no administrados descubiertos**.
- En el listado de **Equipos no administrados descubiertos**, haz clic en **Descubiertos u Ocultos** dependiendo del estado del dispositivo.
- Selecciona las casillas correspondientes a los equipos a instalar.

- Para instalar varios equipos, haz clic en el menú de contexto general y en **Instalar agente de Cytomic**.
- Para instalar un único equipo, haz clic en el menú de contexto del equipo y en **Instalar agente de Cytomic**.
- Configura la instalación según los pasos descritos en **Generar el paquete de instalación y despliegue manual**.
- Escribe una o varias credenciales de instalación. Es necesario utilizar una cuenta de administración local del equipo o del dominio al que pertenece para completar la instalación con éxito.

Instalación remota desde la pantalla de detalles de equipo

Al hacer clic en un equipo descubierto se mostrará su detalle y en la parte superior el botón **Instalar agente de Cytomic**. Sigue los pasos descritos en **Generar el paquete de instalación y despliegue manual**.

Diferencias en la instalación según el método de descubrimiento utilizado

El procedimiento para instalar la protección en los equipos seleccionados varía en función del método por el que fueron descubiertos.

Instalar la protección en equipos descubiertos mediante escaneo de red

Cuando un equipo descubre a otro mediante escaneo de red, siempre tiene conexión con éste, de forma que no requiere ninguna configuración adicional con respecto a lo descrito en **Generar el paquete de instalación y despliegue manual**.

- Si todos los equipos han sido descubiertos por el mismo equipo descubridor: el equipo descubridor lanzará la instalación sobre todos los equipos descubiertos.
- Si NO todos los equipos han sido descubiertos por el mismo equipo descubridor: cada equipo descubridor lanzará la instalación sobre los equipos que hayan sido descubiertos por él.

Instalar la protección en equipos descubiertos mediante directorio activo

Cuando un equipo descubre a otro mediante la búsqueda en directorio activo, no significa necesariamente que tenga conexión con él. En este caso, para hacer una instalación remota del software de seguridad, es imprescindible seleccionar el equipo descubridor que se conectará con él para realizar la instalación.

- Si todos los equipos seleccionados han sido descubiertos solo mediante directorio activo: el administrador deberá seleccionar los equipos instaladores, que lanzarán la instalación sobre los equipos seleccionados.
- Si entre los equipos seleccionados hay alguno o algunos que han sido descubiertos mediante ambos métodos, el administrador deberá seleccionar el equipo descubridor, que lanzará la instalación solo sobre aquellos equipos seleccionados que hayan sido descubiertos exclusivamente mediante directorio activo. Para el resto de equipos la instalación se llevará a cabo de la forma habitual, según lo indicado en **Generar el paquete de instalación y despliegue manual**.

Errores posibles en la instalación

Si el equipo instalador no logra conectarse correctamente al equipo descubierto, se mostrarán los errores de instalación:

- En el listado de equipos no administrados descubiertos: **Error instalando. No es posible conectar con el equipo.** Consulta [Visualizar equipos descubiertos](#)
- En la ventana [Información de equipo](#) en la página **218**: **Error instalando el agente de Cytomic. Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.** Consulta [Descubrimiento de equipos e instalación remota del software cliente](#).

Instalación en sistemas Linux

Visión general del despliegue de la protección

El proceso de instalación en equipos Linux comprende varios pasos, dependiendo del estado de la red en el momento del despliegue y del número de equipos a proteger:

- Localizar los equipos desprotegidos en la red
- Satisfacer los requisitos mínimos
- Desinstalar productos de la competencia y reiniciar equipos
- Establecer la configuración por defecto de los equipos
- Establecer el método de instalación en los equipos
- Comprobar que el software de seguridad se instaló correctamente.

Localizar los equipos desprotegidos en la red

Localiza los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con Advanced EDR, y comprueba que el número de licencias libres contratadas es suficiente. Consulta [Licencias](#) en la página **157**.



Advanced EDR permite la instalación del software sin tener contratadas licencias suficientes. Estos equipos serán visibles en la consola de administración y mostrarán el software instalado, hardware y otras características, pero no estarán protegidos frente al malware.

Satisfacer los requisitos mínimos

Para conocer los requisitos mínimos, consulta [Requisitos de instalación](#).

Desinstalar productos de la competencia

Se recomienda desinstalar el antivirus y el software de seguridad de terceras compañías antes de iniciar la instalación de Advanced EDR.

Establecer la configuración por defecto de los equipos

Con el objeto de proteger a los equipos de la red desde el primer momento, Advanced EDR establece las configuraciones por defecto asignadas al grupo **Todos**. En el proceso de despliegue, es posible cambiar el grupo al que pertenecerá el equipo para asignarle otras configuraciones. Consulta [Gestión de configuraciones](#) en la página 251.

Comprobar que el software de protección se instaló correctamente

- Selecciona el menú superior **Equipos** y localiza el equipo instalado. Para obtener más información sobre buscar equipos consulta [Gestión de equipos y dispositivos](#) en la página 177.
- Haz clic en el equipo en el que has instalado el software de seguridad. Se abrirá la ventana de detalles del equipo.
- Haz clic en la pestaña **Detalles**. Se mostrará toda la información recogida del equipo y el estado de la instalación.
- En la sección **Seguridad** comprueba el estado de los distintos módulos:
 - **Instalando...**: el proceso de instalación no se ha completado o ha terminado en error. Espera unos minutos.
 - **Activado / desactivado**: transcurridos unos minutos, si la instalación terminó correctamente se mostrará el estado de los módulos de protección.

Detectar y solucionar fallos de instalación

Si transcurridos unos minutos la sección **Seguridad** desaparece del detalle del equipo, esto indica que el software de seguridad no se instaló correctamente. Comprueba los siguientes puntos:

- Si el equipo tiene instalada una interface gráfica comprueba si se muestran mensajes de error.
- Comprueba si el equipo se muestra en los listados. Consulta [Comprobar el despliegue](#).
- Consulta que el equipo del usuario cumple con los requisitos indicados en [Requisitos de instalación](#) y actualiza la versión del producto o la versión del sistema operativo. Consulta [Actualización del producto](#) en la página 171.

Requisitos de instalación

Comprueba que el equipo donde vas a instalar el software de seguridad cumple con la lista de requisitos mostrada a continuación, y que los recursos de red necesarios se encuentran disponibles.

Versiones del sistema operativo compatibles

Consulta [Distribuciones soportadas](#) en la página 859.

Kernels soportados

Para comprobar las versiones del kernel de Linux soportadas en cada distribución, consulta [Kernels soportados](#).

Hardware

Consulta [Requisitos hardware](#) en la página 860.

Requisitos de red

Se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento de la detección web de malware. En equipos sin entorno gráfico, la detección web está deshabilitada.

En su funcionamiento normal, Advanced EDR accede a varios recursos alojados en Internet. De forma general se requiere acceso a los puertos 80 y 443.

El agente Advanced EDR requiere acceso al puerto 33000 para la comunicación entre equipos protegidos de la red (consulta [Configuración de Control de Acceso a Endpoints](#) en la página 458 y con dispositivos Firebox o Access Point (consulta [Control de acceso a redes](#) en la página 282

Para un listado completo de las URLs a las que se accede desde los equipos con el software Advanced EDR instalado, consulta [Puertos locales y acceso a URLs](#) en la página 862.

Sincronización horaria de los equipos (NTP)

Aunque no es un requisito indispensable, es muy recomendable que el reloj de los equipos protegidos con Advanced EDR esté sincronizado. La mayoría de las veces, la sincronización se establece mediante el uso de un servidor NTP. Consulta [Sincronización horaria de los equipos \(NTP\)](#) en la página 854.

Acceso al repositorio de la distribución

El proceso de instalación del software de protección tiene como requisito acceder al repositorio donde están almacenados los paquetes de la instalación, siendo el proveedor de la distribución el encargado de mantener al menos un repositorio por cada versión publicada. En muchos casos, al entrar en EOL una versión, el proveedor da de baja el repositorio, con lo que la instalación del software de seguridad fallará. En estos casos se recomienda:

- Utilizar un repositorio local si existe.
- Utilizar la instalación sin dependencias. Consulta [Plataformas Linux con conexión limitada](#) en la página 140.

Paquetes instalados en el equipo

El script de instalación realiza algunas comprobaciones en su inicio que requieren la instalación de uno de los siguientes paquetes:

- wget
- curl

Si ninguno de los paquetes está instalado, la instalación terminará con error.

Generar el paquete de instalación y despliegue manual

- En el menú superior **Equipos** de la consola de administración, haz clic en el botón **Añadir equipos** situado en la parte superior derecha de la pantalla. Se mostrará una ventana con las plataformas compatibles con Advanced EDR.
- Haz clic en el icono **Linux**. Se mostrará la ventana **Linux**.



Figura 5.8: Ventana de selección de plataforma compatible con Advanced EDR

- Para elegir el grupo en el que se integrarán los equipos, haz clic en el desplegable **Añadir los equipos al siguiente grupo**.
- Para integrar el equipo en un grupo Directorio Activo, haz clic en **Añadir los equipos en su ruta de Directorio Activo**.



*Las políticas de seguridad asignadas a un equipo dependen del grupo al que pertenece. Si has elegido **Añadir los equipos en su ruta de Directorio Activo** y el administrador del directorio activo de la empresa mueve el equipo de una unidad organizativa a otra, este cambio se replicará en la consola de Advanced EDR como un cambio de grupo. Por esta razón, las políticas de seguridad asignadas a ese equipo también podrían cambiar sin ser advertido por el administrador de la consola Web.*

- Para establecer una configuración de red alternativa al grupo donde se integrará el equipo, haz clic en **Selecciona la configuración de red para los equipos** y elige una configuración de red en el desplegable. Inicialmente, todas las configuraciones que se aplican al equipo en el momento de la integración son las que están asignadas al grupo de la consola al que pertenecerá. Sin embargo, para prevenir fallos de conectividad y evitar que el equipo quede inaccesible desde la consola de administración por una configuración de red no apropiada, es posible establecer una configuración de red alternativa. Para más información sobre cómo crear configuraciones de red, consulta

Configuración remota del agente en la página 271.

- Para enviar el instalador al usuario por correo electrónico:
 - Haz clic en el botón **Enviar URL por email**. Se mostrará la aplicación de correo instalada por defecto en el equipo del administrador, con un mensaje pregenerado que contiene la URL de descarga.
 - Añade al mensaje los destinatarios de correo y haz clic en el botón **Enviar**.
 - El usuario que reciba el correo deberá hacer clic en la URL desde el dispositivo para iniciar la descarga del instalador.
- Para descargar el paquete de instalación y compartirlo con los usuarios de la red, haz clic en el botón **Descargar instalador**.

Instalación en plataformas Linux

Dependiendo de las características del equipo destino, el agente puede instalarse de varias maneras:

- Instalación en plataformas Linux con conexión a Internet
- Instalación en plataformas Linux con Secure Boot
- Instalación en plataformas Linux sin conexión a Internet (sin dependencias)

Instalación en plataformas Linux con conexión a Internet

Instalar el producto en el equipo de usuario requiere permisos de administrador y que el paquete descargado tenga permisos de ejecución. Al ejecutar el programa de instalación, éste localizará en el equipo del usuario todas las librerías que necesita. Las librerías que no consiga encontrar las descargará de Internet de forma automática.

- Abre una terminal en la carpeta donde reside el paquete descargado y ejecuta los comandos siguientes.

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

- En equipos bastionados utiliza el comando `--target ./install/` para generar una carpeta temporal en la ubicación del script.

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

- Si utilizas un servidor proxy para acceder a Internet, añade el parámetro `--proxy`. Si quieres indicar una lista de proxies, utiliza el parámetro `--proxy=<proxy-list>`. El script de instalación utilizará el primer proxy de la lista y, en caso de error, recorrerá la lista de proxies especificada hasta encontrar uno que funcione correctamente.

`<proxy-list>` es una lista de servidores proxy separadas por comas indicando el usuario y el protocolo con la sintaxis:

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

Por ejemplo, para instalar un agente Linux que utilizará dos proxies:

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

- Para comprobar que el proceso `AgentSvc` se está ejecutando, utiliza el comando siguiente:

```
$ ps ax | grep AgentSvc
```

- Para comprobar que se han creado los directorios de instalación:

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

Instalación en plataformas Linux con Secure Boot

Algunas distribuciones Linux detectan si el equipo tiene la funcionalidad de Secure Boot activada, que deshabilita el software de protección que no esté debidamente firmado. La presencia de Secure Boot puede ser detectada tanto en el momento de la instalación del software de protección como más adelante, si la distribución originalmente no daba soporte a esta funcionalidad, pero posteriormente se añade en alguna actualización. En ambos casos, se muestra un error en la consola y el software de protección no funcionará. Para habilitar el software de protección en este caso, es necesario seguir el procedimiento y cumplir con los requisitos mostrados a continuación.

Requisitos de la distribución

- **Sistemas DKMS (Dynamic Kernel Module Support)**: paquetes `mokutil` y `openssl` instalados.
- **Oracle Linux 7.x/8.x y kernel UEKR6**: repositorio `ol7_optional_latest` activado y los paquetes `openssl`, `keyutils`, `mokutil`, `psign`, `kernel-uek-devel-$(uname -r)` instalados.

Habilitar el software de protección en equipos con Secure Boot activado

Para habilitar el software de protección es necesario seguir el procedimiento mostrado a continuación directamente en el equipo, ya que es necesario interactuar con su sistema de arranque:

- Comprueba el estado de Secure Boot:

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

Si Secure Boot está activado en el equipo se muestra el mensaje `Secure Boot enabled`.

- Verifica que el driver de la protección no está cargado:

```
$ lsmod | grep prot
```

- Importa las claves de la protección:

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



Los ficheros del agente y de la protección tienen el formato **protection-agent-03.01.00.0001-1.5.0_741_g8e14e52**. El nombre varía en función de la versión y del driver.

Se muestra un mensaje de aviso sobre las implicaciones del uso de Secure Boot.

- Presiona C para registrar el certificado usado para firmar los módulos.
- Genera una contraseña de ocho caracteres.
- Reinicia el equipo y completa el proceso de registro:
 - Presiona cualquier tecla para iniciar el proceso de registro (esta pantalla tiene un tiempo limitado, por lo que si no se presiona ninguna tecla dentro del tiempo definido, habrá que reiniciar el proceso de registro).
 - En el menú, selecciona la opción **Enroll MOK**. Se abrirá un nuevo menú que muestra el número de KEYS que se van a registrar.
 - Selecciona la opción **View key** para revisar que las KEYS son las correspondientes a la protección de Panda Security, y selecciona la opción **Continue** para seguir con el proceso de registro.
 - Cuando aparezca la opción **Enroll the key**, selecciona **Yes**.
 - Escribe la contraseña generada en el paso 3 y reinicia el equipo con la opción **REBOOT**.
 - Comprueba que el driver está cargado:

```
$ lsmod | grep prot
```

Oracle Linux 7.x/8.x con Kernel UEKR6

Una vez terminado el procedimiento general, si la distribución instalada en el equipo es Oracle Linux 7.x/8.x con kernel UEKR6, sigue estos pasos adicionales:

- Vuelve a ejecutar el comando:

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

Se añadirá el certificado con el que se firmaron los módulos a la lista de certificados confiables del kernel. Se firmará el kernel modificado y se añadirá a la lista de kernels de GRUB.

- Reinicia el equipo. El módulo estará cargado y arrancado.
- Para comprobar que el certificado se ha añadido correctamente ejecuta el comando:

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

Se obtiene como resultado:

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

Plataformas Linux con conexión limitada

Advanced EDR tiene como requisito el acceso a Internet para su correcto funcionamiento, pero el administrador puede querer limitar la conexión de los servidores donde se ejecuta para evitar la descarga o envío de información desde o hacia proveedores externos desconocidos. En este caso, Advanced EDR no puede completar el proceso de instalación del software de seguridad porque requiere el acceso a repositorios externos para satisfacer sus dependencias.

La instalación en plataformas Linux con conexión limitada permite la instalación del software de seguridad cuando el equipo únicamente tiene acceso a la nube de Cytomic, de donde se descargará un paquete con todas las dependencias necesarias.



En este método de instalación, las librerías de terceros incluidas en el paquete y que presenten fallos o se descubran vulnerabilidades a lo largo del tiempo no se actualizarán en el equipo protegido de forma automática.

El instalador es compatible con las distribuciones basadas en RedHat:

- RedHat
- CentOS
- CentOS Stream
- SuSE Linux Enterprise
- OpenSUSE

- Oracle Linux
- Alma Linux
- Rocky Linux

Para conocer las versiones compatibles de estas distribuciones consulta [Distribuciones soportadas](#) en la página **859**

El instalador es compatible con las siguientes versiones de agente y protección Linux:

- Protección 3.00.00.0050 y posteriores
- Agente 1.10.06.0050 y posteriores

Si se utiliza la instalación sin dependencias en una distribución no compatible, la instalación dará un error. Este método de instalación solo es posible sobre equipos sin versiones anteriores del software de seguridad. En caso contrario, se mantiene la configuración previa del repositorio.

Para instalar el agente Advanced EDR abre una terminal en la carpeta donde reside el paquete descargado y ejecuta:

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

Instalación en sistemas macOS

Visión general del despliegue de la protección

El proceso de instalación en equipos macOS comprende varios pasos, dependiendo del estado de la red en el momento del despliegue y del número de equipos a proteger :

- Localizar los equipos desprotegidos en la red
- Satisfacer los requisitos mínimos
- Desinstalar productos de la competencia
- Establecer la configuración por defecto de los equipos
- Comprobar que el software de seguridad se instaló correctamente.

Localizar los equipos desprotegidos en la red

Localiza los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con Advanced EDR y comprueba que el número de licencias libres contratadas es suficiente. Consulta [Licencias](#) en la página **157**.



Advanced EDR permite la instalación del software sin tener contratadas licencias suficientes. Estos equipos serán visibles en la consola de administración y mostrarán el software instalado, hardware y otras características, pero no estarán protegidos frente al malware.

Satisfacer los requisitos mínimos

Para conocer los requisitos mínimos consulta [Requisitos de instalación](#).

Desinstalar productos de la competencia

Se recomienda desinstalar el antivirus y el software de seguridad de terceras compañías antes de iniciar la instalación de Advanced EDR.

Establecer la configuración por defecto de los equipos

Con el objeto de proteger a los equipos de la red desde el primer momento, Advanced EDR establece las configuraciones por defecto asignadas al grupo **Todos**. En el proceso de despliegue, es posible cambiar el grupo al que pertenecerá el equipo para asignarle otras configuraciones. Consulta [Gestión de configuraciones](#) en la página 251.

Comprobar que el software de protección se instaló correctamente

- Selecciona el menú superior **Equipos** y localiza el equipo instalado. Para obtener más información sobre buscar equipos consulta [Gestión de equipos y dispositivos](#) en la página 177.
- Haz clic en el equipo en el que has instalado el software de seguridad. Se abrirá la ventana de detalles del equipo.
- Haz clic en la pestaña **Detalles**. Se mostrará toda la información recogida del equipo y el estado de la instalación.
- En la sección **Seguridad** comprueba el estado de los distintos módulos:
 - **Instalando...**: el proceso de instalación no se ha completado o ha terminado en error. Si el proceso terminó en error, el estado no cambiará hasta que se resuelva el problema de instalación.
 - **Activado / desactivado**: transcurridos unos minutos, si la instalación terminó correctamente se mostrará el estado de los módulos de protección.

Detectar y solucionar fallos de instalación

Si transcurridos unos minutos la sección **Seguridad** desaparece del detalle del equipo, esto indica que el software de seguridad no se instaló correctamente. Comprueba los siguientes puntos:

- Comprueba en el equipo del usuario si se muestran mensajes de error.
- Comprueba si el equipo se muestra en los listados. Consulta [Comprobar el despliegue](#).

- Consulta que el equipo del usuario cumple con los requisitos indicados en **Requisitos de instalación** y actualiza la versión del producto o la versión del sistema operativo. Consulta **Actualización del producto** en la página 171.

Requisitos de instalación

Comprueba que el equipo donde vas a instalar el software de seguridad cumple con la lista de requisitos mostrada a continuación, y que los recursos de red necesarios se encuentran disponibles.



A partir de la fecha 30/09/2024 no será posible añadir a la consola de administración nuevos equipos que utilicen los siguientes sistemas operativos: Yosemite, El Capitan, Sierra, High Sierra y Mojave. Los equipos instalados en una fecha anterior seguirán protegidos. Consulta <https://www.watchguard.com/wgrd-trust-center/end-of-life-policy>.

Versiones del sistema operativo compatibles

Consulta **Sistemas operativos soportados** en la página 856.

Hardware

Consulta **Requisitos hardware** en la página 857.

Requisitos de red

En su funcionamiento normal Advanced EDR accede a varios recursos alojados en Internet. De forma general, se requiere acceso a los puertos 80 y 443. Para un listado completo de las URLs a las que se accede desde los equipos con el software Advanced EDR instalado, consulta **Puertos locales y acceso a URLs** en la página 862.

El agente Advanced EDR requiere acceso al puerto 33000 para la comunicación entre equipos protegidos de la red (consulta **Configuración de Control de Acceso a Endpoints** en la página 458 y con dispositivos Firebox o Access Point (consulta **Control de acceso a redes** en la página 282

Para poder activar el producto es necesario disponer de acceso a ciertos rangos de direcciones IP. Para más información, consulta **Direcciones IP necesarias para activar el producto** en la página 857

Sincronización horaria de los equipos (NTP)

Aunque no es un requisito indispensable, es muy recomendable que el reloj de los equipos protegidos con Advanced EDR esté sincronizado. La mayoría de las veces, la sincronización se establece mediante el uso de un servidor NTP. Consulta **Sincronización horaria de los equipos (NTP)** en la página 854.

Permisos necesarios

Para el correcto funcionamiento de la protección, es necesario:

- Activar extensiones de red.
- Activar extensiones de sistema.

- Activar el acceso total al disco.
- Activar la ejecución en segundo plano.

Para más información, consulta [Permisos necesarios](#) en la página 857.

Despliegue manual del agente macOS

- En el menú superior **Equipos** de la consola de administración, haz clic en el botón **Añadir equipos** situado en la parte superior derecha de la pantalla. Se mostrará una ventana con las plataformas compatibles con Advanced EDR.
- Haz clic en el icono **macOS**. Se mostrará la ventana **macOS**.



Figura 5.9: Ventana de selección de plataforma compatible con Advanced EDR

- Para elegir el grupo en el que se integrarán los dispositivos, haz clic en el desplegable **Añadir los equipos al siguiente grupo**.
- Para establecer una configuración de red alternativa al grupo donde se integrará el equipo, haz clic en **Selecciona la configuración de red para los equipos** y elige una configuración de red en el desplegable. Inicialmente, todas las configuraciones que se aplican al equipo en el momento de la integración son las que están asignadas al grupo de la consola al que pertenecerá. Sin embargo, para prevenir fallos de conectividad y evitar que el equipo quede inaccesible desde la consola de administración por una configuración de red no apropiada, es posible establecer una configuración de red alternativa. Para más información sobre cómo crear configuraciones de red, consulta [Configuración remota del agente](#) en la página 271.

Para enviar el instalador al usuario por correo electrónico:

- Haz clic en el botón **Enviar URL por email**. Se mostrará la aplicación de correo instalada por defecto en el equipo del administrador con un mensaje ya generado que contiene la URL de descarga.

- Añade al mensaje los destinatarios de correo y haz clic en el botón **Enviar**.
- El usuario que reciba el correo deberá hacer clic en la URL desde el dispositivo para iniciar la descarga del instalador.
- Para descargar el paquete de instalación y compartirlo con los usuarios de la red haz clic en el botón **Descargar instalador (7)**.

Instalación del paquete descargado

- Haz doble clic en el archivo `.dmg` y ejecuta el contenedor `.pkg`. Durante el proceso de instalación se mostrará una ventana con el progreso de la tarea. Independientemente de si existen licencias libres disponibles, el equipo se integrará en el servicio. Si no hay licencias disponibles el equipo no estará protegido.
- Una vez completado, el producto comprobará que tiene la última versión del fichero de firmas y del motor de protección. Si no es así, iniciará una actualización automática.
- Para verificar la instalación del agente, ejecuta el siguiente comando que comprobará si el proceso `AgenSvc` se está ejecutando:

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

- También puedes comprobar que se han creado los siguientes directorios de instalación:

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



Para instalar el agente del producto en dispositivos con macOS Catalina, es necesario asignar permisos específicos. Para más información, consulta la web <https://www.pandasecurity.com/es/support/card?id=700079>.

Comprobar el despliegue

El administrador de la red dispone de tres formas complementarias para determinar el resultado del despliegue del software Advanced EDR en la red gestionada:

- Mediante el widget **Estado de protección**. Consulta **Estado de protección** en la página 608.
- Mediante el listado **Estado de la seguridad de los equipos**. Consulta **Estado de protección de los equipos** en la página 621.
- Mediante el registro **Aplicación** del visor de sucesos en los equipos Windows.

Visor de sucesos Windows

El registro **Aplicación** del visor de sucesos recoge información extendida sobre el resultado de la instalación del agente en el equipo del usuario y sobre su funcionamiento una vez instalado. A continuación se muestra una tabla con la información suministrada por Advanced EDR en cada campo del visor de sucesos.

Mensaje	Nivel	Categoría	Id
The device %deviceid% was unregistered	Advertencia	Registro (1)	101
The device %deviceid% was registered	Información	Registro (1)	101
A new Siteid %Siteid% was set	Advertencia	Registro (1)	102
Error %error%: Cannot change Siteid	Error	Registro (1)	102
Error %error%: Calling %method%	Error	Registro (1)	103
Error %code%: Registering device, %description%	Error	Registro (1)	103
Installation success of %fullPath% with parameters %parameters%	Información	Instalación (2)	201
A reboot is required after installing %fullPath% with parameters %parameters%	Advertencia	Instalación (2)	201
Error %error%: executing %fullPath% with parameters %parameters%	Error	Instalación (2)	201
Message: %Module% installer error with next 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	Instalación (2)	202
Uninstallation success of product with code %productCode% and parameters	Información	Desinstalación (4)	401

Mensaje	Nivel	Categoría	Id
%parameters%			
A reboot is required after uninstalling product with code %productCode% and parameters %parameters%	Advertencia	Desinstalación (4)	401
Error %error%: Uninstalling product with code %productCode% and parameters %parameters%	Error	Desinstalación (4)	401
Uninstallation of product with code %productCode% and command line %commandLine% was executed	Información	Desinstalación (4)	401
Error %error%: Uninstalling product with code %productCode% and command line %commandLine%	Error	Desinstalación (4)	401
Error %error%: Uninstalling product with code %productCode% and command line %commandLine%	Error	Desinstalación (4)	401
Generic uninstaller executed: %commandLine%	Información	Desinstalación (4)	402
Error %error%: executed generic uninstaller %commandLine%	Error	Desinstalación (4)	402
Configuration success of product with code %productCode% and command line %commandLine%	Información	Reparación (3)	301
A reboot is required after configuring product with code %productCode% and command line %commandLine%	Advertencia	Reparación (3)	301

Mensaje	Nivel	Categoría	Id
Error %error%: Configuring product with code %productCode% and command line %commandLine%	Error	Reparación (3)	301

Tabla 5.8: Códigos de resultado del proceso de instalación del agente en el visor de sucesos

Eliminación automática de equipos

Esta funcionalidad libera la licencia del software de seguridad de los equipos protegidos y los elimina de la consola. Los equipos a liberar han de cumplir ciertas condiciones, que se establecen mediante un filtro específico, que es necesario crear antes de activar la funcionalidad. Una vez creado el filtro, se aplicará de forma periódica.

Permisos necesarios

La eliminación automática de equipos es visible para todos los usuarios de la consola web, pero para poder configurar y modificar esta funcionalidad, el usuario ha de tener visibilidad total sobre todos los equipos y el permiso **Añadir, descubrir y eliminar equipos**.

Para más información, consulta [Descripción de los permisos implementados](#) en la página 70

Consecuencias de la eliminación



La eliminación de equipos tiene lugar una vez al día, entre las 01:00 y las 03:00 UTC.

Al eliminar un equipo:

- El equipo y toda su información desaparecerán de la consola web.
- El equipo quedará desprotegido.
- Si el equipo está cifrado, permanecerá cifrado pero no se podrán obtener las claves de recuperación.



Es recomendable apagar el equipo tras su eliminación, ya que de lo contrario volverá a aparecer en la consola web en el momento en que se conecte de nuevo a los servidores de Cytomic.

La información generada por un equipo protegido no se elimina definitivamente de los servidores de Advanced EDR: cuando se reasigna una licencia al equipo y se restablece su conexión con Cytomic, toda

su información aparecerá de nuevo en la consola web. No obstante, si al día siguiente el filtro no se ha desactivado, el equipo volverá a eliminarse.

Crear un filtro para eliminar equipos

Toda la información sobre los diferentes elementos disponibles para configurar un filtro está disponible en [Configurar filtros](#) en la página 184.



Ten en cuenta que al tratarse de una funcionalidad de eliminación de equipos, es recomendable que el nombre del filtro sea fácilmente identificable.

Para filtrar de manera que la búsqueda proporcione como resultado los equipos no conectados al servidor de Cytomic, utiliza los siguientes parámetros:

- **Categoría:** Equipo
- **Propiedad:** Última conexión
- **Operador:**
 - Está entre (para buscar los equipos no conectados entre fechas concretas).
 - Antes de (para buscar los equipos no conectados antes de una fecha concreta).
 - Después de (para buscar los equipos no conectados a partir de una fecha concreta).

Activar la funcionalidad

- Haz clic en el menú superior **Configuración**, panel lateral **Mantenimiento de equipos**.
- Desplaza el control deslizante **Activar la eliminación automática de equipos**.
- En el desplegable, selecciona el filtro que quieres aplicar.
- Haz clic en el botón **Guardar cambios**.



El filtro no puede ser modificado ni eliminado durante su ejecución.

Programar el envío periódico de los equipos a eliminar

El administrador puede programar el envío automático de un informe periódico con el listado de equipos que van a ser eliminados. Consulta [Acceso al envío de informes y listados](#) en la página 787

Desinstalar el software

Puedes desinstalar el software Advanced EDR de forma manual desde el panel de control del sistema operativo, o de forma remota desde el menú superior **Equipos** o desde los listados **Estado de la protección de los equipos** y **Licencias**.

Desinstalación manual

El propio usuario podrá ejecutar una desinstalación manual siempre y cuando el administrador de la protección no haya establecido una contraseña de desinstalación al configurar el perfil de la protección para su PC. Si lo ha hecho, se necesitará autorización o disponer de las credenciales necesarias para poder desinstalar la protección.



Para establecer o eliminar la password de desinstalación del agente, consulta [Configurar la seguridad frente a manipulaciones no deseadas de las protecciones](#) en la página 285.

La instalación de Advanced EDR incluye varios programas independientes, según sea la plataforma de destino:

- **Equipos Windows y macOS:** agente y protección.
- **Equipos Linux:** agente, protección y módulo del kernel.

Para desinstalar completamente Advanced EDR es necesario quitar todos los módulos. Si se desinstala únicamente el módulo de la protección, transcurrido un tiempo el agente la reinstalará de forma automática.

Windows 8 o superior

- Panel de Control > Programas > Desinstalar un programa.
- También puedes desinstalar tecleando, en el menú Metro: “desinstalar un programa”.

Windows Vista, Windows 7, Windows Server 2003 y superiores



A partir de la fecha 30/09/2024 no será posible añadir a la consola de administración nuevos equipos que utilicen los siguientes sistemas operativos: Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008 (no afecta a Windows Server 2008 R2). Los equipos instalados en una fecha anterior seguirán protegidos. Consulta <https://www.watchguard.com/wgrd-trust-center/end-of-life-policy>.

- Panel de Control > Programas y características > Desinstalar o cambiar un programa.

Windows XP

- Panel de Control > Agregar o quitar programas.

Desinstalar mediante la herramienta de desinstalación

En el caso de Windows, durante el proceso de desinstalación normal puede ocurrir que algunos archivos o librerías no se eliminen completamente, provocando ciertos mensajes de error. En estos casos, será necesario utilizar la herramienta que Cytomic pone a tu disposición para completar la desinstalación tanto del agente como de la protección.



Este proceso de desinstalación puede durar unos minutos. Una vez finalizado el proceso, reinicia el equipo.

Sigue los pasos que se indican a continuación:

- Descarga y descomprime el archivo **GU.zip** (contraseña "panda").
- Ejecuta el archivo de desinstalación del agente `GU_AGENT.exe` y reinicia el equipo.
- Ejecuta el archivo de desinstalación de la protección `GU_PROT.exe` y reinicia el equipo.

macOS



El soporte de macOS Yosemite, El Capitan, Sierra, High Sierra y Mojave, solo está disponible para clientes que contrataron Advanced EPDR en la versión 4.30 / 9.30 o anteriores.

- Abre el menú de comandos desde: Finder > Aplicaciones > Utilidades > Terminal
- Para desinstalar la protección ejecuta el comando `sudo sh /Applications/Endpoint-Protection.app/Contents/uninstall.sh`
- Para desinstalar el agente ejecuta el comando `sudo sh /Applications/Management-Agent.app/Contents/uninstall.sh`

Linux

En Linux se utiliza el entorno gráfico para gestionar paquetes incluidos en la distribución.

- **Fedora:** Actividades > Software > Instalado
- **Ubuntu:** Software de Ubuntu > Instaladas

Se recomienda utilizar la línea de comandos como `root` para desinstalar el producto. Utiliza el parámetro `--totp` si está activado el segundo factor de autenticación y `--pass` y has protegido con contraseña la

desinstalación del agente. Consulta **Configurar la seguridad frente a manipulaciones no deseadas de las protecciones** en la página 285.

```
$ /usr/local/management-agent/repositories/pa/install --remove --  
totp=valor  
  
(desinstala la protección)  
  
$ /usr/local/management-agent/repositories/ma/install --remove --  
pass="contraseña" --totp=valor  
  
(desinstala el agente y los repositorios)
```

Resultado de la desinstalación manual

Al desinstalar el software Advanced EDR (agente Cytomic y Protección) el equipo desaparecerá completamente de la consola de administración. Todos los contadores, entradas en informes e información de la actividad del equipo y de sus procesos se borrarán.

Si, posteriormente, el mismo equipo vuelve a ser integrado en la consola de administración mediante la reinstalación del software Advanced EDR, se recuperará toda la información previamente eliminada.

Desinstalación desde la consola de administración



Para equipos con macOS Catalina y Big Sur, la desinstalación remota del software de seguridad no está soportada. En estos casos, la desinstalación debe realizarse directamente en el equipo.

Para desinstalar el software de seguridad de equipos Windows, Linux o macOS desde la consola de administración:

- En el menú superior **Equipos**, o en los listados **Licencias** y **Estado de la protección de equipos** marca los equipos a desinstalar con las casillas de selección.
- En la barra de acciones haz clic en el botón **Eliminar**. Se mostrará una ventana de confirmación.
- En la ventana de confirmación haz clic en la casilla **Desinstalar el agente de Cytomic de los equipos seleccionados** para retirar por completo el software Advanced EDR.
- Para completar la desinstalación en equipos macOS, el software de protección le pedirá al usuario local del dispositivo la contraseña de una cuenta con permisos de administrador .

Reinstalación remota

Para resolver algunas situaciones donde el software Advanced EDR presenta un mal funcionamiento, se permite su reinstalación remota desde la consola de administración, tanto para equipos de usuario como para servidores.

La reinstalación del software se realiza por separado para el agente y para el módulo de la protección.

Requisitos de la funcionalidad de reinstalación remota

- Equipo de usuario o servidor con sistema operativo Windows instalado.
- Un equipo con el rol de descubridor asignado en el mismo segmento de red que el equipo a reinstalar y que comunique con la nube de Cytomic.
- Credenciales de una cuenta de administrador local o de dominio.

Acceso a la funcionalidad

Desde los listados mostrados a continuación accesibles en el menú superior **Estado**, haciendo clic en el enlace **Añadir** del panel lateral:

- **Estado de protección de los equipos** en la página 621.
- **Estado de gestión de parches** en la página 418.
- **Estado de Cytomic Data Watch** en la página 350.
- **Estado del cifrado** en la página 506.
- **Listados del módulo Licencias** en la página 164.
- **Hardware** en la página 209.

La funcionalidad también es accesible desde el listado de **Equipos** en el menú superior **Equipos**, haciendo clic en una rama del árbol de carpetas o filtros situado en el panel lateral.



Las opciones **Reinstalar la protección (requiere reinicio)** y **reinstalar agente** solo se mostrarán en equipos Windows.

Descubrimiento de equipos a reinstalar

Utiliza el listado **Equipos no administrados descubiertos** para localizar los dispositivos en los que es necesario realizar la reinstalación. Consulta **Visualizar equipos descubiertos**.

Reinstalación en un equipo

- Localiza en el listado el equipo a reinstalar.
- En el menú de contexto asociado al equipo selecciona la opción **Reinstalar la protección (requiere reinicio)**  o **Reinstalar el agente** . Se mostrará una ventana donde el administrador configurará el tipo de reinstalación. Consulta [Ventana de selección Reinstalar la protección](#) y [Ventana de selección Reinstalar el agente](#).

Reinstalación en varios equipos

- Selecciona con las casillas de selección en el listado los equipos que reinstalarán su protección o agente.
- En la barra de herramientas selecciona la opción **Reinstalar la protección (requiere reinicio)**  o **Reinstalar el agente** . Se mostrará una ventana donde el administrador configurará el tipo de reinstalación. Consulta [Ventana de selección Reinstalar la protección](#) y [Ventana de selección Reinstalar el agente](#).

Ventana de selección Reinstalar la protección

Al configurar la reinstalación de la protección, se abre una ventana flotante con dos opciones:

- **Reinstalar la protección inmediatamente (requiere reinicio):** el reinicio se producirá en el plazo de 1 minuto. Si el equipo de destino no está accesible en ese momento por encontrarse apagado o fuera de red, la petición de reinicio se mantendrá en el servidor Advanced EDR durante 1 hora.
- **Ofrecer un margen de tiempo antes de forzar la reinstalación:** el reinicio se producirá en el plazo configurado por el administrador. Si el equipo de destino no está accesible por encontrarse apagado o fuera de red, la petición de reinicio se mantendrá en el servidor Advanced EDR durante 7 días.

En el momento en que el administrador inicia la reinstalación de la protección, el usuario del equipo recibe un mensaje emergente dándole la posibilidad de reiniciar el equipo en ese momento o esperar a que finalice el tiempo definido por el administrador. Una vez que ha expirado el plazo, la protección se desinstalará y el equipo se reiniciará de forma automática para reinstalar la protección.

Si la desinstalación de la protección presenta algún tipo de problema, Advanced EDR iniciará de forma transparente para el usuario un desinstalador genérico que tratará de desinstalar nuevamente la protección y limpiar cualquier rastro en el equipo. Para ello es posible que se requiera un reinicio adicional.

Ventana de selección Reinstalar el agente

Al configurar la reinstalación del agente, se muestra una ventana flotante que solicita la información siguiente:

Seleccionar el equipo con el rol de descubridor desde el cual se reinstalará el agente:

- Asegúrate de que el equipo descubridor se encuentra en el mismo segmento de red que el equipo a reinstalar.
- Si el equipo descubridor está apagado, la petición se mantendrá en espera hasta que sea visible de nuevo. Las peticiones se mantienen en espera por un intervalo de 1 hora, transcurrido el cual se descartan.

Credenciales para reinstalar los equipos: escribe una o varias credenciales de instalación. Utiliza una cuenta de administración local del equipo o del dominio al que pertenece para completar la reinstalación con éxito.

Una vez introducida la información, el equipo con el rol de descubridor seguirá los pasos mostrados a continuación:

- Conectará con el equipo a reinstalar.
- Desinstalará el agente instalado en el equipo a reinstalar.
- Descargará un nuevo agente preconfigurado con el cliente, grupo y la configuración de red asignada al equipo, lo copiará y lo ejecutará remotamente en el equipo a reinstalar.
- Si hay algún problema en el transcurso de la operación, se lanzará el desinstalador genérico y, si es necesario, se mostrará al usuario un mensaje con una cuenta atrás para el reinicio del equipo automático y un botón para reiniciar de forma manual e inmediata.

Códigos de error

Para obtener un listado de los mensajes de error y las acciones recomendadas para corregirlos, consulta [Errores en el proceso de reinstalación del software de protección](#) en la página 226.

Capítulo 6

Licencias

Para proteger los equipos de la red de las amenazas es necesario contratar licencias de Advanced EDR en un número igual al número de puestos de usuario y servidores a proteger. Una licencia de Advanced EDR solo se puede asignar a un único dispositivo en un momento concreto.

A continuación se detalla el proceso de gestión de licencias de Advanced EDR: su asignación a los equipos de la red, liberación y comprobación de su estado.

Contenido del capítulo

Definiciones y conceptos clave	158
Mantenimientos	158
Estado de los equipos	158
Estado de las licencias y grupos	158
Tipos de licencias	159
Asignar licencias	159
Liberar licencias	160
Procesos asociados a la asignación de licencias	160
Caso I: Equipos con licencia asignada y equipos excluidos	160
Caso II: Equipos sin licencia asignada	161
Paneles / widgets del módulo licencias	162
Listados del módulo Licencias	164
Licencias caducadas	167
Comportamiento de los productos basados en Cytomic al caducar sus licencias	167
Comportamiento cuando caduca uno de los mantenimientos contratados	168
Comportamiento de Advanced EDR tras caducar todas las licencias	169
Renovar antes de 90 días tras caducar las licencias	169
Renovar tras más de 90 días desde la caducidad de las licencias	169
Mensajes de caducidad próxima y vencida	169
Buscar equipos según su estado de licencia	170

Definiciones y conceptos clave

Para interpretar correctamente la información y las gráficas suministradas por Advanced EDR que reflejan el estado de las licencias del producto es necesario conocer los términos mostrados en este apartado.



Para contratar y/o renovar licencias consulta con tu partner asignado.

Mantenimientos

Las licencias contratadas por el cliente se agrupan en mantenimientos. Un mantenimiento es un conjunto de licencias con características comunes:

- **Tipo de Producto:** Advanced EDR, Cytomic Encryption, Cytomic Patch, Advanced EDR con Cytomic Insights, Advanced EDR con Cytomic Data Watch, Advanced EDR con Cytomic Insights y Cytomic Data Watch.
- **Licencias contratadas:** número de licencias que pertenecen al mantenimiento.
- **Tipo de licencias:** NFR, Trial, Comercial, Suscripción.
- **Caducidad:** Fecha en la que las todas las licencias del mantenimiento caducan y los equipos dejarán de estar protegidos.

Estado de los equipos

Desde el punto de vista de las licencias, Advanced EDR distingue tres estados en los equipos de la red:

- **Equipos con licencia:** equipos con una licencia válida en uso asignada.
- **Equipos sin licencia:** equipos que no tienen una licencia en uso, pero que son candidatos a tenerla.
- **Excluidos:** equipos que no compiten por la obtención de una licencia. Estos equipos no están ni estarán protegidos por Advanced EDR aunque haya licencias sin asignar disponibles. Los equipos excluidos se seguirán mostrando en la consola y podrás utilizar algunas funcionalidades de gestión. Para excluir un equipo es necesario liberar su licencia de forma manual.



Es necesario distinguir entre el número de equipos sin licencia asignada (candidatos a tenerla en caso de existir licencias sin asignar) y el número de equipos excluidos (sin posibilidad de tener una licencia asignada, aunque haya licencias disponibles).

Estado de las licencias y grupos

Las licencias contratadas pueden tener dos estados:

- **Asignada:** licencia usada por un equipo de la red.
- **Sin asignar:** licencia que no está siendo usada por ningún equipo de la red.

Las licencias se agrupan por su estado en dos grupos:

- **Grupo de licencias usadas:** formado por todas las licencias asignadas a equipos.
- **Grupo de licencias sin usar:** formado por las licencias sin asignar.

Tipos de licencias

- **Licencias comerciales:** son las licencias estándar de Advanced EDR. Un equipo con una licencia comercial asignada tiene acceso a toda la funcionalidad del producto licenciado.
- **Licencias de prueba (Trial):** son licencias gratuitas de prueba, válidas por un periodo limitado de 30 días. Un equipo con una licencia de prueba asignada tiene acceso completo a la funcionalidad del producto.
- **Licencias NFR:** licencias Not For Resale, destinadas a personal interno y partners de Cytomic. No está permitida su venta ni uso por personal o partners ajenos a Cytomic.
- **Licencias de tipo suscripción:** son licencias que no tienen fecha de caducidad. El servicio es de tipo “pago por uso”.

Asignar licencias

Puedes asignar licencias de forma manual o automática.



Consulta **Gestión de equipos y dispositivos** en la página **177** para obtener más información acerca de la herramienta de búsqueda y del árbol de carpetas y árbol de filtros.

Asignación automática

Al instalar el software Advanced EDR en un equipo de la red, y siempre que existan licencias sin utilizar, el sistema le asignará de forma automática una licencia libre.

Asignación manual

Sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a asignar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.
- Haz clic en el equipo para mostrar la ventana de detalle.
- En la pestaña **Detalles**, **Licencias** se mostrará el estado **Sin licencias**. Haz clic en el icono  y se asignará de forma automática una licencia libre.

Liberar licencias

Liberar una licencia es un proceso equivalente a la asignación de licencias.

Liberación automática

- Al desinstalar el software Advanced EDR de un equipo de la red, el sistema recupera de forma automática una licencia y la devuelve al grupo de licencias sin usar.
- Al caducar un mantenimiento se liberan automáticamente licencias de los equipos siguiendo la lógica de licencias caducadas explicadas en Lógica de liberación de licencias caducadas.

Liberación manual

La liberación manual de una licencia asignada previamente a un equipo lo convierte en un equipo excluido. Aunque existan licencias libres, estas no son asignadas al equipo de forma automática.

Para liberar manualmente una licencia de Advanced EDR de un equipo de la red sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a liberar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.
- Haz clic en el equipo para mostrar su información.
- En la pestaña **Detalles**, **Licencias** se mostrará el estado del equipo. Haz clic en el icono  para liberar la licencia y devolverla al grupo de licencias sin utilizar.

Procesos asociados a la asignación de licencias

Caso I: Equipos con licencia asignada y equipos excluidos

Por defecto, a cada nuevo equipo integrado en la plataforma Cytomic se le asigna una licencia de producto Advanced EDR de forma automática, pasando a tomar el estado de **Equipo con licencia asignada**. Este proceso se repite hasta que el grupo de licencias sin usar número quede reducido a 0.

Al retirar una licencia de un equipo de forma manual, éste toma el estado de **Equipo excluido**. A partir de ese momento el equipo no competirá por la asignación de una licencia de forma automática, en el caso de existir licencias sin usar.

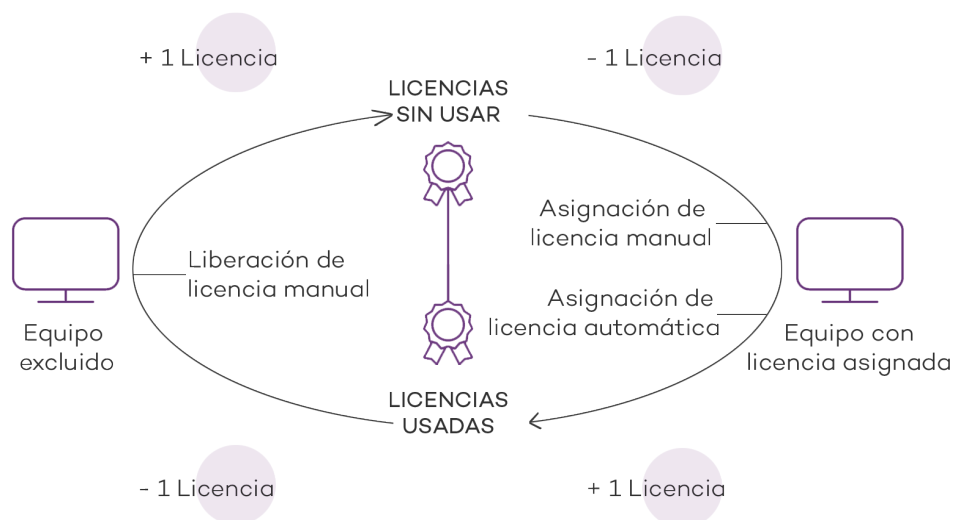


Figura 6.1: Modificación de los grupos de licencias en equipos con licencia asignada y excluidos

Caso II: Equipos sin licencia asignada

En el momento en que nuevos equipos se incorporan a la plataforma Cytomic y el grupo de licencias sin usar está a 0, los equipos pasarán al estado **Equipos sin licencia**. Cuando estén disponibles nuevas licencias, estos equipos tomarán una licencia de forma automática.

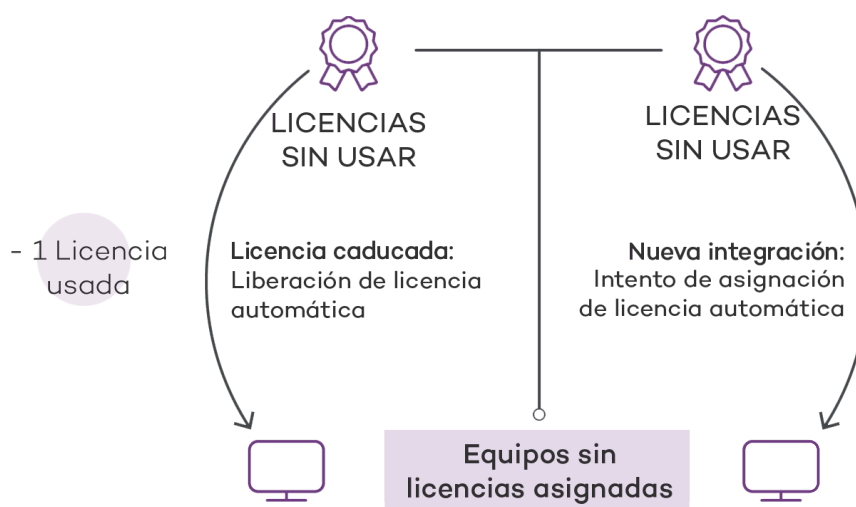


Figura 6.2: Equipos sin licencia asignada por caducar su mantenimiento y estar vacío el grupo de licencias sin usar

De la misma forma, en el momento en que una licencia asignada caduque, un equipo de la red pasará al estado **Sin licencia asignada**, siguiendo la lógica de licencias caducadas explicadas en [Lógica de liberación de licencias caducadas](#).

Paneles / widgets del módulo licencias

Acceso al panel de control

Para acceder haz clic en el menú superior **Estado**, panel lateral **Licencias**.

Permisos requeridos

No se necesitan permisos adicionales para acceder a los widgets asociados al panel de licencias.

Para visualizar el detalle de las licencias contratadas haz clic en el menú superior **Estado** y después en el menú lateral **Licencias**. Se mostrará una ventana con dos gráficas (widgets): **Licencias contratadas** y **Caducidad de licencias**.

Licencias

El panel representa cómo se distribuyen las licencias del producto contratado.

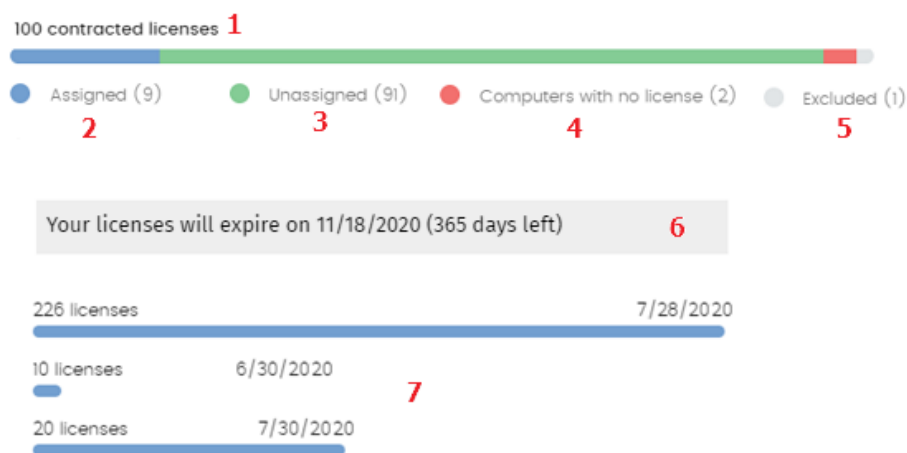


Figura 6.3: Panel de licencias mostrando tres mantenimientos

Significado de las series

Zona activa	Descripción
Número de licencias contratadas totales (1)	Número máximo de equipos que se pueden proteger, en el caso de que todas las licencias contratadas sean asignadas.
Número de licencias asignadas (2)	Número de equipos protegidos con una licencia asignada.
Número de licencias sin	Número de licencias contratadas pero que no se han asignado a ningún equipo y por lo tanto están sin utilizar.

Zona activa	Descripción
asignar (3)	
Número de equipos sin licencia (4)	Equipos no protegidos por no disponer de licencias suficientes. El sistema les asignará licencia de forma automática si se adquieren nuevas licencias.
Número de equipos excluidos (5)	Equipos sin licencia asignada que no son candidatos a tenerla.
Caducidad de las licencias (6)	Si existe un único mantenimiento contratado, todas las licencias caducarán a la vez, en la fecha indicada.
Caducidad por mantenimiento (7)	Si un mismo producto ha sido contratado varias veces a lo largo del tiempo se mostrará una gráfica de barras horizontales con las licencias asociadas a cada contrato / mantenimiento y su fecha de caducidad independiente.

Tabla 6.1: Descripción de las series de Licencias

Filtros preestablecidos desde el panel



Figura 6.4: Zonas activas del panel licencias contratadas

Se muestra el listado **Licencias** con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

Campo para filtrar	Valor
(1) Estado de licencia	Asignada
(2) Estado de licencia	Sin licencia
(3) Estado de licencia	Excluido

Tabla 6.2: Filtros del listado de licencias

Listados del módulo Licencias

Acceso al listado

El acceso a los listados se puede hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Licencias** y en el widget.

ó

- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.
- Selecciona el listado **Licencias** de la sección **General** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

El acceso al listado **Licencias** no requiere permisos adicionales para el administrador.

Licencias

Muestra en detalle el estado de las licencias de los equipos de la red e incorpora filtros que ayudan a localizar los puestos de trabajo o dispositivos móviles en función de su estado.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	•  Licencia asignada •  Equipo sin licencia •  Equipo excluido
Última conexión	Fecha del último envío del estado del equipo a la nube de Cytomic.	Fecha.

Tabla 6.3: Campos del listado Licencias

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el producto.	Cadena de caracteres
Tipo de equipo	Finalidad del equipo en la red de la organización.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Directorio Activo	Ruta dentro del árbol de Directorio Activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o está virtualizado.	Booleano
Versión del agente	Versión interna del componente agente que forma parte del software de cliente Advanced EDR.	Cadena de caracteres
Versión de la protección	Versión interna del componente protección que forma parte del software de cliente Advanced EDR.	Cadena de caracteres
Fecha de arranque del sistema	Fecha en la que el equipo se inició por última vez.	Fecha
Fecha instalación	Fecha en la que el software Advanced EDR se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha del último envío del estado del equipo a la nube de Cytomic.	Fecha

Campo	Descripción	Valores
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	• Asignada • No asignada • Excluido
Grupo	Carpeta dentro del árbol de carpetas de Cytomic a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo.	Cadena de caracteres

Tabla 6.4: Campos del fichero exportado Licencias

Herramienta de filtrado

Campo	Descripción	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Tipo de equipo	Finalidad del equipo en la red de la organización.	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Última conexión	Fecha del último envío del estado de Advanced EDR a la nube de Cytomic.	• Todos • Hace menos de 24 horas

Campo	Descripción	Valores
		• Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	• Asignada • Sin licencia • Excluido

Tabla 6.5: Campos de filtrado para el listado Licencias

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta [Información de equipo](#) en la página 218 para obtener más información.

Licencias caducadas

Excepto los mantenimientos de tipo suscripción, todos los demás tienen asignada una fecha de caducidad, pasada la cual los equipos de la red dejarán de estar protegidos.

Comportamiento de los productos basados en Cytomic al caducar sus licencias

La caducidad de los productos basados en Cytomic, tiene un impacto importante en los equipos afectados ya que:

- Se desactivan todas las protecciones configuradas en los equipos.
- Los equipos pierden el acceso a las actualizaciones del fichero de firmas y a las bases de conocimiento de la inteligencia colectiva.

- Las tareas programadas dejan de funcionar, y, por tanto, ya no es posible realizar análisis programados ni instalaciones de parches para actualizar programas vulnerables.

Por tanto, los equipos pasan a estar en una situación grave de vulnerabilidad y muy expuestos a posibles filtraciones de datos e infecciones de diferente grado de peligrosidad, desde PUPs, a ransomware o incluso amenazas avanzadas con diferentes objetivos (ATPs).

7 días de gracia

Para evitar esta situación, Cytomic ofrece un periodo de siete días de gracia durante el que se garantiza la protección total a los equipos afectados mientras se lleva a cabo la renovación de las licencias.

Comportamiento cuando caduca uno de los mantenimientos contratados

En los casos en los que el cliente tiene contratados varios mantenimientos con fechas de finalización distintas, los equipos con licencias asignadas no pertenecen a un mantenimiento concreto; en su lugar, todas las licencias de todos los mantenimientos se suman en un único grupo de licencias disponibles, que posteriormente se reparten entre los equipos de la red.

En el momento en que un mantenimiento caduca, Advanced EDR determina el número de licencias asignadas a ese mantenimiento. Acto seguido, se ordenan los equipos de la red con licencia asignada utilizando como criterio de ordenación el campo **Última conexión**, que contiene la fecha en la que el equipo se conectó por última vez a la nube de Cytomic.

Los equipos candidatos a retirar su licencia de protección son aquellos no vistos en el periodo de tiempo más alejado. Así, se establece un sistema de prioridades donde la mayor probabilidad de retirar una licencia corresponde a los equipos que no han sido utilizados recientemente.

Seleccionar qué equipos serán los que primero se queden sin licencia

Cytomic permite seleccionar previamente los equipos a los que se retirará la licencia antes de que ésta caduque.

Para ello, puedes:

- Eliminar equipos desde la consola. En las herramientas de gestión del listado de equipos, encontrarás la opción para eliminar un equipo. Consulta [Herramientas de gestión](#) en la página 206.
- Desactivar la licencia de los equipos que no quieras proteger, pero que sí quieras seguir gestionando desde la consola. Para más información, consulta [Liberación manual](#)



Ten en cuenta que si no desinstalas el agente de los equipos eliminados, el equipo se integrará automáticamente de nuevo en la consola y volverá a consumir una licencia cuando el agente contacte con el servidor Advanced EDR.

Comportamiento de Advanced EDR tras caducar todas las licencias

Desde que las licencias caducan y durante el período de gracia de 7 días (días X al X+7):

- Se dispondrá de acceso a la consola
- Las protecciones continuarán actualizadas y funcionando al 100%.

Tras el período de gracia (X+8) y durante 83 días más (días X+8 al X+90) los datos del mantenimiento se mantienen pero los equipos estarán desprotegidos. Durante este período:

- No se dispondrá de acceso a la consola
- Todas las protecciones estarán desactivadas

Renovar antes de 90 días tras caducar las licencias

Si la renovación tiene lugar antes de cumplir 90 días tras la caducidad de las licencias:

- Los equipos volverán a activar las protecciones y a actualizarse en un tiempo máximo de 4 horas desde que se renuevan las licencias, siempre y cuando el equipo se conecte a Internet.

Renovar tras más de 90 días desde la caducidad de las licencias

Transcurridos 90 días desde que caducan las licencias (desde X+90), el agente y las protecciones se desinstalarán automáticamente, y los datos del mantenimiento se eliminarán de las bases de datos de Cytomic.

Para renovar, será necesario comenzar el proceso de instalación y configuración desde cero, es decir:

- Crear los usuarios
- Reinstalar el agente y las protecciones
- Crear de nuevo las configuraciones

Mensajes de caducidad próxima y vencida

A los 30 días de vencer el mantenimiento, el panel **Licencias** contratadas mostrará un mensaje con los días que quedan para finalizar el mantenimiento y el número de licencias que se verán afectadas.

Adicionalmente, se mostrará un mensaje por cada mantenimiento caducado, indicando el número de licencias que ya no son funcionales en el plazo de los 30 últimos días.



Si todos los productos y mantenimientos están caducados se denegará el acceso a la consola de administración.

Buscar equipos según su estado de licencia

Advanced EDR incluye la categoría **Licencia** para crear filtros que ayuden a localizar los equipos de la red que tengan un determinado estado de licencia.



Consulta **Crear y organizar filtros** en la página **182** para obtener más información acerca de cómo crear un filtro en Advanced EDR.

A continuación, se muestran las propiedades de la categoría **Licencias** para crear filtros que generen listados de equipos con información relevante sobre licencias.

Categoría	Propiedad	Valor	Descripción
Licencia	Estado	Establece filtros según el estado de la licencia.	
		Asignada	Lista los equipos con una licencia Advanced EDR asignada.
		Sin asignar	Lista los equipos que no tiene una licencia Advanced EDR asignada.
		Desasignada manualmente	El administrador de la red liberó la licencia Advanced EDR previamente asignada al equipo.
		Desasignada automáticamente	El sistema liberó al equipo la licencia Advanced EDR asignada previamente.

Tabla 6.6: Campos del listado Equipos protegidos

Capítulo 7

Actualización del producto

Advanced EDR es un servicio cloud gestionado, y por lo tanto el administrador de la red no necesita ejecutar tareas de mantenimiento en la infraestructura de back-end que lo soporta. Sin embargo, sí es necesaria la actualización del software cliente instalado en los equipos de la red, así como iniciar la actualización de la consola de administración, si así lo desea.

Contenido del capítulo

Módulos actualizables en el software cliente	171
Actualización del motor de protección	172
Actualizaciones	173
Actualización del agente de comunicaciones	174
Actualizaciones del conocimiento	175
Dispositivos Windows, Linux y macOS	175
Actualización de la consola de administración	175
Consideraciones previas para actualizar la versión de la consola	175

Módulos actualizables en el software cliente

Los elementos instalados en el equipo del usuario son:

- Agente de comunicaciones Cytomic Platform.
- Motor de la protección Advanced EDR.
- Archivo de identificadores / fichero de firmas.

Dependiendo de la plataforma a actualizar, el procedimiento y las posibilidades de configuración varían tal y como se indica en **Formas de actualización según el componente del software cliente**.

Módulo	Plataforma		
	Windows	macOS	Linux
Agente Cytomic	Bajo demanda		
Protección Advanced EDR	Configurable	Configurable	Configurable
Archivo de identificadores	Habilitar / Deshabilitar	Habilitar / Deshabilitar	Habilitar / Deshabilitar

Tabla 7.1: Formas de actualización según el componente del software cliente

- **Bajo demanda:** el administrador puede iniciar la actualización una vez que esté disponible, o retrasarla hasta el momento que considere oportuno.
- **Configurable:** el administrador podrá definir en la consola web ventanas de actualización recurrentes y en el futuro, siendo posible además desactivar la actualización.
- **Habilitar / Deshabilitar:** El administrador puede desactivar la actualización. Si la actualización está activada ésta se producirá automáticamente cuando esté disponible.
- **No:** El administrador no puede influir en el proceso de actualización. Las actualizaciones se efectuarán cuando estén disponibles y no es posible deshabilitarlas.

Actualización del motor de protección

Para configurar la actualización del motor de protección crea y asigna un perfil de configuración de tipo **Ajustes por equipo**, accesible desde el menú superior **Configuración**, en el panel de la izquierda de la consola de administración.

Limitación de la descarga de actualizaciones del motor a través de equipos caché y Proxy Cytomic

La descarga de las actualizaciones del motor de protección puede realizarse directamente desde Internet o también a través de un equipo caché o Proxy Cytomic. Consulta [Configuración de las descargas mediante equipos caché](#) en la página 279 y [Configuración de listas de acceso a través de proxy](#) en la página 277.

Según el sistema operativo instalado en el equipo, pueden existir ciertas limitaciones a la hora de utilizar un método de descarga u otro:

- **Equipos con sistema operativo Windows o macOS:** pueden descargar instaladores a través de equipos caché, proxy e Internet.

- **Equipos con sistema operativo Linux:** al utilizar el gestor de paquetes propio de la distribución para hacer las descargas, no pueden descargar instaladores a través de equipos caché ni proxy de Advanced EDR.

Los equipos caché almacenan los instaladores hasta que dejan de ser válidos, momento en el que se eliminarán.

Actualizaciones

Para habilitar la actualización automática del módulo de protección Advanced EDR haz clic en el botón de activación **Actualizar automáticamente Advanced EDR en los dispositivos**. Esta acción habilitará el resto de configuraciones de la página. Si esta opción está deshabilitada, el módulo de protección no se actualizará nunca.



Se desaconseja totalmente deshabilitar la actualización del motor de protección. Los equipos con la protección sin actualizar serán más vulnerables en el medio plazo frente a las amenazas avanzadas y el malware.

Aplicar actualizaciones en rangos de horas

Indica los siguientes parámetros para que los equipos apliquen las actualizaciones disponibles dentro de un rango de horas concreto:

- Hora de inicio
- Hora de fin

Para aplicar las actualizaciones en cualquier momento haz clic en la casilla de selección **A cualquier hora**.

Aplicar actualizaciones en fechas determinadas

Utiliza el desplegable para indicar las fechas en las que se aplicará la actualización:

- **En cualquier fecha:** las actualizaciones se aplicarán el día que estén disponibles. Esta opción no limita la actualización de Advanced EDR a fechas concretas.
- **Los siguientes días de la semana:** utiliza las casillas de selección para establecer los días de la semana en los que Advanced EDR se actualizará. La actualización se producirá el primer día de la semana que coincida con la selección del administrador en caso de haber una actualización disponible.
- **Los siguientes días del mes:** utiliza los desplegables para establecer un rango de días hábiles dentro del mes en los que Advanced EDR se actualizará. La actualización se producirá el primer día del mes que coincida con los seleccionados por el administrador en caso de haber una actualización disponible.

- **Los siguientes días:** utiliza los desplegables para establecer un rango de días hábiles dentro del calendario en los que Advanced EDR se actualizará. Los rangos definidos en esta opción se establecen de forma absoluta para casos en que el administrador quiera establecer rangos que no se repiten en el tiempo. De esta forma, se permite definir rangos de fechas concretas de actualización, pasadas las cuales dejan de tener efecto. Este método requiere redefinir los rangos de actualización de forma constante una vez hayan vencido.

Reinicio de equipos

Advanced EDR permite definir la lógica de reinicios en caso de que sea necesario, mediante el desplegable situado al final de la pantalla de configuración:

- **No reiniciar automáticamente:** se mostrará al usuario una ventana en intervalos de tiempo cada vez más cortos, aconsejando el reinicio de la máquina para aplicar la actualización.
- **Reiniciar automáticamente sólo las estaciones de trabajo.**
- **Reiniciar automáticamente sólo los servidores.**
- **Reiniciar automáticamente tanto estaciones de trabajo como servidores.**

Actualización del agente de comunicaciones

La actualización del agente Cytomic se ejecuta bajo demanda. Advanced EDR incluirá una notificación en la consola de administración indicando la existencia de una nueva versión del agente, y el administrador podrá lanzar la actualización cuando lo desee.

La actualización del agente Cytomic no requiere reinicio del equipo del usuario y suele implicar cambios y mejoras en la consola de administración que facilitan la gestión de la seguridad.

Limitación de la descarga de actualizaciones del agente de comunicaciones a través de equipos caché y Proxy Cytomic

La descarga de las actualizaciones del agente de comunicaciones puede realizarse directamente desde Internet o también a través de un equipo caché o Proxy Cytomic. Consulta [Configuración de las descargas mediante equipos caché](#) en la página 279 y [Configuración de listas de acceso a través de proxy](#) en la página 277.

Según el sistema operativo instalado en el equipo, pueden existir ciertas limitaciones a la hora de utilizar un método de descarga u otro:

- **Equipos con sistema operativo Windows o macOS:** pueden descargar instaladores a través de equipos caché, proxy e Internet.
- **Equipos con sistema operativo Linux:** al utilizar el gestor de paquetes propio de la distribución para hacer las descargas no pueden descargar instaladores a través de equipos caché ni Proxy Cytomic .

Los equipos caché almacenan los instaladores hasta que dejan de ser válidos, momento en el que se eliminarán.

Actualizaciones del conocimiento

La configuración de la actualización del fichero de firmas en Advanced EDR se realiza en el perfil de configuración de seguridad asignado al equipo, según sea su tipo.

Descarga del conocimiento a través de equipos caché y Proxy Cytomic

Los sistemas operativos Windows, Linux y macOS pueden descargar el conocimiento directamente desde Internet, así como desde equipos con el rol de Proxy Cytomic o caché asignado.

Los equipos caché almacenan los ficheros de firmas hasta que dejan de ser válidos, momento en el que se eliminarán.

Dispositivos Windows, Linux y macOS

La configuración se realiza en los perfiles de tipo **Estaciones y Servidores**, accesibles desde el panel de la izquierda en el menú superior **Configuración**.

En la pestaña **General** las opciones disponibles son:

- **Actualizaciones automáticas de conocimiento:** habilita o deshabilita la descarga del fichero de firmas. Si se deshabilita el fichero de firmas nunca será actualizado.



Se desaconseja totalmente deshabilitar la actualización del conocimiento. Los equipos con la protección sin actualizar serán más vulnerables en el corto plazo frente a las amenazas avanzadas y el malware.

Actualización de la consola de administración

El administrador de la red puede indicar el momento en el que iniciar el proceso para actualizar la versión de la consola en los servidores de Cytomic. En caso contrario, Cytomic actualizará de forma automática la consola de administración a la última versión disponible.

Para realizar este proceso, es necesario que la cuenta de usuario que accede a la consola web tenga asignado el rol de Control total. Consulta [El rol Control total](#) en la página 68.

Consideraciones previas para actualizar la versión de la consola

Aunque se trata de un proceso que se produce íntegramente en los servidores de Cytomic, el cambio de versión de la consola puede acarrear la disponibilidad de nuevas versiones del software de seguridad instalado en los equipos del cliente. Esto puede generar un consumo de tráfico y la necesidad de reiniciar los equipos en algunos casos. Para mitigar el consumo de tráfico en las actualizaciones, consulta [Configuración de las descargas mediante equipos caché](#) en la página 279.

La actualización de la consola es transparente para el administrador y no verá interrumpido su funcionamiento. Cuando el proceso se completa, la consola se cierra automáticamente. Al iniciar de nuevo la sesión, el administrador accederá a la consola actualizada.

Iniciar la actualización de la consola de administración

- Haz clic en icono **Notificaciones web**  situado en la parte derecha del menú superior. Se desplegarán las notificaciones pendientes de leer.
- Si hay una actualización de la consola disponible, se muestra el mensaje **Nueva versión de la consola de Administración** con el enlace **Nuevas características y mejoras**, la versión de la consola a la que se actualizará, y el botón **Actualizar la consola ahora**. Este tipo de notificación no se puede eliminar ya que no tiene el icono  asociado. Consulta **Icono Notificaciones web** en la página 39.



*El botón **Actualizar la consola ahora** solo se muestra si la cuenta de usuario utilizada para acceder a la consola de administración tiene asignado el rol Control total. En caso de no tener el nivel de permisos requeridos, este botón no se mostrará.*

- Al hacer clic en el botón, la petición de actualización entra en la cola del servidor para ser procesada. El tiempo de permanencia máximo de la petición en la cola del servidor son 10 minutos.
- Una vez procesada la petición, se inicia el proceso de actualización y la notificación muestra el texto **Actualización en curso**. Si alguna cuenta de usuario inicia la sesión en la consola será expulsada, y mientras dure el proceso de actualización no será posible iniciar sesión en la consola de administración.
- Al cabo de un tiempo que depende del número de equipos administrados y de los datos almacenados en la consola, se finalizará el proceso de actualización a la nueva versión.

Cancelar la actualización

- Una vez iniciado el proceso de actualización, haz clic en el icono **Notificaciones web**  situado en la parte derecha del menú superior. Se desplegarán las notificaciones pendientes de leer.
- Si hay una actualización de la consola en la cola de peticiones pero que todavía no se ha iniciado, se muestra el mensaje **Nueva versión de la consola de Administración** con el enlace **Nuevas características y mejoras** y el botón **Cancelar la actualización**.
- Para eliminar de la cola la petición de actualización, haz clic en el botón **Cancelar la actualización**. El botón desaparecerá y se mostrará nuevamente el botón **Actualizar la consola ahora**.

Capítulo 8

Gestión de equipos y dispositivos

La consola web muestra los dispositivos administrados de forma ordenada y flexible, aplicando distintas estrategias que permiten localizarlos rápidamente para facilitar su gestión.

Para que un equipo de la red sea gestionable por Advanced EDR se requiere como mínimo de la instalación del agente Cytomic en el equipo. Los equipos sin licencia pero con el agente Cytomic instalado, aparecerán en la consola de administración, aunque su protección estará desactualizada y no podrán ejecutar tareas, análisis ni otras acciones vinculadas con el servicio de protección.

Contenido del capítulo

La zona equipos	178
El panel Árbol de equipos	179
Árbol de filtros	180
Definición de filtro	180
Filtros predefinidos	180
Crear y organizar filtros	182
Configurar filtros	184
Casos de uso comunes	185
Árbol de grupos	188
Crear y organizar grupos	190
Mover equipos entre grupos	192
Filtrar resultados por grupos	193
Filtrar grupos	194
Listados disponibles para gestionar equipos	194
Listado de equipos	194
El panel Mis listados	208
Información de equipo	218

Sección general (1)	219
Sección alertas de equipo (2)	220
Sección Detalles (3)	230
Sección Detecciones (4) en Windows, Linux y macOS	238
Sección Investigación (5)	238
Conexiones monitorizadas (6)	243
Sección Hardware (7)	244
Sección Software (8)	245
Sección Configuración (9)	247
Barra de acciones (10)	247
Iconos ocultos (11)	249

La zona equipos

La zona **Equipos** es el área de la consola web donde se gestionan los dispositivos integrados en Advanced EDR.

Para acceder a la ventana de administración de equipos, haz clic en el menú superior **Equipos**. Se mostrarán dos zonas diferenciadas: el panel lateral con el **Árbol de equipos (1)** y el panel central con el **Listado de equipos (2)**. Ambos paneles trabajan de forma conjunta: al seleccionar una rama del árbol de equipos, el listado de equipos se actualiza con todos sus equipos asignados.

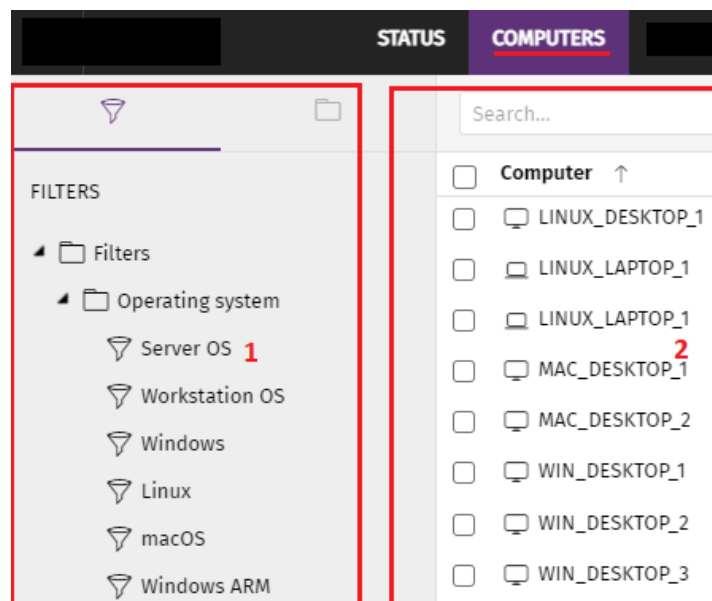


Figura 8.1: Vista general de los paneles en la zona Equipos

Mostrar equipos en subgrupos

Para ampliar o limitar el listado de los equipos activa o desactiva la opción **Mostrar equipos de los subgrupos** disponible en el menú de contexto general.

- Si la opción está activada, al seleccionar una rama del árbol se mostrarán todos los equipos que pertenecen a ella y a todas las ramas de orden inferior.
- Si la opción está desactivada, al seleccionar una rama del árbol se mostrarán únicamente todos los equipos que pertenecen a ella.

El panel Árbol de equipos

Advanced EDR representa la estructura de equipos mediante el **Árbol de equipos (1)**, que presenta dos vistas o árboles independientes **(2)**:

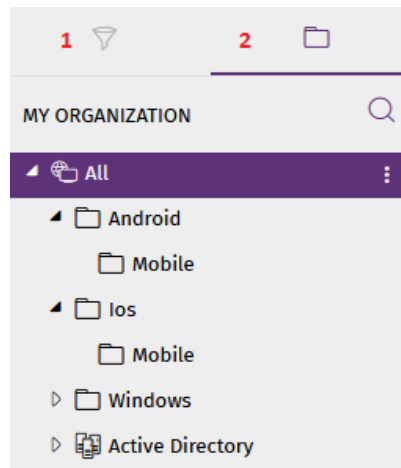


Figura 8.2: El panel Árbol de equipos

- **Árbol de filtros (1)**: gestiona los equipos de la red mediante agrupaciones dinámicas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma automática.
- **Árbol de grupos (2)**: gestiona los equipos de la red mediante agrupaciones estáticas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma manual.

Los dos árboles muestran el parque de dispositivos del cliente de distintas formas, con el objeto de favorecer la ejecución de tareas de diferentes tipos, tales como:

- Localizar los equipos que cumplan con características determinadas, relativas al hardware, software o a la seguridad.
- Asignar perfiles de configuración de seguridad de forma rápida.
- Ejecutar acciones de resolución sobre grupos de equipos.



*Para localizar equipos desprotegidos o de características determinadas relativas a la seguridad o al estado de la protección consulta **Visibilidad del malware y del parque informático** en la página 607. Para asignar perfiles de configuración de seguridad consulta **Asignación manual y automática de configuraciones** en la página 261. Para ejecutar tareas de resolución de problemas consulta **Herramientas de resolución** en la página 797.*

Al pasar el puntero del ratón por las ramas del árbol de filtros y de grupos se muestra el icono de menú de contexto. Haz clic para desplegar un menú emergente con todas las operaciones disponibles sobre la rama del árbol seleccionada.

Árbol de filtros

Es una de las dos vistas del Árbol de equipos, y permite agrupar de forma dinámica los equipos en la red mediante reglas y condiciones que describen características de los dispositivos. Estas reglas se pueden combinar mediante operaciones lógicas para producir expresiones complejas.

Para acceder al Árbol de filtros haz clic en el icono del filtro  desde el panel de la izquierda. Al hacer clic en los diferentes elementos del árbol, el panel de la derecha se actualiza, presentando todos los equipos que cumplen con los criterios establecidos en el filtro seleccionado.

Definición de filtro

Son agrupaciones dinámicas de equipos. La pertenencia de un equipo a un filtro se determina de forma automática cuando el equipo en cuestión cumple con las condiciones de pertenencia al filtro que haya configurado el administrador.



Un equipo puede pertenecer a más de un filtro.

Un filtro está constituido por un conjunto de reglas o condiciones que los equipos tendrán que satisfacer para pertenecer a aquél. En la medida en que el equipo cumpla con las características descritas formará parte del filtro; de la misma forma, cuando un equipo cambie su estado y no cumpla los criterios de pertenencia, automáticamente dejará de formar parte de la agrupación descrita por el filtro.

Los filtros se pueden ordenar de forma manual agrupándolos en carpetas, con el criterio que el administrador considere oportuno.

Filtros predefinidos

Advanced EDR incorpora filtros de uso muy común que el administrador puede utilizar desde el primer momento para ordenar y localizar equipos en la red. Los filtros predeterminados se pueden modificar o

borrar.



No es posible recuperar un filtro predeterminado que haya sido borrado.

Nombre	Grupo	Descripción
SO de servidores	Sistema operativo	Lista los equipos con un sistema operativo de tipo Servidor instalado.
SO de estaciones	Sistema operativo	Lista los equipos con un Sistema operativo de tipo estación de trabajo.
Windows	Sistema operativo	Lista todos los equipos con sistema operativo Windows instalado.
Linux	Sistema operativo	Lista todos los equipos con sistema operativo Linux instalado.
macOS	Sistema operativo	Lista todos los equipos con sistema operativo macOS instalado.
Windows ARM	Sistema operativo	Lista todos los equipos con sistema operativo Windows y microprocesador ARM.
Estaciones y servidores	Tipo de sistema	Lista los equipos físicos de sobremesa o servidores.
Portátiles	Tipo de sistema	Lista los equipos físicos portátiles.
Móviles y tablets	Tipo de sistema	Lista los dispositivos de tipo smartphone y tablet.
Virtuales	Tipo de sistema	Lista los equipos virtualizados.
< 2GB de memoria	Hardware	Lista los equipos con una memoria menor que 2 GByte

Nombre	Grupo	Descripción
Java	Software	Lista todos los equipos que tiene instalado el SDK JRE Java.
Adobe Acrobat Reader	Software	Lista todos los equipos que tiene instalado el software Acrobat Reader.
Adobe Flash Player	Software	Lista todos los equipos que tiene instalado el plugin de reproducción Flash.
Google Chrome	Software	Lista todos los equipos que tiene instalado el navegador Chrome.
Mozilla Firefox	Software	Lista todos los equipos que tiene instalado el navegador Firefox.

Tabla 8.1: Listado de filtros predefinidos

Crear y organizar filtros

Para crear y organizar filtros haz clic en el icono de menú de contexto de las ramas del árbol de filtros. Se mostrará un menú emergente con las opciones permitidas en esa rama en particular.

Crear carpetas

- Haz clic en el menú de contexto de la rama donde quieres crear la carpeta y haz clic en **Añadir carpeta**.
- Introduce el nombre de la carpeta y haz clic en **Aceptar**.



Una carpeta no puede depender de un filtro. Si seleccionas un filtro antes de crear la carpeta, ésta se creará al mismo nivel que el filtro, compartiendo su carpeta padre.

Crear filtros

Para crear un filtro es necesario seguir los pasos mostrados a continuación:

- Selecciona el menú de contexto de la carpeta en el árbol donde será creado el filtro.
 - Si deseas crear una estructura jerárquica de filtros, crea carpetas contenedoras y mueve los filtros dentro de ellas. Una carpeta puede contener otras carpetas con filtros.
- Haz clic en **Añadir filtro**.

- Introduce el nombre del filtro. No es necesario que sea un nombre único. El resto de la configuración se detalla en [Configurar filtros](#).

Borrar filtros y carpetas

Para borrar un filtro o una carpeta haz clic en el menú de contexto de la rama a borrar y elige la opción **Eliminar**. La rama se borrará junto a todos sus descendientes.



No se permite borrar el nodo raíz Filtros.

Mover y copiar filtros y carpetas

- Haz clic en el menú de contexto de la rama a copiar o mover.
- Haz clic en **Mover** o **Hacer una copia**. Se mostrará una ventana emergente con el árbol de filtros de destino.
- Selecciona la carpeta de destino y pulsa **Aceptar**.



No es posible copiar carpetas de filtros. Únicamente se permite la copia de filtros.

Renombrar filtros y carpetas

- Haz clic en el menú de contexto de la rama a renombrar.
- Haz clic en **Renombrar**.
- Introduce el nuevo nombre.



No es posible renombrar la carpeta raíz. Para renombrar un filtro es necesario editarlo.

Buscar filtros

En infraestructuras IT muy grandes, el árbol de filtros puede contener un gran número de elementos, lo que dificulta la localización de un determinado filtro.

Para localizar un filtro, sigue los siguientes pasos:

- Haz clic en el icono  situado en la parte superior del árbol de filtros. Se mostrará una caja de texto debajo.

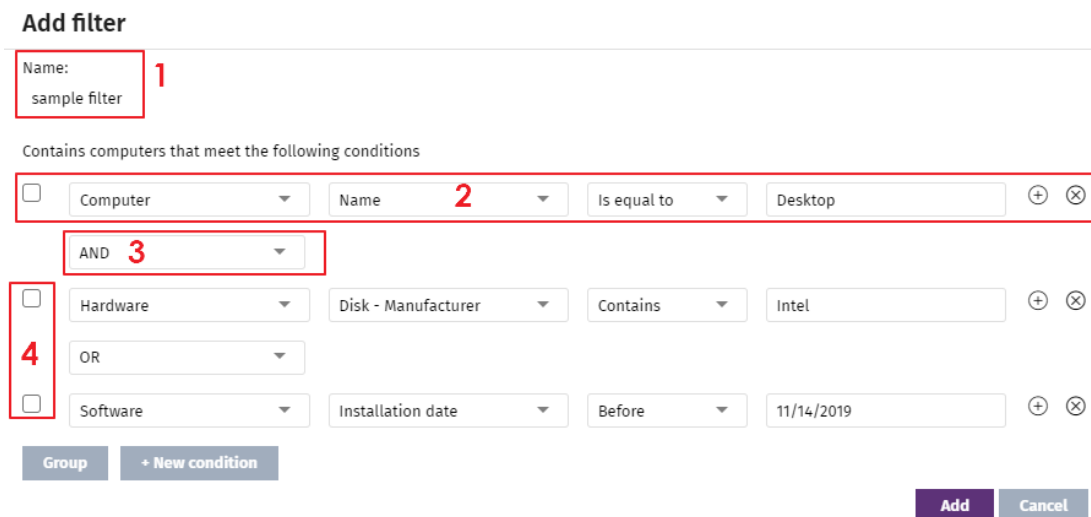
- Escribe las letras que forman parte del nombre del filtro que quieres buscar. Se mostrarán los filtros que comiencen, terminen o contengan la cadena de caracteres indicada.
- Una vez realizada la búsqueda, selecciona el filtro de tu interés y haz clic en el icono . Se volverá a mostrar el árbol de filtros completo pero conservando la selección sobre el filtro que has buscado.

Configurar filtros

Haz clic en el menú de contexto del filtro y elige la entrada **Editar filtro** del menú. Se mostrará la ventana de configuración de filtros.

Un filtro está formado por una o más reglas, relacionados entre sí mediante operadores lógicos Y / O. Un equipo formará parte de un filtro si cumple con los valores especificados en las reglas del filtro.

El esquema general de un filtro se compone de cuatro bloques:



Add filter

Name: sample filter **1**

Contains computers that meet the following conditions

☐ Computer **2** Name Is equal to Desktop + -

AND **3**

☐ Hardware ☐ Software **4**

Hardware Disk - Manufacturer Contains Intel + -

OR

Software Installation date Before 11/14/2019 + -

Group + New condition

Add Cancel

Figura 8.3: Vista general de configuración de un filtro

- **Nombre del filtro (1):** identifica al filtro.
- **Reglas de filtrado (2):** construye condiciones indivisibles de pertenencia al filtro. Una regla de filtrado únicamente comprueba una característica concreta de los equipos de la red.
- **Operadores lógicos (3):** combina dos reglas de filtrado mediante los operadores lógicos Y o O.
- **Agrupaciones (4):** varían el orden de evaluación de las reglas de filtrado configuradas y relacionadas mediante operadores lógicos.

Reglas de filtrado

Una regla de filtrado se compone de los elementos mostrados a continuación:

- **Categoría:** agrupa las propiedades en secciones para facilitar su localización.
- **Propiedad:** característica del equipo que se evaluará para determinar su pertenencia al filtro.

- **Operador:** establece el modo de comparación del contenido de la propiedad del equipo con el valor de referencia que establezca el administrador para el filtro.
- **Valor:** contenido de la propiedad. Dependiendo del tipo de propiedad el campo valor cambiará para ajustarse a entradas de tipo fecha, literales etc.

Para añadir reglas de filtrado a un filtro haz clic en el icono  y para borrarlas en el icono .

Operadores lógicos

Para combinar dos reglas en un mismo filtro se utilizan los operadores lógicos Y y O. Al añadir una segunda regla y sucesivas a un filtro se mostrará de forma automática un desplegable con los operadores lógicos disponibles, que se aplicarán a las reglas adyacentes.

Agrupaciones de reglas de filtrado

Los paréntesis en una expresión lógica se utilizan para variar el orden de evaluación de los operadores que relacionan las reglas de filtrado introducidas.

Para encerrar dos o más reglas en un paréntesis crea una agrupación marcando con las casillas de selección las reglas que formarán parte del grupo y haz clic en el botón **Agrupación**. Se mostrará una línea delgada que abarcará las reglas de filtrado que forman parte de la agrupación.

Mediante el uso de paréntesis se definen agrupaciones de varios niveles para poder anidar grupos de operandos en una expresión lógica.

Casos de uso comunes

A continuación se indican, a modo de ejemplo, algunos casos de uso de filtros muy utilizados por los administradores de redes:

Equipos Windows según el procesador instalado (x86, x64, ARM64)

Lista los equipos que tienen instalado el sistema operativo Windows y su microprocesador pertenece a la familia ARM.

Este filtro se compone de dos condiciones unidas mediante el operador Y:

- **Condición 1:**
 - **Categoría:** Equipo
 - **Propiedad:** Plataforma
 - **Condición:** Es igual a
 - **Valor:** Windows
- **Condición 2:**
 - **Categoría:** Equipo
 - **Propiedad:** Arquitectura

- **Condición:** Es igual a
- **Valor:** {nombre de la arquitectura: ARM64, x86, x64}

Equipos sin parches instalados

Lista los equipos que no tienen un determinado parche instalado. Para obtener más información sobre Cytomic Patch, consulta [Cytomic Patch \(Actualización de programas vulnerables\)](#) en la página 375.

- **Categoría:** Programas
- **Propiedad:** Nombre del software
- **Condición:** No contiene
- **Valor:** {Nombre del parche}

Equipos sin conectar con la nube de Cytomic en X días

Lista los equipos que no conectaron con la nube de Cytomic en el intervalo configurado:

- **Categoría:** Equipo
- **Propiedad:** Última conexión
- **Condición:** Antes de
- **Valor:** {Fecha en formato dd/mm/aa}

Equipos que no conectan con los servicios de inteligencia de seguridad de Cytomic

Localiza todos los equipos que muestran problemas de conexión con alguno de los servicios de inteligencia de seguridad de Cytomic. Crea las reglas siguientes relacionadas con el operador O:

- **Regla:**
 - **Categoría:** Seguridad
 - **Propiedad:** Conexión para envío de eventos
 - **Condición:** Es igual a
 - **Valor:** Con problemas
- **Regla:**
 - **Categoría:** Seguridad
 - **Propiedad:** Conexión para inteligencia colectiva
 - **Condición:** Es igual a
 - **Valor:** Con problemas

Equipos aislados

Lista los equipos que han sido aislados de la red. Para más información, consulta [Aislar un equipo](#) en la página **804**.

- **Categoría:** Equipo
- **Propiedad:** Estado de aislamiento
- **Condición:** Es igual
- **Valor:** Aislado

Equipos en modo Contención de ataque RDP

Lista los equipos que han recibido un volumen alto de intentos de conexión por RDP, razón por la que Advanced EDR ha comenzado a bloquearlos.

- **Categoría:** Equipo
- **Propiedad:** Modo “Contención de ataque por RDP”
- **Condición:** Es igual
- **Valor:** Verdadero

Integración con otras herramientas de gestión

Muestra los equipos que coinciden con alguno de los nombres de equipo especificados en un listado obtenido por una herramienta de terceros. Cada línea del listado deberá terminar con un retorno de carro y será considerada como un nombre de equipo.

- **Categoría:** Equipo
- **Propiedad:** Nombre
- **Condición:** En
- **Valor:** listado de nombres de equipo

Equipos no compatibles con firma de drivers SHA-256

- **Categoría:** Equipo
- **Propiedad:** Soporta drivers con firma SHA-256
- **Condición:** Es igual a
- **Valor:** Falso

Equipos con IP pública

Busca los equipos que accedieron a Internet a través de un dispositivo (router / proxy / extremo VPN) con la IP indicada.

- **Categoría:** Equipo
- **Propiedad:** Dirección IP pública
- **Condición:** Es igual a (Para buscar los equipos que acceden a Internet a través de un dispositivo que tiene una IP concreta)

Equipos descubiertos en directorio activo

Busca los equipos administrados y no administrados que han sido descubiertos mediante el método de descubrimiento en directorios activos.

- **Categoría:** Equipo
- **Propiedad:** Última vez visto en directorio activo
- **Condición:** Está entre (para buscar los equipos descubiertos entre fechas concretas)

Árbol de grupos

El árbol de grupos reúne de forma estática los equipos en la red en las agrupaciones definidas por el administrador.

Para acceder al árbol de grupos:

- Haz clic en el icono de carpeta  en el panel lateral.
- Al hacer clic en las diferentes ramas del árbol, el panel de la derecha se actualiza, presentando todos los equipos que contienen el grupo seleccionado y sus subgrupos.

Definición de grupo

Es un contenedor de equipos asignados de forma manual por el administrador. El árbol de grupos admite crear una estructura de n niveles compuesta por grupos, subgrupos y equipos.



El máximo nivel de profundidad del árbol es 10.

Tipos de grupos

Tipo de grupo	Descripción
Grupo raíz 	Grupo padre del que cuelgan el resto de carpetas.
Grupos nativos 	Grupos estándar de Advanced EDR que soportan todas las operaciones (movimiento, renombrado, borrado etc.) Pueden contener otros grupos nativos y equipos.

Tipo de grupo	Descripción
Grupos IP 	Grupo nativo con IPs o rangos de IPs asociados para acelerar la integración de nuevos equipos en el servicio de seguridad.
Grupos Directorio Activo 	Replican la estructura del Directorio Activo instalado en la empresa, por esta razón tienen limitadas algunas operaciones. Pueden contener otros grupos de Directorio Activo y equipos.
Grupo raíz del directorio activo 	Abarca todos los dominios del Directorio Activo configurados en la red de la organización. Contiene grupos de dominio Directorio Activo.
Grupo de dominio Active Directory 	Ramas del Directorio Activo que representan dominios. Contienen otros grupos de dominio Directorio Activo, grupos Directorio Activo y equipos.

Tabla 8.2: Tipos de grupos en Advanced EDR

El tamaño de la organización, lo homogéneos que sean los equipos gestionados y la presencia o no de un servidor de Directorio Activo en la red de la empresa determinará la estructura del árbol de grupos. La estructura de grupos podrá variar desde un árbol plano de un único nivel para los casos más sencillos, hasta una estructura compleja con varios niveles, para redes grandes formadas por equipos muy heterogéneos.



En un momento determinado un equipo solo puede pertenecer a un grupo, a diferencia de los filtros donde un equipo puede pertenecer a varios simultáneamente.

Grupos de Directorio Activo

Para las organizaciones que tienen instalado un servidor de Directorio Activo en la red, Advanced EDR puede obtener de forma automática la estructura configurada y replicarla en el árbol de grupos: los agentes Cytomic reportan a la consola Web el grupo del Directorio Activo al que pertenecen y, conforme se despliegan los agentes en los equipos, el árbol se completará con las distintas unidades organizativas. De esta manera, bajo la rama  se presentará una distribución de los equipos familiar para el administrador, con el objeto de acelerar la localización de dispositivos y su gestión.

Para mantener la coherencia entre el Directorio activo de la empresa y el árbol representado en la consola de administración, los grupos de directorio activo no son modificables desde la consola de Advanced EDR: únicamente cambiarán cuando lo haga la estructura de Directorio Activo de la empresa. Los cambios se replicarán en la consola Web de Advanced EDR transcurrido un máximo de una hora.

Si el administrador de la red mueve en la consola de Advanced EDR un equipo que reside en un grupo de tipo Directorio Activo a un grupo nativo o al grupo raíz se romperá la sincronización con el Directorio Activo de la empresa. Cualquier cambio de grupo en el Directorio Activo de la empresa que afecte a ese equipo no se replicará en la consola de Advanced EDR.

Para restablecer la sincronización de un equipo y así continuar replicando la estructura original del Directorio Activo de la empresa en la consola de Advanced EDR consulta [Restaurar la pertenencia de varios equipos a su grupo Active Directory](#).

Crear y organizar grupos

Para acceder a las operaciones disponibles sobre grupos haz clic en el icono de menú de contexto de las ramas del árbol de grupos. Se mostrará un menú emergente con las opciones permitidas para esa rama en particular.

Crear grupos

- Selecciona el menú de contexto del grupo padre del cual dependerá el grupo a crear, y haz clic en **Añadir grupo**.
- Introduce el nombre del grupo en la caja de texto **Nombre** y haz clic en el botón **Añadir**.



No es posible crear grupos de Directorio Activo en el árbol de grupos. Solo se replicarán los grupos y unidades organizativas creadas en el servidor de Directorio Activo de la empresa.

Si deseas que los equipos sobre los cuales se va a instalar un agente Advanced EDR se muevan a un determinado grupo según su IP sigue los pasos mostrados a continuación:

- Haz clic en el enlace **Añadir reglas de asignación automática por IPs**, se mostrará una caja de texto donde añadir las IPs de los equipos que serán movidos al grupo.
- Especifica IPs individuales separadas por comas o rangos de IPs separados por un guion.

El movimiento del equipo se efectuará únicamente en el momento de la instalación del agente Advanced EDR. Si posteriormente el equipo cambia de IP éste permanecerá en el grupo asignado inicialmente.

Borrar grupos

Selecciona el menú de contexto del grupo a borrar. Si el grupo contiene subgrupos o equipos asignados, la consola de administración mostrará un error.



No se permite borrar el nodo raíz Todos.

Para borrar los grupos vacíos de tipo Directorio Activo que cuelgan de uno dado, haz clic en el menú de contexto del grupo y selecciona **Eliminar grupos vacíos**.

Mover grupos

- Selecciona el menú de contexto del grupo a mover.
- Haz clic en **Mover**. Se mostrará una ventana emergente con el árbol de grupos de destino.
- Selecciona el grupo de destino y pulsa **Aceptar**.



No se permite el movimiento del nodo raíz Todos ni de grupos Directorio Activo.

Renombrar grupos

- Selecciona el menú de contexto del grupo a renombrar.
- Haz clic en **Cambiar nombre**.
- Introduce el nuevo nombre.



No es posible renombrar el grupo raíz Todos ni grupos Directorio Activo.

Importar reglas de asignación por IPs en grupos ya creados

Para añadir direcciones IP a un grupo nativo ya creado sigue los pasos mostrados a continuación:

- Selecciona el menú de contexto de un grupo nativo que no sea el grupo Todos y haz clic en la opción **Importar reglas de asignación por IPs**. Se mostrará una ventana para poder arrastrar un fichero con las direcciones IP.
- El fichero deberá contener una o más líneas de texto con el formato mostrado a continuación:
 - Para direcciones IP independientes añadir una línea por cada una de ellas a asignar:
 - `.\Grupo\Grupo\Grupo (tabulación) IP`
 - Para rangos de IPs, añadir una línea por cada rango a asignar:
 - `.\Grupo\Grupo\Grupo (tabulación) ExtremoInferiorIP-ExtremoSuperiorIP`
- Todas las rutas indicadas son interpretadas por Advanced EDR como relativas a la rama del árbol seleccionada.
- Si los grupos indicados en el fichero no existieran, Advanced EDR los creará y asignará la direcciones IP indicadas.

- Haz clic en **Importar**. Las IPs se asignarán a los grupos indicados en el fichero y el árbol de grupos actualizará sus iconos para mostrar el cambio de tipo de grupo.



Las direcciones IP previamente asignadas a un grupo IP se borrarán al importar un fichero con nuevos pares grupo - IP.

Una vez terminado el procedimiento, todos los equipos nuevos que se integren en Advanced EDR se moverán al grupo indicado según su dirección IP.

Exportar reglas de asignación por IPs

Para exportar un fichero con las reglas de grupos IP ya asignadas sigue los pasos mostrados a continuación:

- Selecciona el menú de contexto de un grupo IP, y haz clic en la opción **Exportar reglas de asignación por IPs**. Se descargará un fichero .csv con las reglas de asignación de IPs establecidas en el grupo IP y en todos sus descendientes.
- El formato del fichero .csv es el indicado en el punto **Importar reglas de asignación por IPs en grupos ya creados**.

Mover equipos entre grupos

Para mover uno o varios equipos a un grupo, el administrador puede seguir varias estrategias:

Mover conjuntos de equipos a grupos

- Selecciona el grupo **Todos** para listar todos los equipos administrados o utiliza la herramienta de búsqueda para localizar los equipos a mover.
- Selecciona con las casillas los equipos en el panel de listado de equipos.
- Haz clic en el icono  situado a la derecha de la barra de búsqueda. Se mostrará un menú desplegable con la opción **Mover a**. Haz clic para mostrar el árbol de grupos destino.
- Selecciona el grupo destino del árbol de grupos mostrado.

Mover un único equipo a un grupo

Para asignar un único equipo a un grupo se pueden seguir varias estrategias:

- Seguir el método mostrado más arriba para asignar conjuntos de equipos a grupos, pero seleccionando un único equipo.
- Seleccionar con la casilla el equipo dentro del panel de listado de equipos que quieras asignar y haz clic en el icono de menú  situado en la parte derecha de la fila de ese equipo.

- Desde la ventana de detalles del propio equipo a mover:
 - Dentro en el panel de listado de equipos haz clic en el equipo que quieras mover para mostrar la ventana de detalles.
 - Localiza el campo **Grupo** y haz clic en el botón **Cambiar**. Se mostrará una ventana con el árbol de grupos de destino.
 - Selecciona el grupo destino y haz clic en **Aceptar**.

Mover equipos desde grupos Active Directory

Un equipo que reside en un grupo Directorio Activo está sincronizado con el Directorio Activo de la empresa y por tanto no es posible mover lo a otro grupo de tipo Directorio Activo desde la consola de Advanced EDR. En este caso será necesario mover el equipo en el Directorio Activo de la empresa y esperar como máximo 1 hora hasta que la consola Advanced EDR se sincronice. Sin embargo, un equipo que reside en un grupo de tipo Directorio Activo sí puede moverse a un grupo nativo.



Al mover un equipo desde un grupo de tipo Directorio Activo a un grupo nativo se dejarán de sincronizar los cambios del grupo de origen. Consulta [Grupos de Directorio Activo](#) para más información.

Mover equipos hacia grupos Active Directory

No es posible mover un equipo desde un grupo nativo a un grupo Directorio Activo específico. El único movimiento que se permite es mover el equipo al grupo de tipo Directorio Activo en el que reside dentro del servidor de Directorio Activo de la empresa. Para ello haz clic en el menú de contexto del equipo y selecciona **Mover a su ruta de Active Directory**.

Restaurar la pertenencia de varios equipos a su grupo Active Directory

Para restablecer la pertenencia de equipos a su grupo Directorio Activo original haz clic en el menú de contexto de un grupo de Directorio Activo y selecciona la opción **Recuperar los equipos de esta rama de Active Directory**. Todos los equipos que pertenecen a ese grupo en el Directorio Activo de la empresa y que el administrador movió a otros grupos dentro de la consola Advanced EDR serán devueltos a su grupo original.

Filtrar resultados por grupos

La función de filtrar resultados por grupos muestra en la consola únicamente la información generada por los equipos de la red que pertenecen a los grupos elegidos por el administrador. Es una forma rápida de establecer un filtro que afecta de forma transversal a toda la consola (listados, paneles de control y configuraciones) y que ayuda a resaltar los datos de interés para el administrador.

Configurar el filtro de resultados por grupos

Para configurar el filtrado de resultados por grupos sigue los pasos mostrados a continuación:

- Haz clic en el botón del menú superior. Se desplegará una ventana con el árbol de grupos.
- Selecciona los grupos que se mostrarán de entre el árbol de equipos y pulsa en el botón **Aceptar**.

La consola mostrará únicamente la información generada de los equipos que pertenecen a los grupos seleccionados.



Figura 8.4: Filtrar resultados por grupos

Filtrar equipos no afecta a la visibilidad de tareas, ni al envío de alertas por email, ni al envío programado de informes ejecutivos.

Filtrar grupos

En infraestructuras IT muy grandes, el árbol de grupos puede contener un gran número de nodos distribuidos en muchos niveles, dificultando la localización de un determinado grupo. Para filtrar el árbol de grupos y mostrar únicamente aquellos que coincidan con el patrón de caracteres introducido:

- Haz clic en el icono  situado en la parte superior del árbol de grupos. Se mostrará una caja de texto debajo.
- Introduce las letras que forman parte del nombre del grupo a buscar. Se mostrarán los grupos que comiencen, terminen o contengan la cadena de caracteres indicada.
- Una vez realizada la búsqueda, selecciona el grupo de tu interés y haz clic en el icono  para volver a mostrar el árbol de grupos completo, pero conservando la selección del grupo.

Listados disponibles para gestionar equipos

Listado de equipos

Acceso al listado

- Haz clic en el menú superior **Equipos**. En el panel lateral izquierdo se mostrará el árbol de equipos o de carpetas, y en el panel lateral derecho un listado con todos los equipos administrados en la red.
- Haz clic en un elemento del árbol de grupos o de filtros en el panel lateral izquierdo. El panel derecho se refrescará con el contenido del elemento seleccionado.

☐	Computer ↑	IP address	Group	Operating system	Last connection
☐	WIN_DESKTOP_1	192.168.0.162	Workstation	Windows 7 Enterprise	4/10/2018 5:41:52 AM
☐	WIN_DESKTOP_2	192.168.0.86	Workstation	Windows 8.1 Enterprise SP4	4/10/2018 5:41:52 AM
☐	WIN_DESKTOP_3	192.168.0.19	Workstation	Windows Server 2012 R2 Datacenter	4/10/2018 5:41:53 AM
☐	WIN_DESKTOP_4	192.168.0.202	Workstation	Windows Server 2008 R2 Enterprise	4/10/2018 5:41:55 AM
☐	WIN_LAPTOP_1	192.168.0.164	Laptop	Windows Small Business Server 2003 SP2	4/10/2018 5:41:54 AM
☐	WIN_SERVER_1	192.168.0.40	SUPPORT	Windows 2003 Web SP2	4/7/2018 5:41:51

25 rows 1 to 14 of 14 1

Figura 8.5: El panel Listado de equipos

Permisos requeridos

El acceso al panel **Listado de equipos** no requiere permisos adicionales para el administrador.

Equipos

El listado de equipos muestra los puestos de usuario y servidores correspondientes al grupo o filtro seleccionado en el árbol de equipos. Además, incluye herramientas que permiten gestionar uno o varios equipos simultáneamente.

A continuación, se muestra un esquema del panel listado de equipos:

- (1) Listado de equipos que pertenecen a la rama del árbol seleccionada.
- (2) Herramienta de búsqueda: localiza equipos por su nombre, descripción, dirección IP, último usuario registrado o MUID (identificador de equipo utilizado en Cytomic Orion), admitiendo coincidencias parciales sin tener en cuenta mayúsculas y minúsculas.
- (3) Menú de contexto general: aplica una misma acción a varios equipos.
- (4) Casillas de selección de equipos.
- (5) Sistema de paginación en la parte inferior del panel.
- (6) Menú de contexto del equipo.

El listado de equipos es configurable para poder adaptar la información mostrada a las necesidades del administrador.

Para añadir o quitar columnas, haz clic en el menú de contexto situado en la parte superior derecha y elige la opción **Añadir o eliminar columnas**. Se mostrarán las columnas disponibles y el enlace **Columnas por defecto** para restaurar la configuración del listado a sus valores iniciales.

Utiliza el menú de contexto para exportar el listado de equipos. La exportación puede incluir todos los datos del listado de equipos (consulta [Campos mostrados en el fichero exportado](#)) o una versión reducida (consulta [Campos mostrados en el fichero reducido exportado](#)), muy útil cuando se trata de una gran número de equipos.

- Haz clic en el icono para desplegar las opciones de listados.
- Haz clic en el icono  correspondiente al tipo de listado para generar las exportaciones o las exportaciones reducidas del listado de los equipos.

Por cada equipo se incluye la información mostrada a continuación:

Campo	Descripción	Valores
Equipo	Nombre del equipo y su tipo.	Cadena de caracteres: •  Puesto de trabajo o servidor •  Equipo portátil
Estado del equipo	Reinstalación del agente: •  Reinstalando agente. •  Error en la reinstalación del agente Reinstalación de la protección: •  Reinstalando la protección •  Error en la reinstalación de la protección. •  Pendiente de reinicio. Estado de aislamiento del equipo: •  Equipo en proceso de entrar e aislamiento. •  Equipo aislado. •  Equipo en proceso de salir del aislamiento. Modo Contención de ataque RDP:	Icono

Campo	Descripción	Valores
	 Equipo en modo contención de ataque RDP.  Finalizando modo de contención de ataque RDP. Modo detallado del equipo:  Equipo en modo detallado.	
Dirección IP	Dirección IP principal del equipo.	Dirección IP
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo y su tipo.	Cadena de caracteres:  Grupo  Grupo IP  Dominio AD o raíz del Directorio Activo  Unidad Organizativa  Raíz del árbol de grupos
Ruta del directorio Activo	Ruta dentro del árbol de Directorio Activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Sistema operativo	Nombre y versión del sistema operativo instalado en el equipo.	Cadena de caracteres
Última	Fecha del último envío del estado del equipo a la nube	Fecha

Campo	Descripción	Valores
conexión	de Cytomic.	

Tabla 8.3: Campos del Listado de equipos

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Lista separada por comas de todas las direcciones IP de las tarjetas instaladas en el equipo.	Cadena de caracteres
Dirección IP pública	Dirección IP del último dispositivo (router / proxy / extremo VPN) que conecta la red del cliente con Internet.	Dirección IP
Direcciones físicas (MAC)	Lista separada por comas de todas las direcciones físicas de las tarjetas instaladas en el equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Directorio Activo	Ruta dentro del árbol de Directorio Activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres
Fecha arranque del	Fecha en la que se inicio el equipo por última	Fecha

Campo	Descripción	Valores
sistema	vez.	
Fecha de instalación	Fecha en la que el Software Advanced EDR se instaló con éxito en el equipo.	Fecha
Fecha de última conexión	Fecha más reciente en la que el equipo contactó con la nube.	Fecha
Plataforma	Tipo de sistema operativo instalado.	- Windows - Linux - macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o está virtualizado.	Booleano
Es equipo no persistente	Indica si el sistema operativo de la máquina virtual reside en un dispositivo de almacenamiento que perdura entre reinicios o, por el contrario, se regenera a su estado original.	Booleano
Versión de la protección	Versión interna del módulo de protección instalado en el equipo.	Cadena de caracteres
Fecha de última actualización	Fecha de la última actualización de la protección.	Fecha
Licencias	Producto licenciado en el equipo.	Advanced EDR
Configuración de red	Nombre de la configuración de red que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de red.	Cadena de caracteres
Seguridad para estaciones y	Nombre de la configuración de seguridad que afecta al puesto de trabajo o servidor.	Cadena de caracteres

Campo	Descripción	Valores
servidores		
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad.	Cadena de caracteres
Ajustes por equipo	Nombre de la configuración de ajustes que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de ajustes.	Cadena de caracteres
Cytomic Data Watch	Nombre de la configuración de seguimiento de información personal (Cytomic Data Watch) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguimiento de información personal.	Cadena de caracteres
Gestión de parches	Nombre de la configuración de parcheo (Cytomic Patch) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de parcheo.	Cadena de caracteres
Cifrado	Nombre de la configuración de cifrado (Cytomic Encryption) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de cifrado.	Cadena de caracteres
Software autorizado	Nombre de la configuración del módulo Software Autorizado que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de Software autorizado.	Cadena de caracteres
Bloqueo de programas	Nombre de la configuración de programas bloqueados por el administrador que afecta al	Cadena de caracteres

Campo	Descripción	Valores
	equipo.	
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de bloqueo de programas.	Cadena de caracteres
Indicadores de ataque (IOA)	Nombre de la configuración de Indicadores de ataque (IOA) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de Indicadores de ataque (IOA) que afecta al equipo.	Cadena de caracteres
Estado de aislamiento	Muestra el estado del aislamiento del equipo.	• Aislado • Aislado • Dejando de aislar • No aislado
Modo "Contención de ataque RDP"	Estado del Modo de "Contención de ataque RDP".	Booleano
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Último usuario logueado	Nombres de las cuentas de usuario separados por coma que mantienen una sesión interactiva abierta en equipos Windows.	Cadena de caracteres
Acción solicitada	Petición pendiente de ejecutar o en ejecución.	• Reinicio • Reinstalación de protección • Reinstalación de agente
Error en la acción solicitada	Tipo de error reportado en la acción solicitada.	• Credenciales incorrectas • Equipo descubridor no disponible • No es posible conectar

Campo	Descripción	Valores
		con el equipo • Sistema operativo no soportado • No es posible descargar el instalador del agente • No es posible copiar el instalador del agente • No es posible desinstalar el agente • No es posible instalar el agente • No es posible registrar el agente • Requiere intervención del usuario
Último proxy utilizado	Método de acceso empleado por Advanced EDR en su última conexión con la nube de Cytomic. Este dato no se actualiza de forma inmediata y puede tardar hasta 1 hora en reflejar su valor correcto.	Cadena de caracteres
Shadow Copies	Indica el estado de la funcionalidad: • Activo • Desactivado • Error 2010: No se ha podido habilitar el servicio de Shadow copies. • Error 2011: Se ha producido un error al crear el último Shadow copy.	Enumeración
Última copia realizada	Fecha y hora en la que se realizó la última copia.	Fecha

Tabla 8.4: Campos del fichero exportado Listado de equipos

Campos mostrados en el fichero reducido exportado

Al seleccionar **Exportación reducida** se genera un fichero con la siguiente información:

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	• Estación • Portátil • Servidor
Dirección IP	Lista separada por comas de todas las direcciones IP de las tarjetas instaladas en el equipo.	Cadena de caracteres
Dirección IP Pública	Dirección IP del último dispositivo (router / proxy / extremo VPN) que conecta la red del cliente con Internet.	Dirección IP
Direcciones físicas (MAC)	Lista separada por comas de todas las direcciones físicas de las tarjetas instaladas en el equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Directorio Activo	Ruta dentro del árbol de Directorio Activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Última vez visto en directorio activo	Fecha en la que el equipo fue visto por última vez en el Directorio Activo.	
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres
Fecha de arranque del sistema	Fecha en la que se inicio el equipo por última vez.	Cadena de caracteres
Fecha de	Fecha en la que el Software Advanced EDR se instaló	Fecha

Campo	Descripción	Valores
instalación	con éxito en el equipo.	
Fecha de última conexión	Fecha más reciente en la que el equipo contactó con la nube.	Fecha
Plataforma	Tipo de sistema operativo instalado.	- Windows - Linux - macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o está virtualizado.	Booleano
Es equipo no persistente	Indica si el sistema operativo de la máquina virtual reside en un dispositivo de almacenamiento que perdura entre reinicios o, por el contrario, se regenera a su estado original.	Booleano
Versión de la protección	Versión interna del módulo de protección instalado en el equipo.	Cadena de caracteres
Fecha de última actualización	Fecha de la última actualización de la protección.	Fecha
Licencias	Producto licenciado en el equipo.	Advanced EDR
Estado de aislamiento	Muestra el estado del aislamiento del equipo.	- Aislado - Aislando - Dejando de aislar - No aislado
Modo "Contención de ataque RDP"	Estado del modo de "Contención de ataque RDP".	Booleano
Descripción	Descripción asignada al equipo.	Cadena de caracteres

Campo	Descripción	Valores
Último usuario logueado	Nombres de las cuentas de usuario separados por coma que mantienen una sesión interactiva abierta en equipos Windows.	Cadena de caracteres
Acción solicitada	Petición pendiente de ejecutar o en ejecución.	• Reinicio • Reinstalación de protección • Reinstalación de agente
Error en acción solicitada	Tipo de error reportado en la acción solicitada.	• Credenciales incorrectas • Equipo descubridor no disponible • No es posible conectar con el equipo • Sistema operativo no soportado • No es posible descargar el instalador del agente • No es posible copiar el instalador del agente • No es posible registrar el agente • Requiere intervención del usuario
Último proxy utilizado por agente	Método de acceso empleado por Advanced EDR en su última conexión con la nube deCytomic. Este dato no se actualiza de forma inmediata y puede tardar hasta 1 hora en reflejar su valor correcto.	Cadena de caracteres

Campo	Descripción	Valores
Shadow Copies	Indica el estado de la funcionalidad: • Activo • Desactivado • Error 2010: No se ha podido habilitar el servicio de Shadow Copies • Error 2011: Se ha producido un error al crear el último Shadow Copies	Enumeración
Última copia realizada	Fecha y hora en la que se realizó la última copia.	Fecha

Tabla 8.5: Campos del fichero exportado reducido Listado de equipos

Herramientas de filtrado

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres.

Tabla 8.6: Filtros disponibles en el listado Equipos

Herramientas de gestión

Las herramientas de gestión están disponibles en:

- Al seleccionar uno o más equipos con las casillas de selección (4), la herramienta de búsqueda (2) se oculta y en su lugar se muestra la barra de acciones (7).

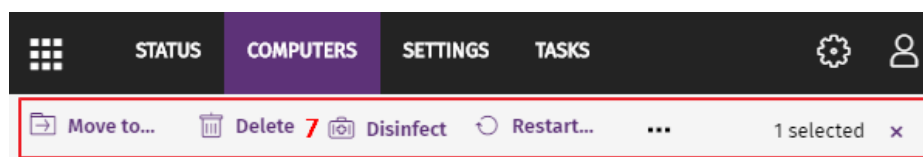


Figura 8.6: Barra de acciones solapando a la herramienta de búsqueda

Al seleccionar la casilla de selección situada a la altura de la cabecera de la tabla (4), se marcarán todos los equipos de la página actual del listado y se mostrará el mensaje **Seleccionar las xx filas del listado**, que permite marcar todos los equipos del listado independientemente de la paginación.

- Al hacer clic en el menú de contexto (6) asociado a un equipo o dispositivo móvil.

Acción	Descripción
 Mover a	Muestra una ventana con el árbol de grupos. Elige un grupo como destino de los equipos seleccionados. Los equipos heredarán las configuraciones asignadas al grupo de destino. Para más información, consulta Crear y gestionar configuraciones en la página 258.
 Mover a su ruta de directorio activo	Mueve los equipos seleccionados al grupo que se corresponde con la unidad organizativa del directorio activo de la empresa.
 Eliminar	Borra el equipo de la consola y desinstala el software de cliente Advanced EDR. Para más información, consulta Desinstalar el software en la página 150.
 Reiniciar	Reinicia el equipo. Par más información, consulta Reiniciar equipos en la página 803.
 Desinfectar	Programa una tarea de desinfección de ejecución inmediata.
 Aislar equipo	Impide todas las comunicaciones del equipo excepto las necesarias para conectar con la nube de Cytomic. Para más información, consulta Aislar uno o varios equipos de la red de la organización en la página 805.
 Dejar de aislar equipo	Restaura las comunicaciones del equipo. Para más información, consulta Quitar el aislamiento de un equipo en la página 805.
 Visualizar parches disponibles	Abre el listado Parches disponibles filtrado por el equipo seleccionado. Consulta Parches disponibles en la página 423.
 Programar instalación de parches	Para obtener información sobre cómo instalar parches en equipos Windows, consulta Cytomic Patch(Actualización de programas vulnerables) en la página 375.
 Ver inventario del equipo	Abre el listado Archivos con información personal filtrado por el equipo seleccionado. Consulta Archivos con información personal en la página 358.
 Control remoto	Inicia una conexión remota con el equipo seleccionado. Consulta Control remoto de los equipos en la página 807.

Acción	Descripción
 Modo Detallado	Activa el modo detallado para generar telemetría ampliada. Consulta Modo detallado en la página 306.
 Desactivar modo Detallado	Desactiva el modo detallado para generar telemetría estándar. Consulta Modo detallado en la página 306
 Finalizar modo "Contención de ataque RDP"	Finaliza de forma manual el bloqueo de conexiones RDP. Consulta Finalizar manualmente el estado de Contención de ataque RDP en la página 565.
 Reinstalar la protección (requiere reinicio)	Reinstala la protección en caso de mal funcionamiento. Para más información, consulta Reinstalación remota en la página 153.
 Reinstalar agente	Reinstala el agente en caso de mal funcionamiento. Para más información, consulta Reinstalación remota en la página 153.
 Seleccionados	Anula la selección actual de equipos.
Notificar un problema	Envía un informe al departamento de soporte de Cytomic para diagnosticar problemas en el equipo.

Tabla 8.7: Herramientas para gestionar equipos

El panel Mis listados

Acceso al panel Mis listados

- Haz clic en el menú superior **Estado** y en el menú lateral **Mis listados**. Se mostrará una ventana con todos los listados disponibles.
- Selecciona en el grupo **General** el listado **Hardware**, **Software** o **Equipos con nombre duplicado**.



Para obtener información sobre los tipos de listados y como operar con ellos, consulta [Gestión de listados](#) en la página 47.



Consulta el capítulo correspondiente al grupo al que pertenece cada listado para obtener información acerca de sus campos y de las herramientas de filtrado y búsqueda que implementan.

Permisos requeridos

El acceso al panel **Mis listados** no requiere permisos adicionales para el administrador.

Hardware

Contiene los componentes hardware instalados en cada equipo del parque informático. Un mismo componente hardware se mostrará de forma independiente cada vez que sea detectado en un equipo.

Campo	Descripción	Valores
Equipo	Nombre y tipo del equipo que contiene el componente hardware.	Cadena de caracteres: •  Puesto de trabajo o servidor. •  Equipo portátil.
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
CPU	Marca y modelo del microprocesador instalado en el equipo. Se indica el número de núcleos / cores instalados entre paréntesis.	Cadena de caracteres
Memoria	Cantidad total de memoria RAM instalada.	Cadena de caracteres
Capacidad de disco	Suma de la capacidad de todos los discos duros internos conectados al equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Advanced EDR a la nube de Cytomic.	Fecha

Campo	Descripción	Valores
Menú de contexto	Herramientas de gestión. Para más información, consulta Herramientas de gestión .	

Tabla 8.8: Campos del Listado de hardware

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dirección IP pública	Dirección IP del último dispositivo (router / proxy / extremo VPN) que conecta la red del cliente con Internet.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres

Campo	Descripción	Valores
Última conexión	Fecha del último envío del estado de Advanced EDR a la nube de Cytomic.	Fecha
Plataforma	Tipo de sistema operativo instalado.	• Windows • Linux • macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Sistema	Nombre del modelo hardware del equipo.	Cadena de caracteres
CPU-X	Marca, modelo y características de la CPU numerada X.	Cadena de caracteres
CPU-X Número de núcleos	Número de núcleos o cores de la CPU numerada X.	Numérico
CPU-X Número de procesadores lógicos	Número de núcleos lógicos mostrados al sistema operativo por el sistema de HyperThreading / SMT (Simultaneous MultiThreading).	Numérico
Memoria	Suma de todos los bancos de memoria RAM instalados en el equipo.	Cadena de caracteres
Disco-X Capacidad	Espacio total del medio de almacenamiento interno numerado X.	Cadena de caracteres
Disco-X Particiones	Numero de particiones reportadas al sistema operativo del medio de almacenamiento interno numerado X.	Numérico
Versión de especificación del TPM	Versiones de las APIs compatibles con el chip TPM.	Cadena de caracteres

Campo	Descripción	Valores
BIOS - número de serie	Número de serie de la BIOS del equipo.	Cadena de caracteres

Tabla 8.9: Campos del fichero exportado Hardware

Herramienta de filtrado

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil - Servidor
Plataforma	Marca del sistema operativo.	Windows

Tabla 8.10: Filtros disponibles en el Listado de hardware

Software

Contiene todos los programas instalados en los equipos de la red. Por cada paquete se indica el número de equipos que lo tienen instalado e información sobre la versión y su fabricante.

Al hacer clic en un paquete de software, se abrirá el listado **Equipos** filtrado por el paquete seleccionado, para mostrar los equipos que lo tienen instalado.

Campo	Descripción	Valores
Nombre	Nombre del paquete software encontrado en el parque.	Cadena de caracteres
Editor	Fabricante del paquete software.	Cadena de caracteres
Versión	Versión interna del paquete software.	Cadena de caracteres
Equipos	Número de equipos que contienen el paquete encontrado.	Numérico

Tabla 8.11: Campos del Listado de software

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres

Campo	Descripción	Valores
Nombre	Nombre del paquete software encontrado en el parque.	Cadena de caracteres
Editor	Fabricante del paquete software.	Cadena de caracteres
Versión	Versión interna del paquete software.	Cadena de caracteres
Equipos	Número de equipos que contienen el paquete encontrado.	Numérico

Tabla 8.12: Campos del Listado de software

Campos mostrados en el excel de detalle

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Equipo que contiene el paquete encontrado.	Numérico
Nombre	Nombre del paquete software encontrado en el parque.	Cadena de caracteres
Editor	Fabricante del paquete software.	Cadena de caracteres
Fecha de instalación	Fecha en la que se instaló el software.	Fecha
Tamaño	Tamaño del software instalado.	Numérico
Versión	Versión interna del paquete software.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres

Campo	Descripción	Valores
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 8.13: Campos del listado exportado de detalle

Herramienta de filtrado

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Plataforma	Marca del sistema operativo.	• Windows • Linux • macOS

Tabla 8.14: Filtros disponibles en el Listado de software

Ventana listado de equipos

Al hacer clic en una de las filas del listado se mostrará el listado de equipos filtrado por el paquete de software seleccionado. Para obtener más información, consulta [Equipos](#).

Equipos con nombre duplicado

Muestra los equipos detectados en la red con el mismo nombre y que pertenecen al mismo dominio. De cada grupo de equipos duplicados Advanced EDR considerará correcto el equipo con la fecha de conexión a la nube de Cytomic más reciente, y el resto como erróneos. El equipo considerado correcto se excluirá del listado para que el administrador seleccione y elimine el resto de equipos de una vez.

Para eliminar los equipos duplicados selecciónalos mediante las casillas de selección y la opción **Eliminar** del menú de herramientas. Se mostrará una ventana preguntando si quieres desinstalar el agente Advanced EDR o no.



Borrar equipos del listado **Equipos con nombre duplicado** sin desinstalar el agente Advanced EDR únicamente los borra de la consola de Advanced EDR. Un equipo así eliminado volverá a aparecer en la consola de Advanced EDR al ponerse en contacto con la nube. Ante un borrado masivo de equipos sin tener la seguridad de cuales están realmente duplicados se recomienda no desinstalar previamente el agente de ningún equipo y comprobar qué equipos reaparecen en la consola.

Campo	Descripción	Valores
Equipo	Nombre y tipo del equipo	Cadena de caracteres: - Puesto de equipo o servidor - Equipo portátil.
Dirección IP	Dirección principal del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel del parche aplicado.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Advanced EDR a la nube de Cytomic.	Fecha

Tabla 8.15: Campos del Listado de Equipos con nombre duplicado

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil - Servidor

Campo	Descripción	Valores
		Dispositivo móvil
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres
Versión de la protección	Versión interna del módulo de protección instalado en el equipo.	Cadena de caracteres
Fecha de instalación	Fecha en la que el Software Advanced EDR se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha del último envío del estado de Advanced EDR a la nube de Cytomic.	Fecha
Plataforma	Tipo de sistema operativo instalado.	- Windows - Linux - macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Directorio Activo	Ruta completa del equipo en el Directorio Activo de la empresa.	Cadena de caracteres

Campo	Descripción	Valores
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.	Cadena de caracteres
Fecha arranque del sistema	Fecha en la que se inició el equipo por última vez.	Fecha

Tabla 8.16: Campos del fichero exportado Equipos con nombre duplicado

Herramienta de filtrado

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Plataforma	Marca del sistema operativo.	• Todos • Windows • Linux • macOS

Campo	Descripción	Valores
Última conexión	Fecha del último envío del estado de Advanced EDR a la nube de Cytomic.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días

Tabla 8.17: Filtros disponibles en el listado Equipos con nombre duplicado

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Para obtener más información, consulta [Información de equipo](#).

Información de equipo

Al seleccionar un dispositivo en el panel de listado de equipos se muestra una ventana con el detalle de la información del hardware y software instalado, así como de la configuración de seguridad asignada.

Para ocultar o mostrar la información del dispositivo y las notificaciones, haz clic en el icono  o .

La ventana de detalle del equipo se divide en varias secciones:

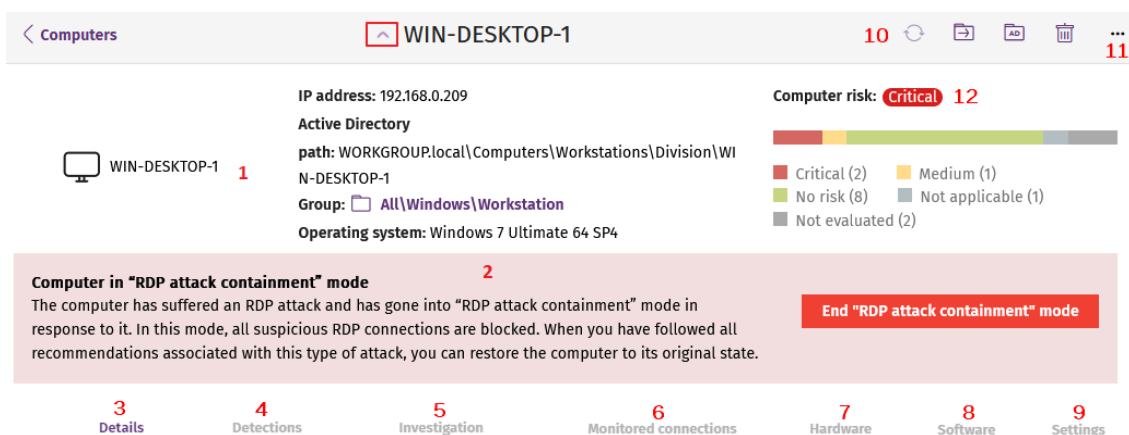


Figura 8.7: Vista general de la información de equipo

- **General (1):** información que ayuda a identificar el equipo.
- **Alertas de equipo (2):** mensajes con problemas potenciales asociados al equipo.
- **Detalles (3):** resumen ampliado del hardware, software y seguridad configurada en el equipo.
- **Detecciones (4):** estado de la seguridad del equipo.
- **Investigación (5):** abre la consola de investigación de Cytomic Orion para mostrar la telemetría recogida en el equipo. Consulta [Sección Investigación \(5\)](#)
- **Conexiones monitorizadas (6):** conexiones entrantes detectadas en el equipo. Consulta [Opciones de configuración de Control de Acceso a Endpoints](#) en la página 459
- **Hardware (7):** hardware instalado en el equipo, componentes y periféricos conectados, su consumo y uso.
- **Software (8):** paquetes de software instalados en el equipo, su versión y un registro de cambios.
- **Configuración (9):** configuraciones de seguridad y otras asignadas al equipo.
- **Barra de herramientas (10):** agrupa las operaciones disponibles para aplicar sobre el equipo administrado.
- **Iconos ocultos (11):** si la ventana no es lo suficientemente grande, parte de las herramientas se ocultan agrupadas.
- **Riesgo del equipo (12):** gráfica de distribución que muestra el nivel de riesgo global del equipo y los riesgos detectados en él. Consulta [Listados del módulo Evaluación de riesgos](#) en la página 651.

Sección general (1)

Contiene la siguiente información para todos los tipos de dispositivo:

Campo	Descripción
Equipo	Nombre del equipo e icono de estado del equipo.

Campo	Descripción
Dirección IP	Dirección IP del equipo.
Último usuario logueado	Nombre del último usuario logueado en el equipo.
Descripción	Información del equipo asignada por el administrador.
Grupo	Carpeta del árbol de grupos a la que pertenece el equipo.
Ruta del directorio activo	Ruta completa del equipo en el Directorio Activo de la empresa.
Dominio	Dominio al que pertenece el equipo.
Sistema operativo	Versión completa del sistema operativo instalado en el equipo.
Última conexión	Fecha de la última conexión del software de cliente con la nube de Advanced EDR
Riesgo del equipo	Gráfica de distribución que muestra el nivel de riesgo global del equipo y los riesgos detectados en él. Consulta Listados del módulo Evaluación de riesgos en la página 651 .

Tabla 8.18: Campos de la sección general de la información del equipo

Sección alertas de equipo (2)

Las alertas describen los problemas encontrados en los equipos de la red en lo que respecta al funcionamiento de Advanced EDR y su motivo, así como indicaciones para solucionarlos.

En ocasiones las alertas (1) van acompañadas de códigos (2).

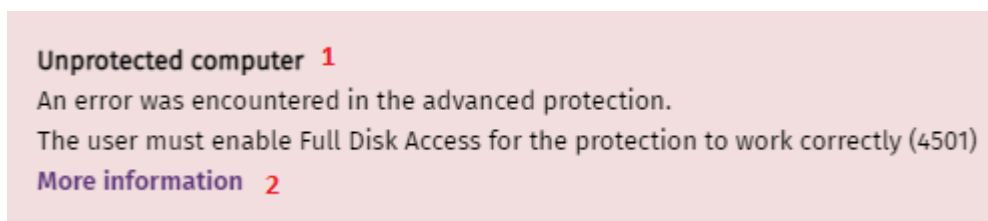


Figura 8.8: Alerta de Equipo desprotegido y código asociado

Cada código se relaciona con un error que puede aparecer durante o después de la instalación de la protección en los equipos. Para acceder a toda la información sobre los diferentes códigos, consulta <https://www.pandasecurity.com/es/support/card?id=700031>

A continuación, se muestra un resumen de los tipos de alertas generadas y las acciones recomendadas para su resolución.

Equipos aislados

Alerta	Descripción	Referencia
Equipo aislado	El administrador ha aislado el equipo y se bloquean todas las conexiones excepto aquellas necesarias para el buen funcionamiento de Advanced EDR.	Para más información, consulta Aislar un equipo en la página 804 .
Estamos intentando aislar este equipo	El servidor Advanced EDR está tratando de aislar el equipo pero la operación todavía no se ha completado por estar el equipo apagado o sin conexión a Internet.	Para más información, consulta el widget Equipos sin conexión en la página 611 .
Estamos intentando dejar de aislar este equipo	El servidor Advanced EDR está tratando de retirar el aislamiento del equipo pero la operación todavía no se ha completado por estar el equipo apagado o sin conexión a Internet.	Para más información, consulta el widget Equipos sin conexión en la página 611 .

Tabla 8.19: Alertas relacionadas con la funcionalidad de aislar equipos

Equipo en estado de contención

Alerta	Descripción	Referencia
Equipo en modo "Contención de ataque RDP"	El equipo ha recibido un gran volumen de intentos de conexión por RDP erróneos, y se han bloqueado las conexiones por este protocolo para contener el ataque.	Consulta Detección y protección frente ataques RDP en la página 562 .
Estamos intentando finalizar el modo "Contención de"	El administrador ha finalizado manualmente el modo Contención de ataque RDP en este equipo, pero todavía no se ha completado la acción. Puede que el equipo esté apagado, sin conexión, pendiente de reinicio o que la acción esté en curso.	Consulta Detección y protección frente ataques

Alerta	Descripción	Referencia
ataque RDP" en este equipo.		RDP en la página 562 .

Tabla 8.20: Alertas relacionadas con la funcionalidad de contención de equipos

Licencias

Alerta	Descripción	Referencia
Equipo sin licencia	No hay licencias libres para asignar al equipo. Retira una licencia asignada o adquiere más licencias de Advanced EDR.	Para más información, consulta Liberar licencias en la página 160 .
	Hay licencias libres pero no se han asignado a este equipo.	Para más información, consulta Asignar licencias en la página 159 .

Tabla 8.21: Alertas relacionadas con la asignación de licencias

Equipo en Modo auditoría

Alerta	Descripción	Referencia
Equipo en modo auditoría	Al activar el modo auditoría en una configuración, no se modifica el estado global de las diferentes protecciones en los equipos asignados a esa configuración, ni la configuración de las protecciones en la consola web. Las protecciones continúan detectando amenazas en los equipos e informando de ellas, pero no se llevan a cabo labores de bloqueo o desinfección.	Para más información, consulta Modo auditoría en la página 306

Tabla 8.22: Alerta relacionada con el Modo auditoría

Errores en el proceso de instalación del software de protección



Los errores ocurridos durante el proceso de instalación del software de protección se reflejan mediante un código de error, su código extendido de error asociado y un subcódigo extendido de error, si están disponibles. Para más información, consulta **Campos mostrados en fichero exportado** en la página 624.

Alerta	Descripción	Referencia
Equipo desprotegido	Se ha producido un error instalando la protección en el equipo. En el caso de errores de origen conocido se mostrará una descripción de la causa que lo motiva. Si el origen es desconocido, se mostrará el código de error asociado.	Para más información, consulta Funcionalidades del producto y requisitos en la página 847.
	El equipo requiere un reinicio para completar la instalación debido a una desinstalación previa.	Para más información, consulta Reiniciar equipos en la página 803 .
	El agente no cuenta con los permisos necesarios en equipos macOS.	Para más información, consulta Requisitos de plataformas macOS en la página 856.
	Error al instalar en macOS 13 Ventura. El usuario debe permitir EndpointProtectionService en Login Items	Para más información, consulta Requisitos de plataformas macOS en la página 856.
	El Kernel del equipo Linux no es compatible.	Para más información consulta https://www.pandasecurity.com/en/support/card?id=700031 .

Alerta	Descripción	Referencia
	Versión del Unbreakable Enterprise Kernel (UEK) no es compatible.	Para más información consulta https://www.pandasecurity.com/en/support/card?id=700031 .
Error instalando Cytomic Data Watch	Se ha producido un error instalando Cytomic Data Watch en el equipo.	Para más información, consulta Requisitos de Cytomic Data Watch en la página 315.
Error instalando la protección y Cytomic Data Watch	Se ha producido un error instalando la protección y el módulo en el equipo.	Para más información, consulta Funcionalidades del producto y requisitos en la página 847 y Requisitos de Cytomic Data Watch en la página 315.
Error instalando el gestor de parches	Se ha producido un error instalando el módulo de gestión de parches.	Para más información, consulta Comprobar que Cytomic Patch funciona correctamente en la página 380.
Error instalando el módulo de cifrado	Se ha producido un error instalando el módulo de cifrado.	Para más información, consulta Requisitos mínimos de Cytomic Encryption en la página 487 .
Error instalando el agente de Cytomic	Credenciales incorrectas.	Para más información, consulta Equipos sin conexión en la página 611.
	El equipo descubridor no está disponible.	Para más información, consulta el widget Paneles/Widgets del módulo de seguridad en la página 608 y Asignar el rol de descubridor a un equipo en la página 118.
	No es posible conectar con el equipo destinatario del paquete de instalación por estar apagado o no cumplir con los requisitos de	Para más información, consulta el widget Paneles/Widgets del módulo de seguridad en la página 608 y Funcionalidades del producto y requisitos en la página 847.

Alerta	Descripción	Referencia
	hardware y de red.	
	El sistema operativo del equipo no está soportado.	Para más información, consulta Funcionalidades del producto y requisitos en la página 847.
	No es posible descargar el instalador del agente por un fallo de red.	Para más información, consulta Funcionalidades del producto y requisitos en la página 847.
	No es posible copiar el instalador del agente en el equipo por falta de espacio.	Para más información, consulta Funcionalidades del producto y requisitos en la página 847.
	No es posible instalar el agente por no cumplirse los requisitos de instalación remota o el equipo está apagado.	Para más información, consulta el widget Equipos sin conexión en la página 611 y Funcionalidades del producto y requisitos en la página 847.
	No es posible registrar el agente.	Para más información, consulta el widget Equipos sin conexión en la página 611 y Funcionalidades del producto y requisitos en la página 847.
Error comunicando con servidores.	El equipo no puede conectar con alguno de los servidores de la nube de Cytomic.	Para más información, consulta Funcionalidades del producto y requisitos en la página 847.

Tabla 8.23: Alertas relacionadas con la instalación del software Advanced EDR

Errores en el proceso de reinstalación del software de protección



Los errores ocurridos durante el proceso de instalación del software de protección se reflejan mediante un código de error, su código extendido de error asociado y un subcódigo extendido de error, si están disponibles. Para más información, consulta [Campos del fichero exportado Estado de protección de los equipos](#) en la página 626.

Alerta	Descripción	Referencia
Pendiente de reinstalación de la protección	El administrador solicitó la reinstalación de la protección de este equipo pero todavía no se ha realizado porque el equipo está apagado, sin conexión o porque todavía no ha terminado el plazo configurado antes de forzar el reinicio.	Consulta el widget Equipos sin conexión en la página 611 y Requisitos de la funcionalidad de reinstalación remota en la página 153.
Pendiente de reinstalación del agente	El administrador solicitó la reinstalación del agente en este equipo pero todavía no se ha realizado porque el equipo está apagado, sin conexión o porque todavía no ha terminado el plazo configurado antes de forzar el reinicio.	Consulta el widget Equipos sin conexión en la página 611 y Requisitos de la funcionalidad de reinstalación remota en la página 153.
Error instalando el agente de Cytomic	Credenciales incorrectas.	Consulta el widget Equipos sin conexión en la página 611.
	Equipo descubridor no disponible.	Consulta el widget Equipos sin conexión en la página 611.
	No es posible conectar con el equipo por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget Equipos sin conexión en la página 611 y Requisitos de la funcionalidad de reinstalación remota en la página 153.
	Sistema operativo no soportado por no cumplir	Consulta Requisitos de la

Alerta	Descripción	Referencia
	con los requisitos de instalación remota.	funcionalidad de reinstalación remota en la página 153.
	No es posible descargar el instalador del agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget Equipos sin conexión en la página 611 y Requisitos de la funcionalidad de reinstalación remota en la página 153.
	No es posible copiar el instalador del agente por no estar encendido o no cumplir los requisitos de instalación remota.	Consulta el widget Equipos sin conexión en la página 611 y Requisitos de la funcionalidad de reinstalación remota en la página 153.
	No es posible desinstalar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget Equipos sin conexión en la página 611 y Requisitos de la funcionalidad de reinstalación remota en la página 153.
	No es posible instalar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget Equipos sin conexión en la página 611 y Requisitos de la funcionalidad de reinstalación remota en la página 153
	No es posible registrar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget Equipos sin conexión en la página 611 y Requisitos de la funcionalidad de reinstalación remota en la página 153

Alerta	Descripción	Referencia
	Requiere intervención del usuario.	Consulta el widget Equipos sin conexión en la página 611 y Requisitos de la funcionalidad de reinstalación remota en la página 153

Tabla 8.24: Alertas relacionadas con la reinstalación del agente Advanced EDR

Errores de funcionamiento del software Advanced EDR

Alerta	Descripción	Referencia
Equipo desprotegido	Se ha detectado un error en la protección avanzada. Reinicia el equipo para solucionar el problema.	Consulta Reiniciar equipos en la página 803
Error en Cytomic Data Watch	Se ha detectado un error en Cytomic Data Watch. Reinicia el equipo para solucionar el problema.	Consulta Reiniciar equipos en la página 803
Error cifrando el equipo	No se puede cifrar el equipo por un error.	Consulta Reiniciar equipos en la página 803

Tabla 8.25: Alertas relacionadas con el mal funcionamiento del software Advanced EDR

Acción pendiente del usuario o del administrador

Alerta	Descripción	Referencia
Cifrado pendiente de acción del usuario	Para completar el proceso de cifrado es necesario que el usuario reinicie el equipo o introduzca las credenciales de cifrado.	Consulta Proceso de cifrado y descifrado en Windows en la página 488 y Proceso de cifrado y descifrado en macOS
Pendiente de reinicio	El administrador ha solicitado el reinicio de este equipo pero todavía no se ha completado por falta de conexión o por no	Consulta el widget Equipos sin conexión en la página 611

Alerta	Descripción	Referencia
	haberse cumplido el plazo para ejecutar un inicio forzoso.	
Reinstalando la protección	El administrador ha solicitado la reinstalación de la protección en este equipo y todavía no se ha completado por estar el equipo apagado, sin conexión, sin completar el plazo configurado antes del reinicio o por estar el proceso en curso.	Consulta Reinstalación remota en la página 153
Equipo desprotegido	La protección avanzada está desactivada. Activa la protección.	Consulta Asignación manual y automática de configuraciones en la página 261 , Crear y gestionar configuraciones en la página 258 y Protección avanzada en la página 296
Equipo sin conexión desde hace X días	Es posible que el equipo esté apagado o no se cumplan los requisitos de acceso a la red.	Consulta Funcionalidades del producto y requisitos en la página 847 .
Protección desactualizada	La protección necesita que el usuario local reinicie manualmente el equipo para completar la instalación*.	* solo reproducible en las versiones Windows Home y Starter.
Problemas de conexión con los equipos de Cytomic	El equipo no se puede conectar correctamente con los servidores donde se almacena la inteligencia de seguridad.	Consulta Funcionalidades del producto y requisitos en la página 847 .
El administrador ha cambiado el estado de las protecciones desde la consola local	El administrador cambió la configuración de la protección desde el propio agente instalado en el equipo del usuario o servidor. De esta forma, la configuración actual no coincide con la establecida desde la consola web.	
No es posible	Las nuevas versiones de la protección	Consulta Compatibilidad

Alerta	Descripción	Referencia
actualizar la protección de este equipo a la última versión.	requieren que el sistema operativo reconozca los drivers firmados con el formato SHA-256. Este equipo no soporta dicho formato de firma, y por lo tanto no es posible actualizar la protección instalada en él a la última versión.	con firma de drivers SHA-256 en la página 855.

Tabla 8.26: Alertas relacionadas con la falta de acción del usuario o administrador de la red

Equipo desactualizado

Alerta	Descripción	Referencia
Protección desactualizada	La protección requiere que el equipo se reinicie para terminar la actualización.	Para más información, consulta Reiniciar equipos en la página 803
	Se ha producido un error intentando actualizar la protección. Comprueba que se cumplen los requisitos de hardware y de red.	Consulta Funcionalidades del producto y requisitos en la página 847 y el espacio disponible en disco en Sección Hardware (7) .
	Las actualizaciones están desactivadas para este equipo. Asigna un perfil de configuración con las actualizaciones activadas.	Consulta Actualización del motor de protección en la página 172.
Conocimiento sobre malware y otras amenazas desactualizado	Las actualizaciones de conocimiento están desactivadas para este equipo. Asigna un perfil de configuración con las actualizaciones activadas.	Consulta Actualizaciones del conocimiento en la página 175.

Tabla 8.27: Alertas relacionadas con el software Advanced EDR desactualizado

Sección Detalles (3)

La información se divide en los siguientes apartados:

- **Equipo:** información de la configuración del dispositivo ofrecida por el agente Cytomic.
- **Seguridad:** estado de las protecciones de Advanced EDR.

- **Protección de datos** (sólo Windows): estado de los módulos que protegen el contenido de los datos almacenados en el equipo.

Equipo

Campo	Descripción
Riesgo	Para los dispositivos Android, se muestra la gráfica de distribución que muestra el nivel de riesgo global del equipo y los riesgos detectados en él. Consulta Listados del módulo Evaluación de riesgos en la página 651.
Nombre	Nombre del equipo.
Descripción	Texto descriptivo asignado por el administrador.
Direcciones IP	Listado con todas las direcciones IP (principal y alias).
Dirección IP pública	Dirección IP del último dispositivo (router / proxy / extremo VPN) que conecta a la red del cliente con Internet.
Direcciones físicas (MAC)	Dirección física de las tarjetas de red instaladas.
Dominio	Dominio Windows al que pertenece el equipo. Vacío si no pertenece a un dominio.
Ruta de directorio activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo.
Grupo	Grupo dentro del árbol de grupos al que pertenece el equipo. Para cambiar el grupo del equipo haz clic en el botón Cambiar .
Sistema operativo	Sistema operativo instalado en el equipo.
Máquina virtual	Indica si el equipo es físico o esta virtualizado.
Es equipo no persistente	Indica si el sistema operativo de la máquina virtual reside en un dispositivo de almacenamiento que perdura entre reinicios o por el contrario se regenera a su estado original.
Licencias	Licencias de productos de Cytomic instalados en el equipo. Consulta Licencias en la página 157 para más información.

Campo	Descripción
Versión del agente	Versión interna del agente Cytomic instalado en el equipo.
Fecha de arranque del sistema	Fecha en la que se inició el equipo por última vez.
Fecha de instalación	Fecha en la que se instaló el sistema operativo del equipo por última vez.
Último proxy utilizado	Método de acceso empleado por Advanced EDR en su última conexión con la nube de Cytomic. Este dato no se actualiza de forma inmediata y puede tardar hasta 1 hora en reflejar su valor correcto.
Última conexión del agente con la infraestructura Cytomic	Fecha de la última conexión del software de cliente con la nube de Cytomic. Como mínimo el agente de comunicaciones contactará cada 4 horas.
Último chequeo de la configuración	Fecha en la que Advanced EDR comprobó por última vez la configuración en la nube de Cytomic en busca de cambios.
Shadow Copies	Indica el estado de la funcionalidad; • Activado • Desactivado • Código de error
Última copia realizada	Indica la fecha y hora de la última copia realizada.
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.
Control remoto	Indica el estado de la funcionalidad: • Activado • Desactivado • Error instalando: el módulo de control remoto reportó un error en el proceso de instalación. • Sin licencia: el software de seguridad no tiene una licencia de Advanced

Campo	Descripción
	EDR asignada. • Sin información: el agente todavía no ha enviado información del estado del módulo al servidor.

Tabla 8.28: Campos de la sección detalles del equipo

Seguridad

En esta sección se indican el estado (Activado, Desactivado, Error) de las distintas tecnologías de Advanced EDR que protegen al equipo del malware.

Campo	Descripción
Protección avanzada	Protección frente a amenazas avanzadas, APTs y exploits.
Gestión de parches	Instalación de parches y actualizaciones de sistemas operativos Windows, macOS, Linux y aplicaciones de terceros. Detección del estado del parcheo de los equipos y desinstalación de los parches problemáticos.
Instalación de parches	Indica si se ha bloqueado la instalación de parches en el equipo, o si se trata de un equipo de prueba para la instalación de parches. Para más información, consulta Funcionalidades de Cytomic Patch
Bloqueo de programas	Bloqueo de la ejecución de los programas que el administrador considere peligrosos o no compatibles con la actividad desarrollada en la empresa.
Fecha de la última comprobación	Fecha en la que Cytomic Patch consultó a la nube para comprobar si se publicaron nuevos parches.
Versión de la protección	Versión interna del módulo de la protección instalado en el equipo.
Versión de actualización del conocimiento	Fecha de la última descarga del fichero de firmas en el equipo.
Cifrado de discos duros (solo equipos Mac)	Estado del módulo de cifrado: • No disponible: el equipo no es compatible con Cytomic Encryption.

Campo	Descripción
	• Sin información: el equipo todavía no ha enviado información del módulo de cifrado. • Activado: el equipo tiene asignada una configuración que establece el cifrado de sus dispositivos de almacenamiento y no se han producido errores. • Desactivado: el equipo tiene asignada una configuración que establece el descifrado de sus dispositivos de almacenamiento y no se han producido errores. • Error instalando: error en la descarga o instalación de los ejecutables necesarios para gestionar el servicio de cifrado en caso de no estar disponibles previamente en el equipo. • Sin licencia: el equipo no tiene una licencia de Advanced EDR asignada. Obtener la clave de recuperación: muestra una ventana con el identificador de la clave de recuperación asociada al equipo y la propia clave. Consulta Proceso para obtener la clave de recuperación en la página 494 para más información. Estado del proceso de cifrado: • Desconocido: alguna unidad no tiene un estado conocido. • Discos no cifrados: el inicio del proceso de cifrado en el equipo está pendiente de que el usuario introduzca la contraseña con permisos de administrador. • Discos cifrados: todas las unidades compatibles con la tecnología de cifrado están cifradas. • Cifrando: al menos una unidad del equipo está siendo cifrada. • Descifrando: al menos una unidad del equipo está siendo descifrada. • Cifrado por el usuario: todos los medios de almacenamiento se encuentran cifrados por el usuario. • Cifrado por el usuario (parcialmente): algunos de los medios de almacenamiento se encuentran cifrados por el usuario.
Método de autenticación (equipos Mac)	• Contraseña: el método de autenticación aplicado es la contraseña solicitada en el inicio del equipo.

Campo	Descripción
Conexión con servidores de conocimiento	Estado de la conexión del equipo con los servidores de Cytomic. En caso de errores se incluyen los enlaces a las páginas de ayuda que recopilan los requisitos de obligado cumplimiento.

Tabla 8.29: Campos de la sección detalles de la seguridad

Protección de datos (Windows)

En esta sección se indica el estado de los módulos que protegen los datos almacenados en el equipo.

Campo	Descripción
Seguimiento de información personal	Monitorización de los ficheros que contienen datos susceptibles de poder identificar a usuarios o clientes de la empresa (módulo Cytomic Data Watch).
Permitir búsquedas de información en este equipo	Indica si el equipo tiene asignado un perfil de configuración que le permita recibir búsquedas de ficheros y reportar sus resultados.
Inventario de información personal	Si se permiten búsquedas de ficheros por contenido, es necesario que Cytomic Data Watch examine todos los ficheros de los medios de almacenamiento soportados para recuperar su contenido y generar una base de datos.
Estado de indexación	• No indexado • Indexado • Indexado (solo el texto) • Indexado (todo el contenido) • Indexando
Cifrado de discos duros	Estado del módulo de cifrado: • No disponible: el equipo no es compatible con Cytomic Encryption. • Sin información: el equipo todavía no ha enviado información del módulo de cifrado. • Activado: el equipo tiene asignada una configuración que establece el cifrado de sus dispositivos de almacenamiento y no se han producido errores.

Campo	Descripción
	• Desactivado: el equipo tiene asignada una configuración que establece el descifrado de sus dispositivos de almacenamiento y no se han producido errores. • Error: la configuración establecida por el administrador no permite aplicar un método de autenticación soportado por Cytomic Encryption en la versión del sistema operativo instalada en el equipo. • Error instalando: error en la descarga o instalación de los ejecutables necesarios para gestionar el servicio de cifrado en caso de no estar disponibles previamente en el equipo. • Sin licencia: el equipo no tiene una licencia de Advanced EDR asignada. Obtener la clave de recuperación: muestra una ventana con los identificadores de los medios de almacenamiento cifrados del equipo. Al hacer clic en cualquier de ellos se muestra la clave de recuperación. Consulta Proceso para obtener la clave de recuperación en la página 494 para más información. Estado del proceso de cifrado: • Desconocido: alguna unidad no tiene un estado conocido. • Discos no cifrados: alguna de las unidades compatibles con la tecnología de cifrado no esta cifrada ni en proceso de cifrado. Discos no cifrados: alguna de las unidades compatibles con la tecnología de cifrado no esta cifrada ni en proceso de cifrado. • Discos cifrados: todas las unidades compatibles con la tecnología de cifrado están cifradas. • Cifrando: al menos una unidad del equipo está siendo cifrada. • Descifrando: al menos una unidad del equipo está siendo descifrada. • Cifrado por el usuario: todos los medios de almacenamiento se encuentran cifrados por el usuario. • Cifrado por el usuario (parcialmente): algunos de los medios de almacenamiento se encuentran cifrados por el usuario.
Método de autenticación	• Desconocido: método de autenticación no compatible con los soportados por Cytomic Patch. • Procesador de seguridad (TPM). • Procesador de seguridad (TPM) + Contraseña.

Campo	Descripción
	• Contraseña: método de autenticación por PIN, PIN extendido o passphrase. • USB método de autenticación por llave USB. • Ninguno: ninguna de las unidades compatibles con la tecnología de cifrado está cifrada ni en proceso de cifrado.
Fecha de cifrado	Fecha del proceso de cifrado completado más antigua dentro de la primera vez que se cifró de forma total el equipo.
Cifrado de unidades de almacenamiento extraíbles	Estado del módulo de cifrado: • No disponible: el equipo no es compatible con Cytomic Encryption. • Sin información: el equipo todavía no ha enviado información del módulo de cifrado. • Activado: el equipo tiene asignada una configuración que establece el cifrado de sus dispositivos de almacenamiento y no se han producido errores. • Desactivado: el equipo tiene asignada una configuración que establece el descifrado de sus dispositivos de almacenamiento y no se han producido errores. • Error: la configuración establecida por el administrador no permite aplicar un método de autenticación soportado por Cytomic Encryption en la versión del sistema operativo instalada en el equipo. • Error instalando: error en la descarga o instalación de los ejecutables necesarios para gestionar el servicio de cifrado en caso de no estar disponibles previamente en el equipo. • Sin licencia: el equipo no tiene una licencia de Advanced EDR asignada. Ver dispositivos cifrados de este equipo: muestra una ventana con los identificadores de los medios de almacenamiento externos cifrados del equipo. Al hacer clic en cualquier de ellos se muestra la clave de recuperación. Consulta Proceso para obtener la clave de recuperación en la página 494.

Tabla 8.30: Campos de la sección Protección de datos

Sección Detecciones (4) en Windows, Linux y macOS

Muestra los contadores asociados a la seguridad y al nivel de parcheo del equipo mediante los siguientes widgets:

Panel de Control	Descripción
Detecciones mediante políticas avanzadas de seguridad	Consulta Detecciones mediante políticas avanzadas de seguridad en la página 618.
Actividad de malware	Consulta Actividad de malware / PUP en la página 613.
Programas actualmente bloqueados en clasificación	Consulta Panel Programas actualmente bloqueados en clasificación en la página 710.
Programas bloqueados por el administrador	Consulta Programas bloqueados por el administrador en la página 520.
Actividad de pups	Consulta Actividad de malware / PUP en la página 613.
Actividad de exploits	Consulta Actividad de exploits en la página 615.
Parches disponibles	Consulta Parches disponibles en la página 407.
Evolución de los parches disponibles	Consulta Evolución de los parches disponibles en la página 404.
Programas "End of life"	Consulta Programas "End of life" en la página 402.
Indicadores de ataque (IOA) detectados	Consulta Indicadores de ataque (IOA) detectados en la página 598.
Evolución de las detecciones	Consulta Evolución de las detecciones en la página 594.

Tabla 8.31: Listado de widgets disponibles en la sección Detecciones

Sección Investigación (5)

Muestra la telemetría recogida en el equipo para que el administrador pueda investigar el origen de los ataques y su alcance.



Para conocer el significado de los campos que forman parte de la telemetría, consulta [Formato de los eventos recogidos en la telemetría en la página 867](#).

Para visualizar la telemetría, el administrador dispone de las herramientas siguientes:

- **Consola de investigación**
- **Consultas avanzadas SQL**
- **Grafos**

El administrador puede utilizar una o varias herramientas. La barra de pestañas aloja las herramientas utilizadas en la sesión. Al hacer clic en la pestaña **Investigación**, la consola añade automáticamente la herramienta **Consola de investigación** en el equipo gestionado. Para cambiar de herramienta, haz clic en la pestaña correspondiente. Para añadir una nueva herramienta, haz clic en el icono .

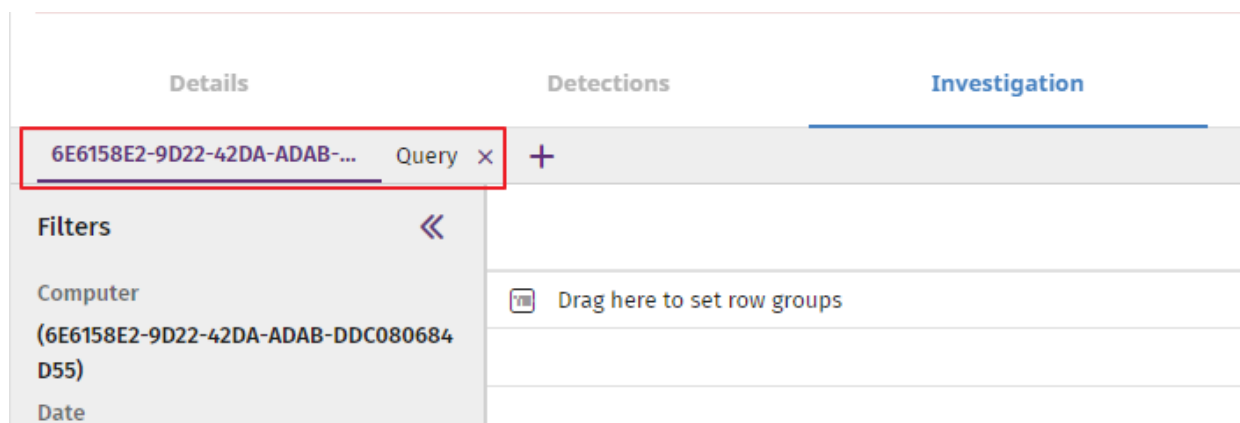


Figura 8.9: Barra de pestañas con las herramientas Consola de investigación y Consultas avanzadas SQL abiertas

Consola de investigación

La consola de investigación de Cytomic Orion muestra un listado con todos los eventos registrados en el equipo durante el intervalo de 1 día. El administrador puede cambiar la fecha de inicio del intervalo hasta 7 días atrás, para acceder a la telemetría registrada en días anteriores.



Para obtener información sobre la consola de investigación de Cytomic Orion consulta [Estructura de la consola de investigación](#).

Abrir una nueva consola de investigación

Conforme la investigación del administrador progresa, es posible que necesite abrir otras consolas de investigación sobre distintos equipos de la red [Esquema de base de datos](#)

Para crear una nueva consola de investigación:

- Haz clic en la pestaña **Investigación** del equipo seleccionado. Se abrirá la consola de Cytomic Orion.
- Haz clic en el icono . Se mostrará el menú de contexto.
- Selecciona **Investigación de equipos**. Se abrirá la ventana **Investigar equipo**.

Investigate computer

☒ MUID ☐ MD5 ☐ MUID + MD5 ☐ Computer name



From





To





Time zone



OK

Cancel

Figura 8.10: Ventana de selección del nuevo equipo a investigar

- Para investigar todos los eventos de un equipo en un día:
 - Selecciona **MUID** o **Nombre de equipo** (la herramienta de consultas avanzadas SQL trabaja con MUIDs. Consulta [Identificadores de dispositivos \(MUID\)](#)).
 - Escribe en la caja de texto el **Nombre de equipo** o el **MUID**.
 - Elige el intervalo de tiempo que la consola de investigación utilizará para recuperar datos del océano de eventos. El administrador puede cambiar la fecha de inicio del intervalo hasta 7 días atrás para acceder a la telemetría registrada en días anteriores. El mayor intervalo soportado es de 1 día.
 - Establece la zona horaria del intervalo.
 - Haz clic en el botón **OK**. Se añadirá una nueva pestaña con la consola de investigación configurada para mostrar la telemetría del equipo seleccionado.
- Para investigar un fichero si no conoces el equipo que lo contiene:

- Selecciona **MD5** y escribe en la caja de texto el **MD5**.
- Haz clic en el botón **OK**. Se añadirá una nueva pestaña con la consola de investigación mostrando dos paneles.
- En el panel de la izquierda, selecciona el equipo que quieres investigar. El panel de la derecha mostrará todos los eventos relacionados con ese fichero en el equipo.
- Para investigar un fichero si conoces el equipo que lo contiene:
 - Selecciona **MUID + MD5** y escribe el **MUID** del equipo y el **MD5** del fichero en las cajas de texto.
 - Haz clic en el botón **OK**. Se abrirá la consola de investigación con los eventos que involucran al fichero en el equipo.

Consultas avanzadas SQL

El administrador puede navegar por el océano de datos para localizar mediante su MUID eventos específicos del equipo seleccionado, o de cualquier otro que pertenezca a la red administrada. Con la herramienta de consultas avanzadas SQL, el administrador puede acceder a la telemetría registrada en el día actual y en los 7 días previos. Para ello es necesario utilizar el lenguaje SQL y conocer el esquema de base de datos utilizado. Consulta [Esquema de base de datos](#)

Para acceder a la herramienta de consultas avanzadas SQL:

- Haz clic en la pestaña **Investigación** del equipo seleccionado. Se abrirá la consola de investigación de Cytomic Orion.
- Haz clic en el icono . Se mostrará el menú de contexto.
- Selecciona **Consulta avanzada SQL**. Se abrirá la herramienta de consultas avanzadas SQL.

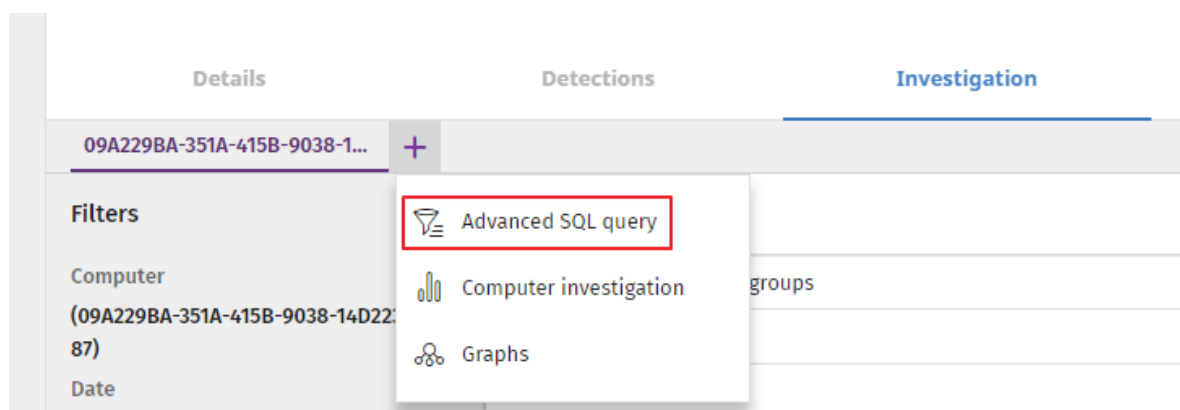


Figura 8.11: Menú desplegable Investigación

Para obtener información sobre cómo utilizar la herramienta de consultas avanzadas SQL, consulta [Módulo de consultas avanzadas SQL](#).



Algunas funcionalidades de la herramienta de consultas avanzadas SQL solo están disponibles para los clientes que acceden directamente a ella a través de la consola de Cytomic Orion.

Para conocer la sintaxis de la variante del lenguaje SQL utilizado en Cytomic Orion, consulta [Sintaxis SQL del módulo Consultas avanzadas](#).

Esquema de base de datos

Cuando el administrador accede a la herramienta de consultas avanzadas SQL desde Advanced EDR, los eventos registrados en el equipo se almacenan en dos tablas:

- **Telemetry:** almacena la telemetría registrada en los equipos.
- **Indicators:** contiene los indicios registrados en los equipos. Los registros se muestran agrupados. Para conocer el algoritmo de agrupación consulta [Agrupación de indicios](#).

El campo **EventType** de la tabla **Telemetry** es un enumerado que indica el tipo de evento almacenado en la fila correspondiente. Para conocer todos los tipos de eventos, consulta [Formato de los eventos recogidos en la telemetría](#) en la página 867.

Identificadores de dispositivos (MUID)

La herramienta de consultas avanzadas muestra los eventos del océano de datos tal y como se almacenan en la base de datos. Algunas tablas almacenan las referencias a los equipos de la red utilizando su MUID (Machine Universal Identifier). Para obtener el nombre del equipo que corresponde a un MUID, busca el MUID en la consola de Advanced EDR. Consulta [Equipos](#).

Grafos

Esta herramienta utiliza un diagrama de grafos para representar de forma gráfica mediante nodos y flechas los procesos involucrados en el análisis del administrador y sus relaciones. La información mostrada en un diagrama de grafos es equivalente a la incluida en la consola de investigación o en las consultas avanzadas, pero ordenada y presentada de forma más clara y fácil de interpretar para el administrador.

Abrir un diagrama de grafos

- Haz clic en la pestaña **Investigación** del equipo seleccionado. Se abrirá la consola de investigación de Cytomic Orion.
- Haz clic en el icono . Se mostrará el menú de contexto.
- Selecciona **Grafos**. Se abrirá la ventana **Nueva Investigación gráfica** con el listado de plantillas de grafos definidas.
- Selecciona una plantilla según el tipo de datos a mostrar en el diagrama. Para conocer las plantillas disponibles consulta [Información contenida en diagramas de grafos](#). Si la plantilla requiere parámetros, se mostrará una ventana de tipo formulario para introducirlos.

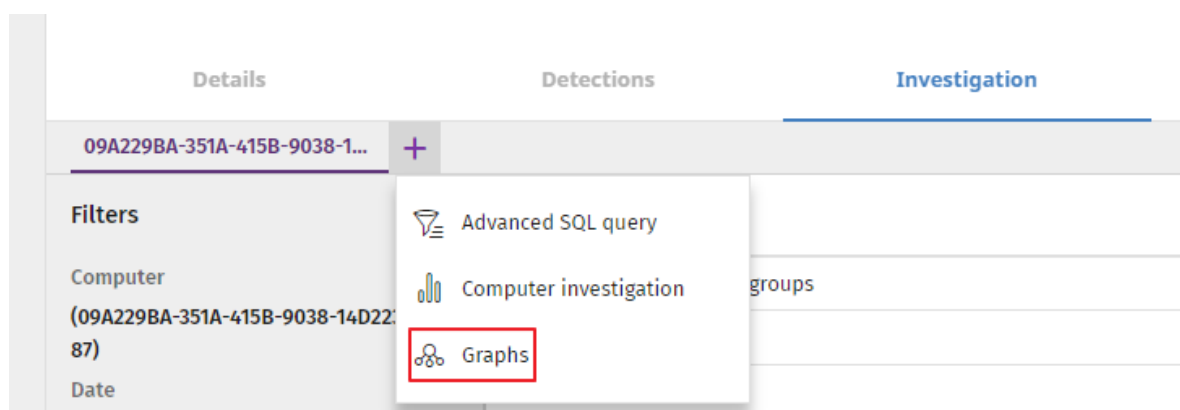
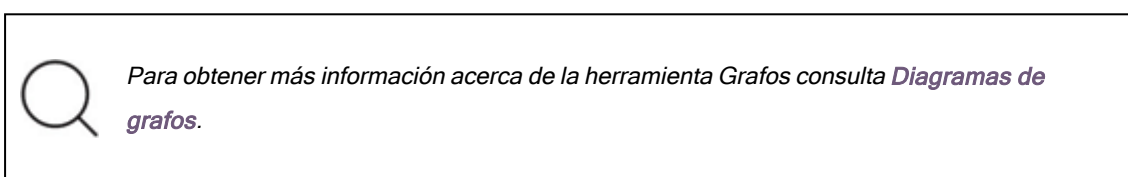


Figura 8.12: Menú desplegable Investigación



Conexiones monitorizadas (6)

Acceso al listado

Para acceder al listado:

- Selecciona el menú superior **Equipos**.
- En el árbol de equipos, haz clic en el grupo que contiene equipos con la configuración Control de Acceso a Endpoints activada.
- En el listado de equipos, haz clic en uno de los equipos, y selecciona la pestaña **Conexiones monitorizadas**.

Permisos requeridos

Permiso	Acceso a listados
Visualizar detecciones y amenazas	Conexiones monitorizadas

Tabla 8.32: Permisos requeridos para acceder al listado Conexiones monitorizadas

Conexiones monitorizadas

El listado contiene información sobre las conexiones entrantes detectadas en el equipo, que cumplen las condiciones configuradas en la política de Control de Acceso a Endpoints. Consulta [Configuración de Control de Acceso a Endpoints](#) en la página 458



Para más información sobre los datos del listado, consulta [Listados del módulo Control de Acceso a Endpoints](#) en la página 472.

Sección Hardware (7)

Contiene información sobre los recursos hardware instalados en el equipo:

Campo	Descripción	Valores
CPU	Información del microprocesador instalado en el equipo y serie temporal con el consumo de CPU en diferentes periodos e intervalos según la selección del desplegable.	• Intervalos de 5 minutos para la última hora. • Intervalos de 10 minutos para las 3 últimas horas. • Intervalos de 40 minutos para las últimas 24 horas.
Memoria	Información sobre las características de los chips de memoria instalados y serie temporal con el consumo de memoria en diferentes periodos e intervalos según la selección del desplegable.	• Intervalos de 5 minutos para la última hora. • Intervalos de 10 minutos para las 3 últimas horas. • Intervalos de 40 minutos para las últimas 24 horas.
Disco	Información sobre las características del sistema de almacenamiento masivo y un gráfico de tarta con el porcentaje de espacio libre y ocupado en el momento de la consulta.	• ID de dispositivo • Tamaño • Tipo • Particiones • Revisión de firmware • Número de serie • Nombre
BIOS	Información sobre la versión de la BIOS instalada en el equipo.	• Versión • Fecha de fabricación

Campo	Descripción	Valores
		- Número de serie - Nombre - Fabricante
TPM	Información del chip de seguridad integrado en la placa base del equipo. Para poder ser utilizado por Advanced EDR el TPM debe de estar activado, habilitado y ser propietario.	Versión del fabricante: versión interna del chip. Versión de especificación: versiones de las APIs compatibles. - Versión - Fabricante Activado: el TPM está preparado para recibir comandos. Se utiliza en sistemas con varios TPMs. Habilitado: el TPM esta preparado para funcionar ya que ha sido activado desde la BIOS. Propietario: el sistema operativo puede interactuar con el TPM.

Tabla 8.33: Campos de la sección hardware de la información del equipo

Sección Software (8)

Contiene información del software instalado en el equipo, de las actualizaciones del sistema operativo Windows y un histórico de sus movimientos.

Herramienta de búsqueda

Introduce el nombre o editor en la caja de texto **Buscar** y presiona la tecla Enter para efectuar una búsqueda. A continuación se muestra la información del software encontrado:

Campo	Descripción
Nombre	Nombre del programa instalado.
Editor	Empresa que desarrolló el programa.
Fecha de instalación	Fecha en la que se instaló el programa por última vez.
Tamaño	Tamaño del programa instalado.
Versión	Versión interna del programa instalado.

Tabla 8.34: Campos de la sección software de la información del equipo

- Para limitar la búsqueda selecciona en el desplegable el tipo de software que se mostrará:
 - Solo programas
 - Solo actualizaciones
 - Todo el software

Instalaciones y desinstalaciones

- Haz clic en el link **Instalaciones y desinstalaciones** para mostrar un histórico de los cambios efectuados en el equipo:

Campo	Descripción
Evento	•  Software desinstalado en el equipo. •  Software instalado en el equipo.
Nombre	Nombre del programa instalado.
Editor	Empresa que desarrolló el programa.
Fecha	Fecha en la que se instaló o desinstaló el programa.
Versión	Versión interna del programa instalado.

Tabla 8.35: Campos de la sección Instalaciones y desinstalaciones

Sección Configuración (9)

Muestra toda la información relevante de la asignación de configuraciones al equipo, y permite su gestión y modificación:

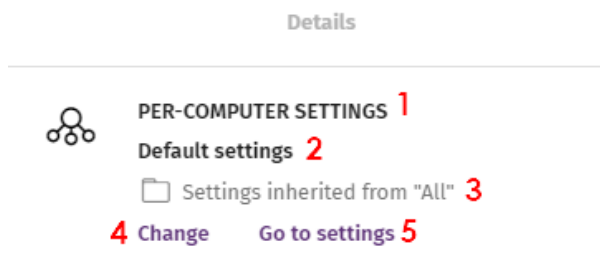


Figura 8.13: Ejemplo de asignación heredada y manual

- (1) **Nombre de la categoría de la configuración:** indica el tipo de configuración. Consulta [Introducción a las clases de configuraciones](#) en la página 253 para conocer los distintos tipos de configuraciones disponibles en Advanced EDR.
- (2) **Nombre de la configuración asignada.**
- (3) **Método de asignación de la configuración:** directamente al equipo o heredada de un grupo superior.
- (4) **Botón para cambiar la asignación de la configuración.**
- (5) **Botón para editar el contenido de la configuración.**



Consulta [Crear y gestionar configuraciones](#) en la página 258 para crear, editar y modificar perfiles de configuración.

Barra de acciones (10)

Recurso que agrupa múltiples operaciones disponibles para aplicar sobre los equipo administrados:

Acción	Descripción
Mover a	Mueve el equipo a un grupo estándar.
Mover a su ruta de Active Directory	Mueve el equipo a su grupo Directorio Activo original.
Eliminar	Libera la licencia de Advanced EDR y elimina el equipo de la consola Web.

Acción	Descripción
 Desinfectar	Programa una tarea de desinfección de ejecución inmediata.
 Aislar equipo	Impide las comunicaciones con el exterior para facilitar las tareas de análisis forense remoto al administrador, en el caso de que el equipo haya sido comprometido. Consulta Aislar uno o varios equipos de la red de la organización en la página 805 para más información.
 Dejar de aislar equipo	Restaura las comunicaciones con el exterior. Consulta Quitar el aislamiento de un equipo en la página 805 para más información.
 Visualizar parches disponibles	Abre el listado Parches disponibles con los parches pendientes de instalación en el equipo. Consulta Listados del módulo Cytomic Patch en la página 416 .
 Programar instalación de parches	Crea una tarea que instalará los parches publicados y no aplicados en el equipo. Consulta Descargar e instalar parches en la página 382 para más información.
 Control remoto	Inicia las herramientas de control remoto. Consulta Control remoto de los equipos en la página 807 .
 Reiniciar	Reinicia el equipo de forma inmediata. Consulta Reiniciar equipos en la página 803 para más información.
 Reinstalar la protección (requiere reinicio)	Reinstala la protección en caso de mal funcionamiento. Consulta Reinstalación remota en la página 153 .
 Reinstalar agente	Reinstala el agente en caso de mal funcionamiento. Consulta Reinstalación remota en la página 153 .
Notificar un problema	Abre un ticket de mantenimiento con el departamento técnico de Cytomic. Consulta Notificar un problema en la página 821 para más información.

Tabla 8.36: Acciones disponibles en la ventana de información del equipo

Iconos ocultos (11)

Dependiendo del tamaño de la ventana y del número de iconos a mostrar, parte de ellos pueden quedar ocultos bajo el icono . Haz clic para desplegar el menú con los iconos restantes.

Capítulo 9

Gestión de configuraciones

Las configuraciones, también llamadas “perfiles de configuración” o simplemente “perfiles”, ofrecen a los administradores un modo rápido de establecer los parámetros de seguridad y conectividad gestionados por Advanced EDR en los equipos que administran.

Contenido del capítulo

Estrategias para crear la estructura de configuraciones	252
Visión general para asignar configuraciones a equipos	252
Introducción a las clases de configuraciones	253
Perfiles de configuración modulares vs monolíticos	256
Crear y gestionar configuraciones	258
Asignación manual y automática de configuraciones	261
Asignación directa / manual de configuraciones	261
Asignación indirecta de configuraciones: las dos reglas de la herencia	263
Límites de la herencia	264
Sobre-escritura de configuraciones	265
Movimiento de grupos y equipos	267
Excepciones a la herencia indirecta	268
Configuraciones recibidas desde el partner	268
Características de las configuraciones enviadas por el partner	269
Requisitos	269
Visualizar las configuraciones asignadas	269

Estrategias para crear la estructura de configuraciones

El administrador de la red creará tantos perfiles como variaciones de configuraciones sean necesarias para gestionar la seguridad de la red. Se genera una nueva configuración por cada grupo de equipos con necesidades de protección similares:

- Equipos de usuario utilizados por personas con distintos niveles de conocimientos en informática requieren configuraciones más o menos estrictas frente a la ejecución de software.
- Usuarios que desempeñan diferentes tareas tienen diferentes usos y necesidades, y por tanto requerirán de configuraciones que permitan el acceso a diferentes recursos.
- Usuarios que manejan información confidencial o delicada para la empresa requieren un nivel de protección superior frente a amenazas e intentos de robo de la propiedad intelectual de la compañía.
- Equipos en distintas delegaciones requieren configuraciones distintas que les permitan conectarse a Internet utilizando diferentes infraestructuras de comunicaciones.
- Servidores críticos para el funcionamiento de la empresa requieren configuraciones de seguridad específicas.

Visión general para asignar configuraciones a equipos

La asignación de configuraciones a los equipos de la red es un proceso de cuatro pasos:

1. Crear los grupos que reúnan equipos del mismo tipo o con idénticos requisitos de conectividad y seguridad.
2. Asignar los equipos de la red a su grupo correspondiente.
3. Asignar los distintos tipos de configuraciones a los grupos creados.
4. Difundir las configuraciones a todos los equipos de la red.

Todas estas operaciones se realizan desde el árbol de grupos, accesible desde el menú superior **Equipos**. El árbol de grupos es la herramienta principal para asignar configuraciones de forma rápida y sobre conjuntos amplios de equipos.

Por lo tanto, la estrategia principal del administrador consiste en reunir todos los equipos similares en un mismo grupo y crear tantos grupos como conjuntos diferentes de equipos existan en la red que gestiona.



*Para obtener más información sobre el manejo del árbol de grupos y asignación de equipos a grupos consulta **El panel Árbol de equipos** en la página 179.*

Difusión inmediata de la configuración

Una vez que una configuración es asignada a un grupo, esa configuración se aplicará a los equipos del grupo de forma inmediata y automática, siguiendo las reglas de la herencia mostradas en [Asignación indirecta de configuraciones: las dos reglas de la herencia](#). La configuración así establecida se aplica a los equipos sin retardos, en cuestión de unos pocos segundos.



Para desactivar la difusión inmediata de la configuración consulta [Configuración de la comunicación en tiempo real](#) en la página 281.

Árbol multinivel

En empresas de tamaño mediano y grande, la variedad de configuraciones puede ser muy alta. Para facilitar la gestión de parques informáticos grandes, Advanced EDR permite generar árboles de grupos de varios niveles para que el administrador pueda gestionar los equipos de la red con la suficiente flexibilidad.

Herencia

En redes de tamaño amplio es muy probable que el administrador quiera reutilizar configuraciones ya establecidas en grupos de orden superior dentro del árbol de grupos. El mecanismo de herencia permite asignar una configuración sobre un grupo y, de forma automática, sobre todos los grupos que dependen de éste, ahorrando tiempo de gestión.

Configuraciones manuales

Para evitar la propagación de configuraciones en todos los niveles inferiores de una rama del árbol, o asignar una configuración distinta a la recibida mediante la herencia sobre un determinado equipo dentro de una rama, es posible asignar de forma manual configuraciones a equipos individuales o a grupos.

Configuración por defecto

Inicialmente todos los equipos en el árbol de grupos heredan la configuración establecida en el nodo raíz **Todos**. Este nodo tiene asignadas las configuraciones por defecto creadas en Advanced EDR para proteger a los equipos desde el primer momento, incluso antes de que el administrador haya accedido a la consola para establecer una configuración de seguridad.

Introducción a las clases de configuraciones

Advanced EDR distribuye la configuración a aplicar en los equipos administrados a lo largo de varias clases de perfiles, cada una de las cuales cubre un área concreta de la seguridad.

A continuación se muestra una introducción a cada una de las clases soportadas en Advanced EDR:

Advanced EDR permite configurar los siguientes aspectos del servicio:

Configuración	Descripción
Usuarios	Gestiona las cuentas que podrán acceder a la consola de administración, así como las acciones permitidas dentro de ella (roles) y su actividad. Para más información, consulta Acceso, control y supervisión de la consola de administración en la página 59.
Ajustes por equipo	Define las plantillas de configuración donde se indica cada cuánto se actualizará el software de seguridad Advanced EDR instalado en los equipos de usuario y servidores. También establece la configuración global frente a manipulaciones externas y desinstalaciones no autorizadas. Para más información, consulta Configuración remota del agente en la página 271.
Control remoto	Define plantillas de configuración que establecen el acceso al equipo del usuario desde el producto de threat hunting Cytomic Orion. Para más información, consulta Control remoto de los equipos en la página 807.
Configuración de red	Define plantillas de configuración que establecen el idioma del software Advanced EDR instalado en los equipos de usuario y servidores, y el tipo de conexión que se utilizará para conectar con la nube de Cytomic. Para más información, consulta Configuración remota del agente en la página 271.
Servicios de red	Define el comportamiento del software Advanced EDR en lo referente a la comunicación con los equipos vecinos de la red del cliente: • Proxy: define de forma global los equipos que realizarán tareas de proxy para facilitar el acceso a la nube de equipos con Advanced EDR instalado y aislados de la red. Para más información, consulta Rol de Proxy Cytomic en la página 272. • Caché: define de forma global los repositorios de ficheros de firmas, parches de seguridad y componentes utilizados para actualizar el software Advanced EDR instalado en los equipos de la red. Para más información, consulta Rol de caché en la página 274. • Descubrimiento: define de forma global los equipos de la red encargados de rastrear la aparición de dispositivos sin proteger. Para más información, consulta Rol de descubridor en la página 276.
Entornos DVI	Define el número de equipos alojados en infraestructuras de virtualización no persistentes para facilitar la asignación de licencias.
Mis Alertas	Establece el tipo de alertas que el administrador recibirá en su buzón de

Configuración	Descripción
	correo. Para más información, consulta Alertas en la página 775.
Estaciones y servidores	Define plantillas de configuración que establecen el comportamiento de Advanced EDR para proteger a los equipos de la red frente a las amenazas y el malware. Para más información, consulta Configuración de la seguridad en estaciones y servidores en la página 291.
Galería de IOCs	Define planillas para importar y exportar IOCs en el producto y buscar en los equipos protegidos indicadores de compromiso. Para más información, consulta Gestión y detección de IOCs en la página 531.
Indicadores de ataque (IOA)	Define plantillas para detectar estrategias sofisticadas de infección, que utilizan por lo general múltiples vectores de ataque y herramientas del sistema operativo en periodos alargados de tiempo. Para más información, consulta Configuración de indicadores de ataque en la página 553.
Bloqueo de programas	Define plantillas de configuración que establecen el comportamiento de Advanced EDR para bloquear la ejecución de programas. Para más información, consulta Configuración del bloqueo de programas en la página 517.
Software autorizado	Define plantillas para evitar el bloqueo de los programas desconocidos en clasificación. Para más información, consulta Configuración de software autorizado en la página 525.
Gestión de parches	Define las plantillas de configuración que establecen el comportamiento del descubrimiento de nuevos parches de seguridad publicados por los proveedores de software y del sistema operativo Windows. Para más información, consulta Cytomic Patch (Actualización de programas vulnerables) en la página 375.
Control de Acceso a Endpoints	Monitoriza las conexiones entrantes recibidas en los equipos de la red corporativa, y las autoriza o bloquea según las condiciones de seguridad que reúne el equipo origen de la conexión. Para mas información, consulta Configuración de Control de Acceso a Endpoints en la página 458
Cytomic Data Watch	Define las plantillas de configuración que permiten realizar un seguimiento de la información personal contenida en los sistemas de almacenamiento. Para más información, consulta Cytomic Data Watch (Supervisión de información

Configuración	Descripción
	sensible) en la página 311.
Cifrado	Define las plantillas de configuración que permiten cifrar el contenido de los dispositivos de almacenamiento interno. Para más información, consulta Cytomic Encryption(Cifrado de dispositivos) en la página 481.
MDR	Describe la infraestructura de IT del cliente que el partner deberá monitorizar y proteger de los ataques de malware y amenazas externas. Esta configuración solo es accesible si el cliente tiene contratado el servicio MDR con su partner. Para obtener más información consulta Configuración del servicio MDR en la página 603.

Tabla 9.1: Descripción de las configuraciones disponibles en Advanced EDR

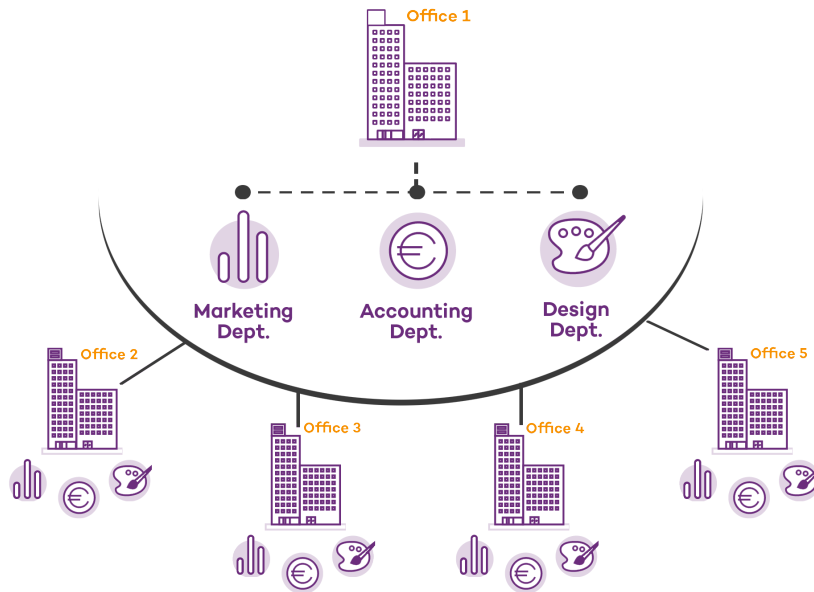
Perfiles de configuración modulares vs monolíticos

Con el soporte de las distintas clases de perfiles, Advanced EDR adopta un enfoque modular para crear y distribuir las configuraciones a aplicar en los equipos administrados. El objetivo de utilizar perfiles modulares y no un único perfil de configuración monolítico que abarque toda la configuración es el de reducir el número de perfiles distintos que el administrador tendría que manejar en la consola y así minimizar el tiempo de gestión. El enfoque modular permite generar configuraciones más pequeñas y ligeras, frente a perfiles monolíticos que fomentan la aparición de muchos perfiles de configuración muy largos y redundantes, con muy pocas diferencias entre sí.

Caso práctico: Creación de configuraciones para varias delegaciones

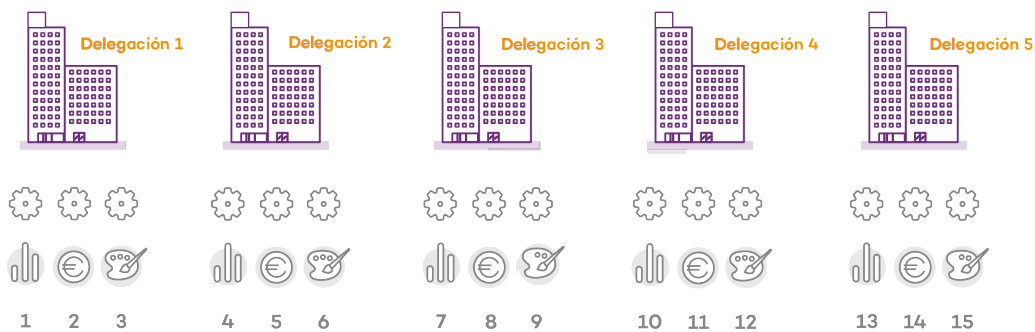
En este caso práctico tenemos una empresa con 5 delegaciones, cada una de ellas tiene una infraestructura de comunicaciones distinta y por tanto una configuración de proxy diferente. Además, dentro de cada delegación se requieren 3 configuraciones de seguridad diferentes, una para el departamento de diseño, otro para el departamento de contabilidad y otra para el departamento de marketing.

Network of a company formed by several offices:



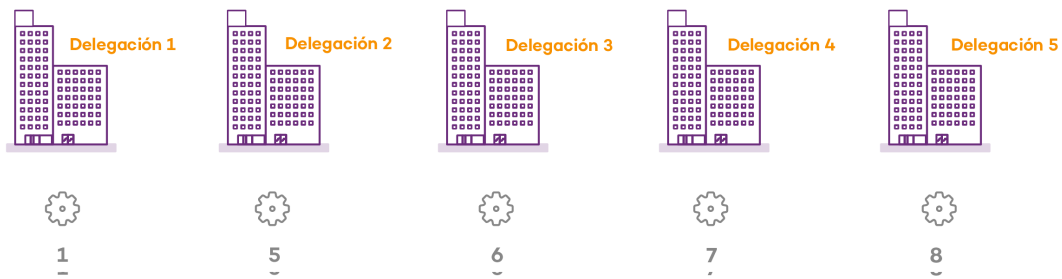
Con un perfil monolítico son necesarios 15 perfiles de configuración distintos (5 oficinas x 3 clases de configuración en cada oficina = 15) para dar servicio a todos los departamentos de todas las delegaciones de la empresa.

Perfil monolítico

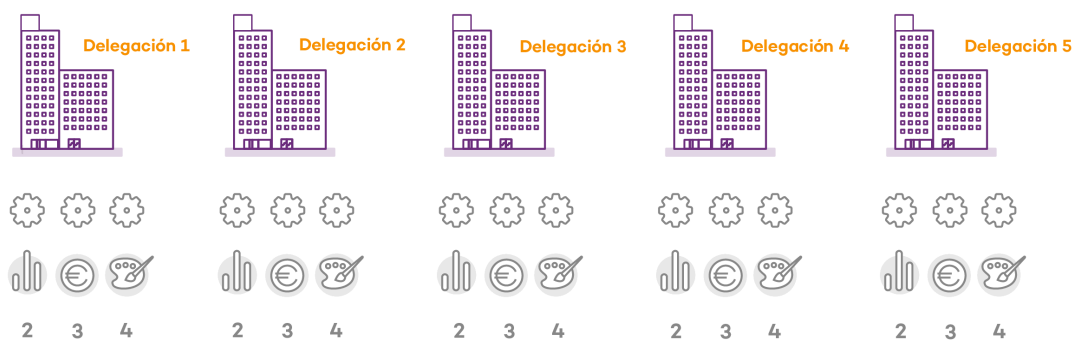


Como Advanced EDR separa la configuración de proxy de la de seguridad, el número de perfiles a crear se reduce (5 perfiles de proxy + 3 perfiles de departamento = 8) ya que los perfiles de seguridad por departamento de una delegación se pueden reutilizar y combinar con los perfiles de proxy en otras delegaciones.

Perfil modular Proxy e idioma



Perfil modular Seguridad



Crear y gestionar configuraciones

Haz clic en el menú superior **Configuración** para crear, copiar y borrar configuraciones.

En el panel de la izquierda se encuentran las entradas correspondientes a las clases de configuraciones posibles (1). En el panel de la derecha se muestran los perfiles de configuración ya creados (2) de la clase seleccionada y los botones para añadir (3), copiar (4) y eliminar configuraciones (5). Utiliza la barra de búsqueda (6) para localizar los perfiles ya creados de forma rápida.

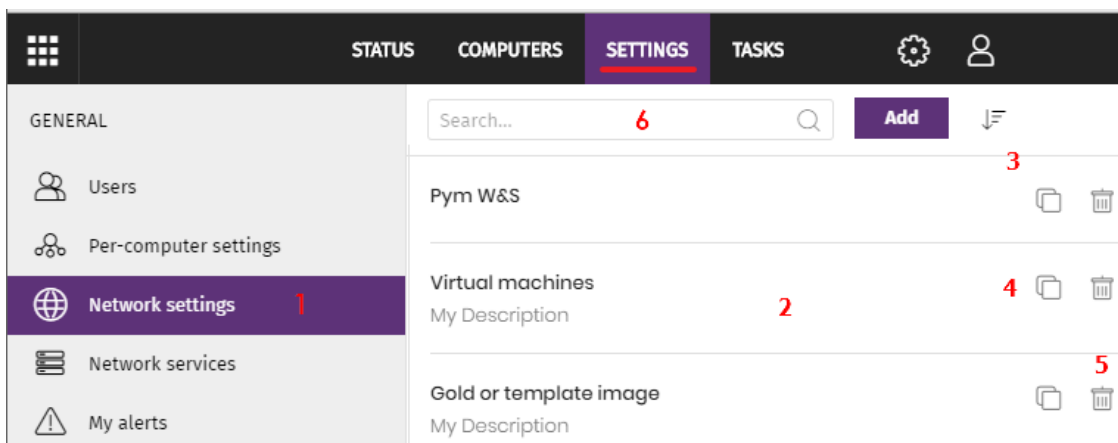


Figura 9.1: Pantalla para crear y gestionar configuraciones

 Las configuraciones creadas desde CYTOMIC Nexus, se muestran con la etiqueta en verde CYTOMIC Nexus. Al posicionarse sobre ella se muestra el mensaje: “Esta configuración está gestionada desde CYTOMIC Nexus”. Las configuraciones creadas desde CYTOMIC Nexus son de sólo lectura, y únicamente permiten cambiar los destinatarios. Para más información, consulta la sección Configuraciones para productos basados en Cytomic, en el manual de CYTOMIC Nexus.

Crear configuraciones

Haz clic sobre el botón **Añadir** para mostrar la ventana de creación de configuraciones. Todos los perfiles tienen un nombre principal y una descripción que se muestran en los listados de configuraciones.

Para crear una configuración ten en cuenta las limitaciones de permisos y visibilidad siguientes:

- Para crear una configuración es necesario que la cuenta de usuario tenga el permiso correspondiente asociado. Consulta [Descripción de los permisos implementados](#) en la página 70.
- Para asignar destinatarios a una configuración, la cuenta de usuario tiene que tener visibilidad sobre los equipos a asignar. Consulta [Gestión de roles y permisos](#) en la página 67.

Listar y ordenar configuraciones

Para visualizar las configuraciones de un tipo determinado, la cuenta de usuario tiene que tener el al menos permiso de lectura correspondiente asociado. Consulta [Descripción de los permisos implementados](#) en la página 70.

Haz clic en el icono  (7) para desplegar un menú de contexto con las opciones de ordenación disponibles:

- Ordenado por fecha de creación
- Ordenado por nombre
- Ascendente
- Descendente

Copiar configuraciones

Para copiar una configuración haz clic en el icono **(4)**. Se copiará toda la configuración excepto el campo **Destinatarios**, que se dejará vacío.

Para copiar una configuración es necesario que la cuenta de usuario tenga el permiso de modificar correspondiente asociado. Consulta [Descripción de los permisos implementados](#) en la página 70.

Editar configuraciones



Antes de modificar un perfil comprueba que la nueva configuración sea correcta ya que, si el perfil ya está asignado a equipos de la red, esta nueva configuración se propagará y aplicará de forma automática y sin retardos.

- Haz clic en la configuración para editarla. Se abrirá la página **Editar configuración**.
- Para guardar los cambios haz clic en el botón **Guardar**.

Para modificar una configuración ten en cuenta las limitaciones de permisos y visibilidad siguientes:

- Es necesario que la cuenta de usuario tenga el permiso de modificar correspondiente asociado. Consulta [Descripción de los permisos implementados](#) en la página 70.
- Para añadir un destinatario a la configuración es necesario que la cuenta de usuario tenga visibilidad sobre el equipo. Consulta [Gestión de roles y permisos](#) en la página 67.
- Para eliminar un destinatario es necesario que la cuenta de usuario tenga visibilidad sobre ese destinatario. Consulta [Gestión de roles y permisos](#) en la página 67.

Borrar configuraciones

Para borrar una configuración haz clic en el icono **(5)**. Si el perfil ya ha sido asignado a uno o más equipos se impedirá su borrado hasta que se libere la asignación.

Para borrar una configuración es necesario que la cuenta de usuario tenga el permiso correspondiente asociado. Consulta [Descripción de los permisos implementados](#) en la página 70.

Asignación manual y automática de configuraciones

Una vez creados los perfiles de configuración, éstos pueden ser asignados a los equipos de la red siguiendo dos estrategias diferentes:

- Mediante asignación manual (asignación directa).
- Mediante asignación automática a través de la herencia (asignación indirecta).

Ambas estrategias son complementarias y es muy recomendable que el administrador comprenda las ventajas y limitaciones de cada mecanismo para poder definir una estructura de equipos lo más simple y flexible posible, con el objetivo de minimizar las tareas de mantenimiento diarias.

Asignación directa / manual de configuraciones

Consiste en establecer de forma directa los perfiles de configuración a equipos o grupos. De esta manera es el administrador el que, de forma manual, asigna una configuración a un grupo o equipo.

Una vez creados los perfiles de configuración, estos se asignan de tres maneras posibles:

- Desde el menú superior **Equipos**, en el árbol de grupos mostrado en el panel de la izquierda.
- Desde el detalle del equipo en el panel de listado de equipos, accesible desde el menú superior **Equipos**.
- Desde el propio perfil de configuración creado o editado.



Para obtener más información sobre el árbol de grupos consulta [Árbol de grupos](#) en la página 188

Desde el árbol de grupos

Para asignar un perfil de configuración a un conjunto de equipos que pertenecen a un grupo:

- Haz clic en el menú superior **Equipos** y selecciona el árbol de grupos en el panel izquierdo.
- Haz clic en el menú contextual en la rama apropiada del árbol de grupos.
- Haz clic en el menú emergente **Configuraciones**, se mostrará una ventana con el nombre de los perfiles ya asignados al grupo seleccionado, separados por su clase, y el tipo de asignación:
- **Manual / Asignación directa:** mediante la leyenda **Asignada directamente a este grupo**.
- **Heredada / Asignación indirecta:** mediante la leyenda **Configuración heredada de** y el nombre del grupo del cual se hereda la configuración, junto con la ruta completa para llegar al mismo.

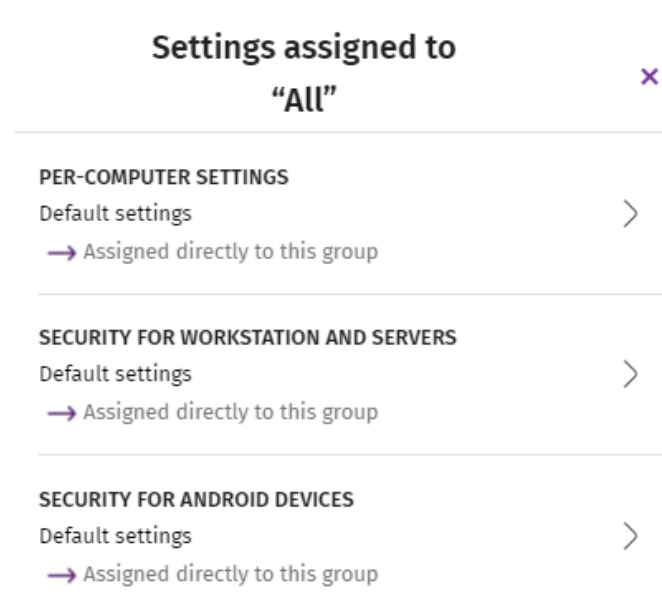


Figura 9.2: Ejemplo de asignación heredada y manual

Haz clic en una de las clases disponibles, selecciona la nueva configuración y haz clic en **Aceptar** para asignar la configuración al grupo. La configuración se propagará de forma inmediata a todos los equipos miembros del grupo y sus descendientes.

Desde el panel listado de equipos

Para asignar un perfil de configuración a un equipo concreto:

- En el menú superior **Equipos** haz clic en el grupo o filtro donde reside el equipo a asignar la configuración. Haz clic sobre el equipo en la lista de equipos mostrada en el panel derecho para ver la pantalla detalles de equipo.
- Haz clic en la pestaña **Configuración**. Se mostrarán los perfiles asignados al equipo separados por su clase, y el tipo de asignación:
 - **Manual / Asignación directa:** mediante la leyenda **Asignada directamente a este grupo**.
 - **Heredada / Asignación indirecta:** mediante la leyenda **Configuración heredada de** y el nombre del grupo del cual se hereda la configuración, junto con la ruta completa para llegar al mismo.
- Haz clic en una de las clases disponibles, selecciona la nueva configuración y haz clic en **Aceptar** para asignar la configuración al equipo. La configuración se aplicará de forma inmediata.

Desde el propio perfil de configuración

La forma más rápida de asignar una configuración a varios equipos que pertenecen a grupos distintos es a través del propio perfil de configuración.

Para asignar equipos o grupos de equipos a un perfil de configuración:

- En el menú superior **Configuración**, panel lateral, haz clic en la clase de perfil que quieres asignar.
- Selecciona la configuración a asignar y haz clic en el botón **Destinatarios**. Se mostrará una ventana dividida en dos secciones: **Grupos de equipos y Equipos adicionales**.
- Haz clic en los botones  para añadir equipos individuales o grupos de equipos al perfil de configuración.
- Haz clic en el botón **Atrás**. El perfil quedará asignado a los equipos seleccionados y la nueva configuración se aplicará de forma inmediata.



Al retirar un equipo de la lista de equipos asignados a una configuración, el equipo volverá a heredar las configuraciones asignadas al grupo al que pertenece. La consola de administración resaltará este hecho mostrando una ventana de advertencia antes de aplicar los cambios.

Asignación indirecta de configuraciones: las dos reglas de la herencia

La asignación indirecta de configuraciones se realiza a través del mecanismo de la herencia. Esta funcionalidad permite propagar de forma automática un mismo perfil de configuración a todos los equipos subordinados del nodo sobre el cual se asignó la configuración.

Las reglas que rigen la interacción entre los dos tipos de asignaciones (manuales / directas y automática / herencia) se muestran por orden de prioridad:

Regla de la herencia automática

Un grupo o equipo hereda de forma automática las configuraciones del grupo del cual depende (grupo padre o de orden superior).

La asignación de configuración es manual sobre el grupo padre y todos sus descendientes (equipos y otros grupos con equipos en su interior) reciben la configuración de forma automática.

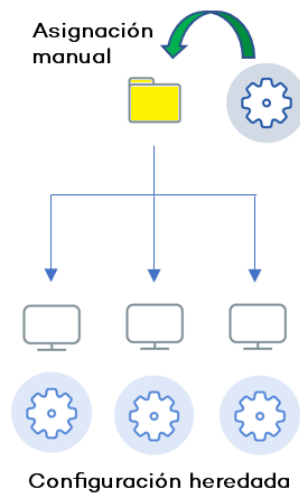


Figura 9.3: Herencia / asignación indirecta

Regla de la prioridad manual

Una configuración manual prevalece sobre una configuración heredada.

Los equipos reciben las configuraciones heredadas por defecto pero si se establece una configuración manual sobre un grupo o equipo, todos sus descendientes recibirán la configuración manual, y no la configuración heredada de orden superior.

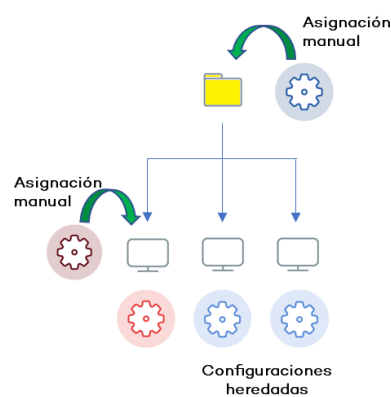


Figura 9.4: Prevalencia de configuración manual sobre heredada

Límites de la herencia

La configuración asignada a un grupo (manual o heredada) se propaga a todos los elementos de la rama del árbol hasta que se encuentra una asignación manual.

Este nodo y todos sus descendientes reciben la configuración manual asignada, y no la establecida en el nodo de orden superior.

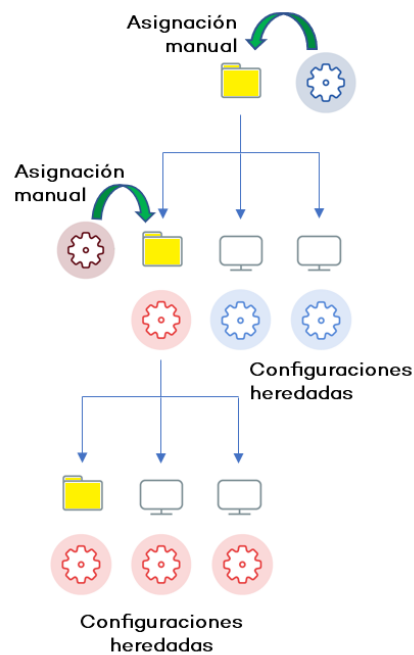


Figura 9.5: Limite de la herencia

Sobre-escritura de configuraciones

La regla de la prioridad manual indica que las configuraciones manuales prevalecen sobre las configuraciones heredadas en un escenario típico donde primero se establece la configuración sobre el nodo de orden superior para que todos sus descendientes la hereden, y posteriormente se asignan de forma manual aquellas configuraciones especiales sobre ciertos nodos de orden inferior.

Sin embargo, es frecuente que una vez establecidas las configuraciones heredadas y manuales, haya un cambio de configuración en un nodo de orden superior. Se distinguen dos casos:

- **No hay configuraciones manuales en los nodos descendientes:** el nodo padre recibe una nueva configuración que se propaga a todos sus nodos descendientes.
- **Sí hay configuraciones manuales en algún nodo descendiente:** el nodo padre recibe una configuración que intenta propagar a todos los nodos descendientes, pero el sistema de herencia no permite asignar una configuración de forma automática sobre un nodo que recibió anteriormente una configuración manual.

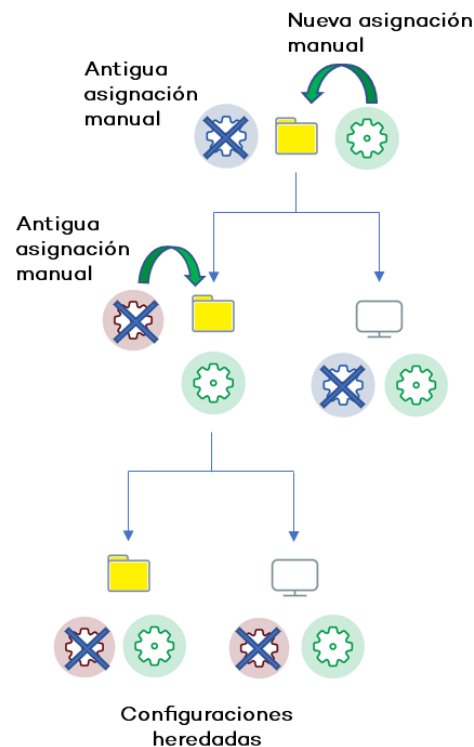


Figura 9.6: Sobre escritura de configuraciones manuales

De esta manera, cuando el sistema detecta un cambio de configuración que tenga que propagar a los nodos subordinados, y alguno de estos tenga una configuración manual (sin importar el nivel en el que se encuentre) se presentará la pantalla de selección, preguntando al administrador sobre el comportamiento a seguir: **Hacer que todos hereden esta configuración** o **Mantener todas las configuraciones**.

Hacer que todos hereden esta configuración



¡Utiliza esta opción con mucho cuidado, esta acción no tiene vuelta atrás! Todas las configuraciones manuales que dependan del nodo padre se perderán y se aplicará la configuración heredada de forma inmediata en los equipos. El comportamiento de Advanced EDR podrá cambiar en muchos equipos de la red

La nueva asignación directa se propaga mediante la herencia a todo el árbol por completo, sobrescribiendo la asignación directa anterior y llegando hasta los nodos hijos de último nivel.

Mantener todas las configuraciones

La nueva configuración solo se propaga a aquellos nodos subordinados que no tengan configuraciones manuales establecidas.

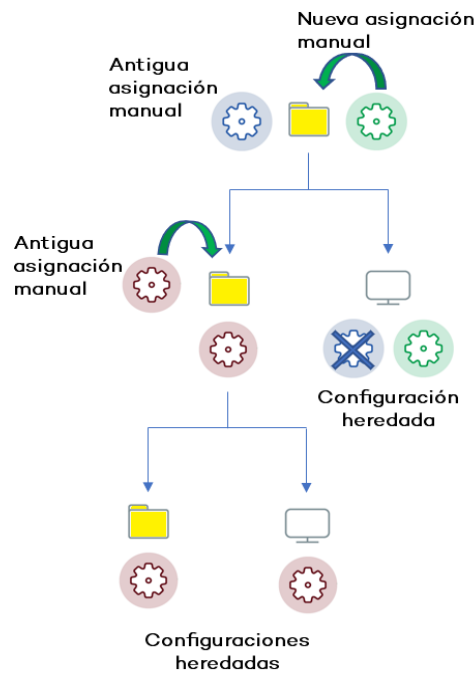


Figura 9.7: Mantener las configuraciones manuales

Si eliges la opción de mantener las configuraciones establecidas de forma manual, la propagación de la nueva configuración heredada se detiene en el primer nodo configurado manualmente.

Eliminar asignaciones manuales y restaurar la herencia

Para eliminar una asignación manual aplicada sobre una carpeta y volver a heredar la configuración de la rama padre:

- En el menú superior **Equipos** haz clic en el grupo que tiene la asignación manual a eliminar, dentro del árbol de grupos situados en el panel izquierdo.
- Haz clic en el icono del menú contextual de la rama apropiada. Se mostrará una ventana emergente con las configuraciones asignadas. Elige el perfil que esté asignado de forma manual y quieres eliminar.
- Se desplegará un listado con todos los perfiles disponibles para realizar una nueva asignación manual, y al final de la lista se mostrará el botón **Heredar del grupo padre** junto con información de la configuración que se heredaría, y el grupo del cual se heredaría.

Movimiento de grupos y equipos

Al mover un equipo o grupo de equipos a otra rama del árbol con una configuración aplicada, el comportamiento de Advanced EDR con respecto a las configuraciones que tomará el equipo o grupo movido varía en función de si se trata de grupos completos o equipos individuales.

Movimiento de equipos individuales

Se respetan las configuraciones manuales establecidas sobre los equipos movidos, y se sobrescriben de forma automática las configuraciones heredadas con las configuraciones establecidas en el nuevo grupo

padre.

Movimiento de grupos

Se muestra una ventana con la pregunta **¿Quieres que las configuraciones asignadas a este grupo mediante herencia, sean sustituidas por las del nuevo grupo padre?**

- En el caso de contestar **SI**, el procedimiento será el mismo que en el movimiento de equipos: las configuraciones manuales se respetan y las heredadas se sobrescriben con las configuraciones establecidas en el grupo padre.
- En el caso de contestar **NO**, las configuraciones manuales se respetan pero las configuraciones heredadas originales del grupo movido prevalece, pasando de esta forma a ser configuraciones manuales.

Excepciones a la herencia indirecta

A los equipos que se integran en la consola Web dentro de un grupo de tipo nativo, Advanced EDR les asigna la configuración de red del grupo de destino mediante el mecanismo estándar de asignación indirecta / herencia. Sin embargo, si un equipo se integra en la consola Web dentro de un grupo de tipo IP o de tipo directorio activo, la asignación de la configuración de red se produce de forma manual. Este cambio en la forma de asignar la configuración de red repercute a su vez en un cambio de comportamiento al mover posteriormente ese equipo de un grupo a otro: ya no heredará de forma indirecta la configuración de red asignada al grupo de destino, sino que conservará la suya propia.

Este comportamiento particular de la herencia, se debe a que en empresas de tamaño medio y grande, el departamento que administra la seguridad puede no ser el mismo que el que administra el directorio activo de la empresa. Por esta razón, un cambio de grupo efectuado por el departamento técnico que mantiene el directorio activo puede desembocar de forma inadvertida en un cambio de configuración de red dentro de la consola de Advanced EDR. Esta situación podría dejar sin conectividad al agente de protección instalado en el equipo y, por lo tanto, en una menor protección. Al asignar de forma manual la configuración de red, se impiden cambios de configuración cuando el equipo cambia de grupo en la consola de Advanced EDR, debido a un cambio de grupo del directorio activo de la empresa.

Configuraciones recibidas desde el partner

Los partners son empresas u organizaciones que tienen como objetivo aprovisionar y gestionar de forma remota las soluciones de seguridad en sus clientes.

Pueden ser de dos tipos:

- Distribuidores que asignan productos a sus clientes y los gestionan de forma remota.
- Compañías que delegan la gestión del servicio de seguridad en cada departamento, pero que además quieren controlar de forma centralizada el cumplimiento de las directrices de protección comunes a toda la empresa.

Para gestionar el software de seguridad de forma remota, los partners envían configuraciones a sus clientes. Estas configuraciones se muestran en la consola de administración con la etiqueta CYTOMIC Nexus .

Características de las configuraciones enviadas por el partner

Las configuraciones enviadas por los partners no son modificables ni se pueden borrar desde la consola de administración. Si el partner autoriza su edición, el administrador podrá modificar ciertos aspectos de la configuración. Para obtener más información consulta [Exclusiones establecidas por el partner](#) en la página 294 y [Software autorizado establecido por el partner](#) en la página 526.

Requisitos

Para recibir las configuraciones enviadas por el partner sigue los pasos mostrados a continuación.

- En el menú superior **Configuración (1)**, selecciona **Usuarios (2)** en el panel lateral izquierdo.
- En la pestaña superior **Usuarios**, activa la opción **Permitir a mi distribuidor acceder a mi consola (3)**.

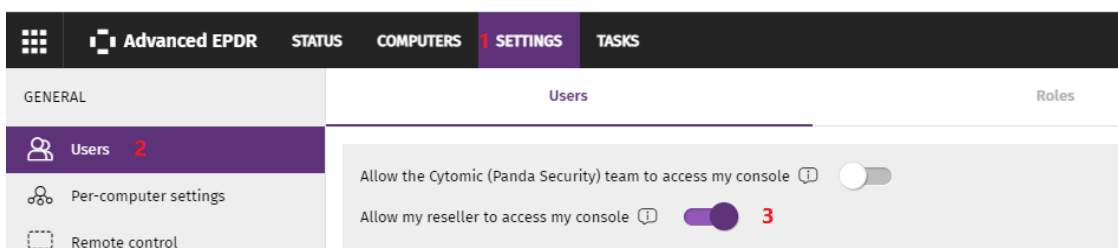


Figura 9.8: Opción Permitir a mi distribuidor acceder a mi consola

Visualizar las configuraciones asignadas

La consola de administración implementa hasta cuatro formas de mostrar los perfiles de configuración asignados a un grupo o equipo:

- En el árbol de grupos.
- En la pantalla de definición de la configuración.
- En la pestaña **Configuración** del equipo.
- En el listado de equipos exportado.

Mostrar las configuraciones en el árbol de grupos

- Haz clic en el menú superior **Equipos** y en la pestaña  situada en la parte superior del panel lateral para mostrar el árbol de grupos.

- Selecciona el menú de contexto de la rama elegida y haz clic en el menú emergente **Configuraciones** para mostrar una ventana con las configuraciones asignadas a la carpeta.

A continuación, se indica la información mostrada en cada entrada:

- **Tipo de configuración:** indica la clase a la que pertenece la configuración mostrada.
- **Nombre de la configuración:** nombre asignado por el administrador en la creación de la configuración.
- **Tipo de herencia aplicada:**
 - **Configuración heredada de...:**  la configuración fue asignada a la carpeta padre indicada, y los equipos que pertenecen a la rama actual la heredan.
 - **Asignada directamente a este grupo:** → la configuración de los equipos es la que el administrador asignó de forma manual a la carpeta.

Mostrar las configuraciones en la definición de la configuración

Haz clic en el menú superior **Configuraciones** y selecciona el tipo de configuración en el menú lateral.

Selecciona una configuración en el listado de configuraciones.

Si la configuración esta asignada a uno o más equipos o grupos, se mostrará el botón **Ver equipos**.

Haz clic en el botón **Ver equipos**. Se mostrará la zona **Equipos** con un único listado formado por todos los equipos que tienen la configuración asignada, tanto si se asignó de forma individual o mediante grupos de equipos. En la parte superior de la ventana se mostrará el criterio de filtrado establecido.

Mostrar las configuraciones en la pestaña configuración del equipo

En el menú superior **Equipos**, selecciona un equipo del panel de la derecha para mostrar la ventana de detalle. En la pestaña **Configuración** se listan los perfiles asignados al equipo.

Mostrar las configuraciones en el listado de equipos exportado

Desde el árbol de equipos (árbol de grupos o árbol de filtros) haz clic en el menú contextual y elige la opción **Exportar**.



Consulta **Campos mostrados en el fichero exportado** en la página **198** para más información.

Capítulo 10

Configuración remota del agente

El administrador puede cambiar desde la consola web el funcionamiento de varios aspectos del agente Cytomic instalado en los equipos de la red:

- El papel o rol que el equipo representa para el resto de puestos y servidores protegidos.
- Las protecciones frente al tampering o manipulación indebida del software cliente Advanced EDR por parte de amenazas avanzadas y APTs.
- La visibilidad del agente en el equipo de usuario o servidor y su idioma.
- La configuración de las comunicaciones de los equipos con la nube de Cytomic.
- La aplicación de una capa extra de seguridad en las conexiones VPN entre los equipos y las redes corporativas.

Contenido del capítulo

Configuración de los roles del agente Cytomic	272
Rol de Proxy Cytomic	272
Rol de caché	274
Rol de descubridor	276
Configuración de listas de acceso a través de proxy	277
Configuración de las descargas mediante equipos caché	279
Requisitos para usar un equipo con el rol de caché asignado	279
Configuración de la comunicación en tiempo real	281
Configuración del idioma del agente	281
Configuración de la visibilidad del agente	282
Control de acceso a redes	282
Requisitos	283
Comprobación de los requisitos	284

Acceso a la configuración de Control de acceso a redes	284
Configurar la seguridad frente a manipulaciones no deseadas de las protecciones	285
Activar verificación en dos pasos (2FA)	286
Excepciones al copiar perfiles con configuraciones de tipo Seguridad frente a manipulaciones no deseadas de las protecciones	288
Configuración de Shadow Copies	289
Acceso a la funcionalidad de Shadow Copies	290

Configuración de los roles del agente Cytomic

El agente Cytomic instalado en los equipos Windows de la red puede adoptar tres roles diferentes:

- Proxy
- Descubridor
- Caché

Para asignar un rol a un equipo con el agente Cytomic ya instalado haz clic en el menú superior **Configuración** y en el panel lateral **Servicios de red**. Se mostrarán cuatro pestañas: Proxy de Advanced EDR, **Caché**, **Descubrimiento** y **Control de acceso a redes**.



Solo los equipos con sistema operativo Windows instalado pueden adquirir el rol de Proxy, Descubridor o Caché.

Rol de Proxy Cytomic

Para acceder a la nube de Cytomic, el software de seguridad instalado en los equipos requiere de acceso a Internet. En los casos de equipos aislados, se permite el acceso a través del proxy corporativo de la organización. Si no existe este recurso, Advanced EDR permite designar a uno o a varios equipos con el rol de proxy Cytomic.

Los equipos con el rol de proxy Cytomic asignado escuchan peticiones de los equipos y las redirigen a la nube de Cytomic por una conexión válida.



Solo se recomienda utilizar equipos con el rol de proxy Cytomic asignado en los casos de equipos aislados que además no tengan acceso a ningún proxy corporativo. El proxy Cytomic no incorpora todas las funcionalidades de un proxy corporativo y está diseñado únicamente para acceder a los recursos alojados en la nube de Cytomic.

Un equipo con el rol de proxy Cytomic asignado puede dar servicio a un número de dispositivos muy variable, que depende de los recursos hardware instalados. Como norma general, se establece que un equipo puede dar servicio como máximo a 100 equipos.

Limitaciones de los equipos con el rol de Proxy Cytomic asignado

Por motivos de seguridad, cuando Advanced EDR tiene asignado el rol de Proxy Cytomic, únicamente puede establecer conexiones con la nube de Cytomic. Por esta razón, existen varias limitaciones al tipo de descargas que el software de seguridad puede realizar si tiene configurado el acceso a Internet a través de un nodo Proxy Cytomic:

- **Windows y macOS:**
 - El software de seguridad no puede descargar parches de Cytomic Patch pero sí puede reportar los parches pendientes de instalación. Consulta [Descargar e instalar parches](#) en la página **382**.
- **Linux:**
 - El software de seguridad no puede descargar parches de Cytomic Patch pero sí puede reportar los parches pendientes de instalación. Consulta [Descargar e instalar parches](#) en la página **382**.
 - Si el software de seguridad requiere la descarga adicional de paquetes desde repositorios no accesibles por el proxy Cytomic, la instalación no será posible. Consulta [Actualización del motor de protección](#) en la página **172**.

Estas limitaciones no aplican al proxy corporativo de la empresa.

Requisitos para asignar el rol de proxy Cytomic a un equipo

- Advanced EDR instalado en un equipo con sistema operativo Windows.
- Soporte para el formato de ficheros 8+3. Consulta el artículo de la MSDN [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778996\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778996(v=ws.10)?redirectedfrom=MSDN) para habilitar esta funcionalidad.
- Puerto TCP 3128 sin usar por otras aplicaciones.
- Configuración del cortafuegos del equipo que permita el tráfico entrante y saliente por el puerto 3128.
- Resolver el nombre del equipo con el rol de proxy asignado desde el equipo que lo utiliza.

Asignar el rol de proxy Cytomic a un equipo

- Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red** y en la pestaña **Proxy**. Se mostrarán todos los equipos con el rol de proxy ya asignado.

- Haz clic en el botón **Añadir servidor proxy**. Se mostrará una ventana con todos los equipos administrados por Advanced EDR que cumplen los requisitos para ejercer de proxy en la red.
- Utiliza la caja de búsqueda para localizar el equipo y haz clic sobre el mismo para agregarlo al listado de equipos con el rol de proxy asignado.

Retirar el rol de proxy Cytomic a un equipo

- Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red** y en la pestaña **Proxy**. Se mostrarán todos los equipos con el rol de proxy ya asignado.
- Haz clic en el icono  del equipo que quieres retirar el rol de proxy.



Para configurar el uso de un equipo con el rol de proxy asignado consulta [Configuración de listas de acceso a través de proxy](#).

Rol de caché

Advanced EDR permite asignar el rol de caché a uno o más puestos de la red. Estos equipos descargan y almacenan de forma automática todos los ficheros que necesitan otros puestos con Advanced EDR instalado. Esto produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada.

Limitaciones de los equipos con el rol de caché asignado

Por motivos de seguridad, cuando Advanced EDR tiene asignado el rol de caché, únicamente puede establecer conexiones con la nube de Cytomic. Por esta razón, hay ciertas restricciones en cuanto al tipo de descargas que el software de seguridad puede llevar a cabo cuando se configuran para realizarse a través de un nodo caché:

- Los equipos Linux no pueden descargar parches de actualización de Cytomic Patch. Consulta [Descargar e instalar parches](#) en la página 382.
- Los equipos Linux no pueden descargar paquetes del software de seguridad para instalarlo o actualizarlo. Consulta [Actualización del motor de protección](#) en la página 172.

Elementos cacheados

Un equipo con el rol de caché asignado puede cachear los elementos siguientes durante un periodo de tiempo variable dependiendo de su tipo:

- **Archivo de identificadores:** hasta que dejan de ser válidos.
- **Paquetes de instalación:** hasta que dejan de ser válidos.
- **Parches de actualización para Cytomic Patch:** 30 días.

Dimensionamiento de un equipo caché

El dimensionamiento de un equipo con el rol de caché asignado depende completamente del número de conexiones simultáneas en los picos de carga y del tipo de tráfico que gestione (descargas de ficheros de firmas, instaladores etc.). Como aproximación, un equipo con el rol de caché asignado puede servir en torno a 1000 equipos de forma simultánea.

Asignar el rol de caché a un equipo

- En el menú superior **Configuración**, panel lateral **Servicios de red** haz clic en la pestaña superior **Caché**.
- Haz clic en el botón **Añadir equipo caché**.
- Utiliza la herramienta de búsqueda situada en la parte superior de la ventana para localizar equipos candidatos a asignar el rol de caché.
- Selecciona un equipo de la lista y pulsa **Aceptar**.

A partir de ese momento, el equipo seleccionado adoptará el rol de caché y comenzará la descarga de todos los archivos necesarios, manteniendo sincronizado su repositorio de forma automática. El resto de los puestos de la subred contactarán con el equipo caché para la descarga de actualizaciones.

Retirar el rol de caché a un equipo

Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Caché**.

Haz clic en el icono  del equipo al que quieres retirar el rol caché.

Establecer la unidad de almacenamiento

Es posible configurar el agente Advanced EDR para almacenar los elementos a cachear en un volumen / unidad concreta del equipo, aunque la ruta de la carpeta dentro del volumen es fija. Para configurar esta característica sigue los pasos mostrados a continuación:

- En el menú superior **Configuración**, panel lateral **Servicios de red** haz clic en la pestaña superior **Caché**.
- En un equipo con el rol de caché asignado y que ya haya reportado a la nube su estado haz clic en el enlace **Cambiar**. Se mostrará una ventana con las unidades locales disponibles.
- Por cada unidad se muestra el nombre del volumen, la unidad asignada, el espacio ocupado y el espacio libre.

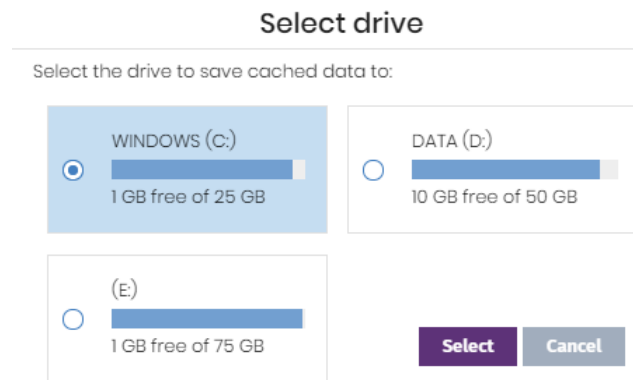


Figura 10.1: Ventana de selección de volumen en un equipo con el rol de caché asignado

- Para ver los porcentajes de espacio ocupado y libre pasa el ratón por encima de las barras y se mostrará una etiqueta con la información.
- Indica con el selector la unidad con 1 Gigabyte libre o más que almacenará los elementos cacheados, y haz clic en el botón **Seleccionar**. Advanced EDR comenzará a copiar los elementos ya cacheados y, una vez completado el proceso, los borrará de su ubicación original.



*Solo es posible seleccionar la unidad donde se almacenarán los elementos a cachear en los equipos que hayan reportado su estado al servidor Advanced EDR. Si no se cumple esta condición, se tomará por defecto la unidad que almacena los ficheros de instalación de Advanced EDR. Una vez reportado, se mostrará el enlace **Cambiar** en el equipo con el rol de caché asignado y se podrá modificar la unidad de almacenamiento. Un equipo puede tardar en reportar su estado varios minutos.*

Si no hay espacio suficiente o se produce algún error de escritura al cambiar la unidad de almacenamiento, se mostrará un mensaje debajo del equipo con el rol de caché asignado, indicando la fuente del problema.

Rol de descubridor

En el menú superior **Configuración**, panel lateral **Servicios de red**, la pestaña **Descubrimiento** está directamente relacionada con el procedimiento de instalación y despliegue de Advanced EDR en la red del cliente.



*Consulta **Visualizar equipos descubiertos** en la página **121** para obtener más información acerca del proceso de descubrimiento e instalación de Advanced EDR.*

Configuración de listas de acceso a través de proxy

Advanced EDR permite asignar a los equipos de la red uno o más métodos de conexión con el exterior, en función de los recursos existentes en la infraestructura IT de la compañía.

Los métodos de conexión se organizan a través de dos listas independientes:

- **Lista de acceso:** contiene los métodos de conexión configurados por el administrador.
- **Lista de fallback:** lista no modificable de métodos de conexión incluidos por defecto en Advanced EDR.

Si existen métodos de conexión repetidos entre ambas listas, se retirarán automáticamente de la lista de fallback.

Lista de acceso

Es la lista de métodos de acceso configurable por el administrador. Se recorre de forma ordenada cuando el agente necesita conectar con la nube de Cytomic. Una vez seleccionado un método de acceso, éste no cambia hasta que queda inaccesible, momento en el cual Advanced EDR recorrerá la lista desde el inicio hasta encontrar un nuevo método de acceso válido. Si llega al final de la lista sin encontrarlo se buscará en la lista de fallback. Consulta [Lista de fallback](#).

Los tipos de conexión admitidos en la lista de acceso son:

Tipo de proxy	Descripción
No usar proxy	Acceso directo a Internet. Los equipos acceden de forma directa a la nube de Cytomic para descargar las actualizaciones y enviar los reportes de estado del equipo. En este caso, el software Advanced EDR utilizará la configuración del equipo para comunicarse con Internet.
Proxy corporativo	Acceso a Internet vía proxy instalado en la red de la organización. • Dirección: dirección IP del servidor de proxy. • Puerto: puerto del servidor de proxy. • El proxy requiere autenticación: habilitar si el proxy requiere información de usuario y contraseña. • Usuario: cuenta de un usuario del proxy que permita su uso. • Contraseña: contraseña de la cuenta de usuario.
Descubrimiento automático de proxy a través de Web Proxy Autodiscovery Protocol	Pregunta a la red mediante DNS o DHCP para recuperar la url de descubrimiento que apunta al archivo PAC de configuración. Alternativamente se puede indicar directamente el recurso HTTP o HTTPS donde se encuentra el archivo PAC de configuración.

Tipo de proxy	Descripción
(WPAD)	En equipos Linux no está disponible este tipo de configuración y será ignorada. Cytomic no se recomienda su uso para este sistema operativo.
Proxy Cytomic	Acceso a la nube de Cytomic a través de un equipo de la red con el rol de proxy Cytomic asignado. Una lista de acceso puede tener varios proxys Cytomic definidos. Para conocer las limitaciones de acceso de un proxy Cytomic y cómo asignar este rol a un equipo de la red consulta Rol de Proxy Cytomic.

Tabla 10.1: Tipos de acceso a la red soportados por Advanced EDR

Configurar una lista de acceso

Para configurar una lista de acceso crea una configuración de tipo **Configuración de red**:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y en el botón **Añadir** o selecciona una configuración ya creada para modificarla.
- En la sección **Proxy** haz clic en el icono . Se mostrará una ventana con los tipos de conexión disponibles.
- Selecciona un tipo de conexión (**Tipos de acceso a la red soportados por Advanced EDR**) y haz clic en el botón **Aceptar**. El tipo de conexión se añadirá a la lista.
- Para modificar el orden de los métodos de conexión selecciona un elemento haciendo clic en la casilla de selección y utiliza las flechas  y  para subirlo o bajarlo.
- Para borrar un método de conexión haz clic en el icono .
- Para modificar un método de conexión selecciónalo con las casillas de selección y haz clic en el icono . Se mostrará una ventana donde editar la configuración del método.

Lista de fallback

Cuando el agente no puede conectar con la plataforma Cytomic y ya ha probado todos los métodos de conexión indicados en la lista de acceso configurada, recorrerá la lista de fallback. Esta lista de métodos de acceso no es configurable por el administrador y se recorre de forma ordenada. Una vez que el agente Cytomic ha encontrado un método de conexión válido, éste no se cambiará hasta que quede inaccesible, momento en el cual se volverá a recorrer la lista de acceso configurada por el administrador desde su inicio. Si ninguno de los métodos de acceso indicados en la lista de acceso o de fallback es válido, el agente devolverá un error de comunicaciones.

La lista de fallback es fija y contiene los métodos de acceso siguientes (no todos están disponibles en todas las plataformas):

- **Internet Explorer:** Advanced EDR intenta recuperar la configuración de proxy de Internet Explorer suplantando a la cuenta de usuario que inició sesión en el equipo. Solo disponible en sistemas operativos Windows.
 - Este método de acceso no se puede utilizar si la configuración de las credenciales para el uso del proxy está definida de forma explícita.
 - Si la configuración de proxy de Internet Explorer utiliza PAC (Proxy Auto-Config), solo se obtendrá la URL del archivo de configuración si el protocolo de acceso al recurso es HTTP o HTTPS.
- **Proxy por defecto:** Advanced EDR lee la configuración del proxy configurada por defecto en el sistema operativo.
- **WPAD:** Advanced EDR pregunta a la red mediante DNS o DHCP para recuperar la url de descubrimiento que apunta al archivo PAC de configuración. En equipos Linux no está disponible este tipo de configuración.
- **Conexión directa:** Advanced EDR intenta conectarse directamente a la nube de Cytomic.

Configuración de las descargas mediante equipos caché

La utilización de un equipo con el rol de caché puede establecerse de dos maneras:

- **Método automático:** el equipo que inicia la descarga utiliza los equipos con el rol de caché descubiertos en la red y que cumplan con los requisitos indicados en [Requisitos para usar un equipo con el rol de caché asignado](#). Si se encuentran varios equipos caché se balancearán las descargas para no sobrecargar a un único equipo caché.
- **Método manual:** el administrador establece de forma manual el equipo de la red con el rol de caché que será utilizado para descargar datos de la nube de Cytomic. El comportamiento de un equipo cache asignado de forma manual tiene las siguientes diferencias con respecto al modo automático:
 - Si un equipo tiene varios equipos cache asignados de forma manual, no se repartirán las descargas.
 - Si el primer equipo caché no está accesible, se recorrerá la lista hasta encontrar un equipo que funcione. Si no se encuentra ningún equipo se intentará la salida directa a Internet.

Requisitos para usar un equipo con el rol de caché asignado

Modo automático

- El equipo con el rol de cache asignado y el equipo que descarga elementos de éste deben estar en la misma subred. Si un equipo caché tiene varias tarjetas de red, podrá servir de repositorio en cada uno de los segmentos a los que esté conectado.



Se recomienda asignar un equipo como rol caché en cada segmento de la red de la compañía.

- El resto de equipos descubrirán de forma automática la presencia de un equipo caché y redirigirán hacia él sus peticiones de actualización.
- Se requiere asignar una licencia de protección al equipo caché para su funcionamiento.
- Configura el cortafuegos para permitir el tráfico SSDP (uPnP) entrante y saliente en los puertos
 - 21226 UDP
 - 18226 TCP

Modo manual

- No es necesario que el equipo con el rol de cache asignado y el equipo que descarga elementos estén en la misma subred.
- Se requiere asignar una licencia de protección al equipo caché para su funcionamiento.
- Configura el cortafuegos para permitir el tráfico entrante y saliente en los puertos
 - 21226 UDP y TCP
 - 18226 TCP

Descubrimiento de equipos caché

En el momento de la asignación del rol al equipo, éste lanzará un broadcast hacia los segmentos de red a los que pertenecen sus interfaces. Los puestos de trabajo y servidores con el método automático de asignación recibirán la publicación del servicio y, en el caso de que en un mismo segmento haya más de un equipo caché designado, los equipos se conectarán al más adecuado en función de los recursos libres que posea.

Adicionalmente, cada cierto tiempo los equipos de la red con el método automático de asignación configurado preguntarán si existe algún equipo con el rol de caché asignado.

Configuración del método de asignación de equipos caché

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y elige una configuración.
- En la sección **Caché** elige una opción:
 - **Utilizar automáticamente los equipos caché vistos en la red:** los equipos que reciben esta configuración buscarán de forma automática los equipos caché de su segmento de red.
 - **Utilizar los siguientes equipos caché (por orden de preferencia):** haz clic en el icono  para añadir equipos con el rol de caché asignado y configurar una lista de ellos. Los equipos

que reciban esta configuración conectarán con los equipos caché indicados en la lista para realizar las descargas.

Configuración de la comunicación en tiempo real

Advanced EDR se comunica en tiempo real con la plataforma Cytomic para recuperar las configuraciones establecidas en la consola sobre los equipos protegidos, transcurriendo unos pocos segundos desde que el administrador asigna una configuración a un equipo hasta que éste la aplica.

Las comunicaciones en tiempo real entre los equipos protegidos y el servidor Advanced EDR requieren el mantenimiento de una conexión abierta por cada puesto de forma permanente. Desactiva las comunicaciones en tiempo real cuando el número de conexiones abiertas afecte al rendimiento del proxy instalado en la red, o cuando el impacto en el consumo de ancho de banda sea elevado al cambiar simultáneamente las configuraciones de un gran número de equipos.

Requisitos para comunicación en tiempo real

- Las comunicaciones en tiempo real son compatibles con todos los sistemas operativos soportados por Cytomic excepto Windows XP y Windows 2003.
- Si el equipo accede a Internet mediante un proxy corporativo, se requiere que las conexiones https no sean manipuladas. Muchos proxys utilizan técnicas Man in the Middle para analizar las conexiones https o funcionar como proxys caché. En estos casos la comunicación en tiempo real no funcionará.

Deshabilitar las comunicaciones en tiempo real

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y en el botón **Añadir** o selecciona una configuración ya creada para modificarla.
- En la sección **Proxy** despliega la sección **Opciones avanzadas** y desactiva la casilla **Activar la comunicación en tiempo real**.

Al deshabilitar las comunicaciones en tiempo real, los equipos se comunicarán con el servidor Advanced EDR cada 15 minutos.

Configuración del idioma del agente

Para asignar el idioma del agente Cytomic a uno o varios equipos es necesario crear una configuración de tipo **Configuración de red**:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y en el botón **Añadir** o selecciona una configuración ya creada para modificarla.
- En la sección idioma elige el idioma de entre los disponibles:

- Alemán
- Español
- Finlandés
- Francés
- Húngaro
- Inglés
- Italiano
- Japonés
- Portugués
- Ruso
- Sueco



Si se produce un cambio de idioma y la consola local de Advanced EDR estaba abierta se pedirá un reinicio de la consola local. Este procedimiento no afecta a la seguridad del equipo.

Configuración de la visibilidad del agente

Para las empresas donde el servicio de seguridad sea 100% administrado por el departamento de IT no es necesario que el icono del agente Advanced EDR sea visible en el área de notificaciones de los equipos de la red. Para ocultar o mostrar el icono sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Preferencias** y activa o desactiva la opción **Mostrar icono en la bandeja del sistema**.

Control de acceso a redes

Control de acceso a redes aporta una capa extra de seguridad cuando los dispositivos de usuario (equipos de sobremesa, servidores, portátiles o dispositivos móviles) se conectan a la red corporativa, ya sea remotamente a través de VPN o localmente a través de Wi-Fi.

El dispositivo de usuario que intenta conectarse a la red corporativa a través de VPN o de Wi-Fi, ha de cumplir una serie de condiciones para que se le permita acceder. Si no las cumple, el acceso se denegará.

El agente Cytomic instalado en el dispositivo del usuario es el encargado de reunir y enviar la información necesaria para que el dispositivo que validará el acceso (Firebox -en el caso de VPN- o Access Point -para Wi-Fi-) pueda realizar las comprobaciones necesarias.

Mecanismo de validación y generación de UUIDs

Un UUID (Universally Unique Identifier) es una cadena de caracteres que identifica de forma única a un dispositivo.

El mecanismo utilizado en el dispositivo (FireBox o Access Point) para validar las conexiones VPN o Wi-Fi es un UUID + contraseña. Esto implica tener configurado el mismo par UUID - contraseña en el dispositivo y en la consola de Advanced EDR.

Si no tienes previamente configurado un UUID en tu dispositivo, será necesario generar uno nuevo. Al ser un formato abierto, existen muchos generadores de UUIDs gratuitos, como por ejemplo <https://www.uuidgenerator.net/>



Utiliza una contraseña lo suficientemente larga que incluya caracteres especiales, números y mayúsculas.



Para más información sobre Firebox y su configuración de conexiones VPN, consulta [Network Access Enforcement Overview](#).

Requisitos

Para que el dispositivo del usuario pueda conectarse a la red corporativa, tiene que cumplir los siguientes requisitos:

- Tener una protección instalada, activa y debidamente configurada en el equipo del usuario.
- Tener un UUID y una clave de autenticación válidos y configurados tanto en el dispositivo que comprueba la conexión como en la consola de Advanced EDR.
- **Sistema operativo instalado en el dispositivo del usuario:**
 - Windows 8.1 o superior.
 - macOS Catalina 10.15 o superiores
 - Android 6 o superiores.



En el caso de Android, el usuario de la consola de Firebox no podrá seleccionar la versión del sistema operativo, como en Windows o macOS. El control de acceso a redes VPN o Wi-Fi se activará en los dispositivos Android 6.0 o superior cuando reciban la configuración procedente de los servidores de Cytomic

- **Puertos abiertos en el dispositivo:** el agente Cytomic requiere el puerto 33000 para comunicarse con el dispositivo que valida la conexión.
- **Una configuración de protección válida:** protección avanzada de Advanced EDR en modo *hardening* o *lock* activada y en ejecución, o la protección antivirus activada y en ejecución.



Control de acceso a redes no es compatible con el sistema operativo Linux.

Comprobación de los requisitos

Cuando el dispositivo del usuario trata de conectarse a la red corporativa, el dispositivo que valida la conexión lleva a cabo las siguientes acciones:

- Solicita información sobre el estado de la protección instalada en el dispositivo del usuario.
- Comprueba que la UUID de la cuenta y la clave de autenticación son válidas.
- Confirma que el sistema operativo del dispositivo del usuario es válido, comparándolo con los que tiene configurados.

Si todas las comprobaciones son positivas, se permitirá el acceso del dispositivo del usuario a la red corporativa; en caso contrario, no lo permitirá.



De forma predeterminada, los equipos tienen activada la exigencia de cumplimiento de los requisitos de seguridad para conectarse a la red corporativa.

Acceso a la configuración de Control de acceso a redes

- Selecciona el menú lateral **Servicios de red**.
- En el menú de pestañas superior, haz clic en **Control de acceso a redes**.
- Para activar la protección, mueve el control deslizante.
- Escribe el UUID de la cuenta y la clave de autenticación.
- Haz clic en el botón **Guardar cambios**.

Configurar la seguridad frente a manipulaciones no deseadas de las protecciones

Para evitar que personas no autorizadas desactiven la protección, Advanced EDR permite establecer las siguientes limitaciones a la hora de desinstalar o configurar la protección desde los equipos:

- **Establecer un primer factor de autenticación** basado en contraseña, para configurar, desactivar o desinstalar la protección desde el propio equipo. Compatible con equipos Windows y Linux.
- **Establecer un segundo factor de autenticación** basado en código QR, para configurar, desactivar o desinstalar la protección desde el propio equipo. Compatible con equipos Windows y Linux. Para utilizar el segundo factor de autenticación es necesario:
 - Acceder a un teléfono móvil o tablet personal con cámara de fotos integrada.
 - Descargar la aplicación gratuita WatchGuard AuthPoint (o una aplicación equivalente) en:
 - **iOS:** <https://apps.apple.com/app/watchguard-authpoint/id1335115425>
 - **Android:**
<https://play.google.com/store/apps/details?id=com.watchguard.authpoint>
- **Activar la protección anti-tamper:** muchas amenazas avanzadas incorporan técnicas para desactivar el software de seguridad de los equipos. La protección Anti-tamper evita la modificación no autorizada del funcionamiento de la protección mediante el establecimiento de una contraseña, que impide que el software se detenga, pause o se desinstale. Compatible con equipos Windows y Linux.
- **Activar la protección cuando el equipo se inicia en modo Seguro:** algunos tipos de malware están diseñados para forzar el reinicio de equipos Windows en modo seguro con funciones de red activadas. En este modo de inicio, el software de protección está desactivado y los equipos son vulnerables. Puedes configurar Advanced EDR para que proteja a los equipos cuando arrancan en modo seguro con funciones de red, de manera que todas las protecciones configuradas se mantengan activas y funcionando con normalidad. Compatible con equipos Windows.



Si un equipo pierde la licencia asignada de manera manual o por caducidad o cancelación, las protecciones anti-tampering y las protección por contraseña contra las desinstalación quedarán desactivadas.

Para configurar la seguridad frente a manipulaciones no deseadas:

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**:

- Para **Solicitar contraseña para desinstalar desde los equipos** activa el control deslizante y escribe en la caja de texto **Contraseña para poder realizar tareas de administración avanzada desde los equipos** una contraseña de entre 6 y 15 caracteres.
- Para **Permitir activar/desactivar temporalmente las protecciones desde la consola de los equipos** activa el control deslizante e introduce en la caja de texto **Contraseña para poder realizar tareas de administración avanzada desde los equipos** una contraseña de entre 6 y 15 caracteres.
- Para **Activar protección anti-tamper (impide que los usuarios o ciertos tipos de malware puedan detener las protecciones)** activa el control deslizante e introduce en la caja de texto **Contraseña para poder realizar tareas de administración avanzada desde los equipos** una contraseña de entre 6 y 15 caracteres.
- Para **Activar protección cuando los equipos Windows arrancan en Modo Seguro** activa el control deslizante. La protección se iniciará cuando el equipo arranca en modo seguro con funciones de red.
- Para activar el segundo factor de autenticación consulta [Activar verificación en dos pasos \(2FA\)](#).

Activar verificación en dos pasos (2FA)

De forma general, el software de seguridad está protegido de manipulaciones no autorizadas por parte de terceros mediante un mecanismo de contraseña simple. Sin embargo, es posible añadir un factor de autenticación adicional sobre la protección. Este factor de autenticación adicional se consigue mediante un código QR que se genera en la consola y se importa en la aplicación Authpoint o en cualquier otra aplicación que genere tokens de autenticación.

Para generar el código QR, Advanced EDR requiere de una palabra clave. Cada palabra clave genera un QR específico.

Una vez activada la verificación en dos pasos en la configuración de **Ajustes por equipo** y leído el código QR en la aplicación, el administrador tendrá que suministrar tanto la contraseña establecida en la consola como el token generado por la aplicación de autenticación para poder cambiar la configuración del agente o desinstalarlo.

Dependiendo del número de administradores que operan la consola, se puede generar un único código QR para toda la cuenta, o varios independientes. De este modo, es posible compartir un mismo QR para todas las configuraciones de **Ajustes por equipo**, solo para algunas o incluso asignar un código QR independiente para cada configuración de **Ajustes por equipo**.

Generar un único código QR a nivel de cuenta

El código QR se genera de forma automática a nivel de cuenta y se aplica a todas las configuraciones que tengan activa la opción **Utilizar un código QR compartido en toda la cuenta**:

- Desde el menú superior **Configuración**, haz clic en **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**

- Activa el control deslizante **Activar verificación en dos pasos (2FA)**.
- Selecciona **Utilizar un código QR compartido en toda la cuenta**.
- Haz clic en **Mostrar código QR**. Se mostrará el código QR generado para todas las configuraciones de **Ajustes por equipo** de la cuenta.
- Sincroniza el código QR de la cuenta con la aplicación Watchguard Authpoint o una equivalente.
- Haz clic en el botón **Cerrar**.
- Haz clic en el botón **Guardar**.

Generar un código QR individual para una configuración

La consola solicita una palabra clave para generar un código QR que se aplicará a una configuración de **Ajustes por equipo** particular:

- Desde el menú superior **Configuración**, haz clic en **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**.
- Activa el control deslizante **Activar verificación en dos pasos (2FA)**.
- Selecciona **Generar un código QR para esta configuración**.
- Haz clic en el botón **GENERAR CÓDIGO**.
- Escribe una contraseña de 6 a 20 caracteres utilizando códigos alfanuméricos. Esta contraseña está vinculada al código QR que genera la consola y puede ser reutilizada en otras configuraciones de **Ajustes por equipo**.
- Haz clic en **GENERAR CÓDIGO**.
- Haz clic en el botón **Cerrar**.
- Haz clic en el botón **Guardar**.

Compartir un código QR entre varias configuraciones

Para asignar un código QR ya generado a otra configuración **Ajustes por equipo**:

- Desde el menú superior **Configuración**, haz clic en **Ajustes por equipo**.
- Haz clic en la configuración a copiar el código QR.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**.
- En la opción **Generar un código QR para esta configuración** haz clic en **Mostrar código QR**. Se abrirá una ventana con el código QR y la clave del código QR.
- Copia en el portapapeles la clave del código QR.

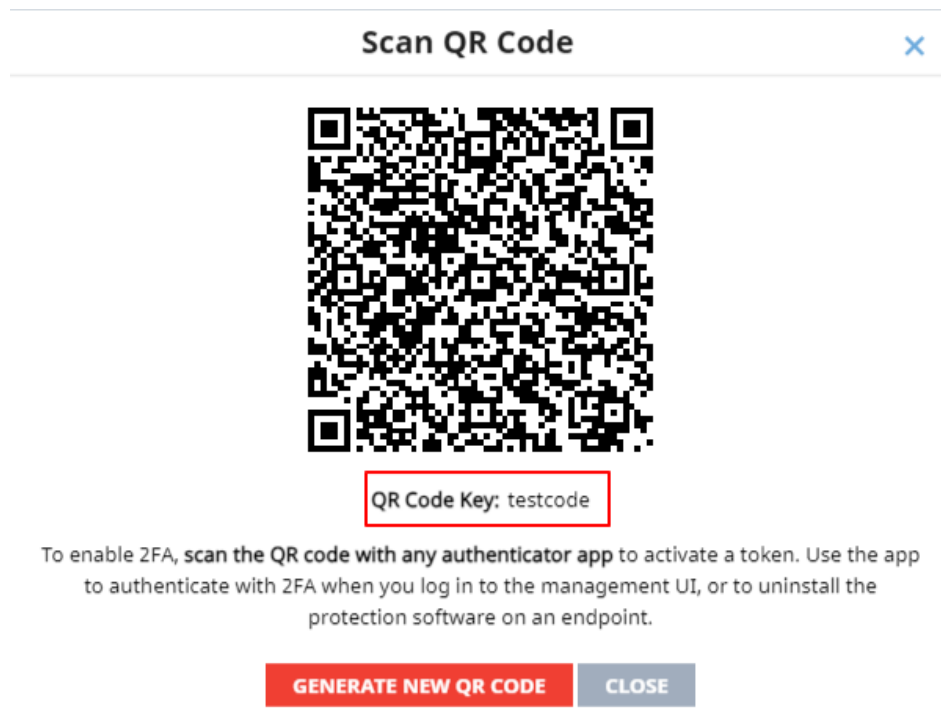


Figura 10.2: Código QR y clave del código QR asociada

- Haz clic en el botón **Cerrar** de la ventana y en el botón **Cerrar** de la configuración.
- Haz clic en la configuración donde quieres utilizar el código QR copiado o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**.
- Activa con el botón **Activar verificación en dos pasos (2FA)**.
- Selecciona **Generar un código QR para esta configuración**.
- Haz clic en el botón **GENERAR CÓDIGO**.
- Pega en la caja de texto la clave del código QR generado.
- Haz clic en **GENERAR CÓDIGO**.
- Haz clic en el botón **Cerrar**.
- Haz clic en el botón **Guardar**.

Excepciones al copiar perfiles con configuraciones de tipo Seguridad frente a manipulaciones no deseadas de las protecciones

Al copiar un perfil con contraseña y / o doble factor de autenticación activado el comportamiento es el descrito en **Copiar configuraciones** en la página 260 exceptuando:

- En la configuración copiada no se copia la contraseña indicada en la caja de texto **Contraseña para poder realizar tareas de administración avanzada desde los equipos**. El administrador deberá introducir una nueva contraseña.
- Si el administrador copia una configuración enviada por el partner, Advanced EDR establecerá automáticamente la opción **Generar un código QR para esta configuración**, generará un nuevo código QR y no copiará la contraseña indicada en la caja de texto **Contraseña para poder realizar tareas de administración avanzada desde los equipos**.

Configuración de Shadow Copies

Shadow Copies es una tecnología implementada en sistemas operativos Windows que permite realizar copias de seguridad transparentes de los ficheros almacenados en el equipo del usuario.

A través de la consola de Advanced EDR, el administrador puede interactuar con el servicio Shadow Copies de los equipos de la red de forma remota y centralizada, y utilizarlo como herramienta de resolución frente ataques de tipo ransomware.

Características de Shadow Copies en Advanced EDR

Advanced EDR completa al servicio Shadow Copies de Windows con características adicionales que permiten proteger los datos del usuario frente a las amenazas:

- Configura y gestiona un repositorio de copias (snapshot) independiente de los que haya creado el usuario.
- Protege al servicio y al snapshot frente a modificaciones realizadas por amenazas o por el mismo usuario. De esta manera, se impide la detención del servicio o el borrado de las copias de seguridad ya realizadas por Advanced EDR.
- Permite configurar el porcentaje de espacio del disco duro dedicado a la copia de seguridad (por defecto utiliza un 10% del espacio del dispositivo).
- Realiza una copia de los ficheros cada 24 horas. La primera copia se produce en el momento en el que el administrador activa la funcionalidad (por defecto se entrega desactivada).
- Guarda hasta un total de 7 copias de cada fichero, dependiendo del espacio libre asignado al repositorio. Si el espacio no es suficiente, se elimina la copia más antigua para dar cabida a la más reciente.

Requisitos

- Sistema operativo:
 - Windows Vista, 7 y superiores.
 - Windows 2003 Server 2012 y superiores.
- Espacio en disco suficiente para realizar las copias.

- Medio de almacenamiento identificado por el sistema operativo como fijo (discos duros internos y conectados por usb) y con formato NTFS.

Acceso a la funcionalidad de Shadow Copies

- Haz clic en el menú superior **Configuración** y en el panel lateral izquierdo **Ajustes por equipo**. Se mostrará el listado de configuraciones.
- Haz clic sobre una configuración o crea una nueva.
- En el apartado **Shadow Copies** mueve el control deslizante para activar la funcionalidad, y establece el porcentaje máximo del disco que ocuparán las copias en los discos de los equipos.



Aunque Advanced EDR utiliza un snapshot independiente de los creados por el usuario o el administrador de la red, todos ellos comparten la misma configuración. Además, el porcentaje máximo del disco establecido en la consola de administración tiene prioridad frente a otras configuraciones establecidas por el administrador de la red.

Buscar los equipos con Shadow Copies activado mediante filtros

- Haz clic en el menú superior **Equipos**
- Haz clic en el icono del panel lateral. Se mostrará el árbol de filtros.
- Haz clic en el icono de cualquier carpeta del árbol de filtros. Se desplegará el menú de contexto.
- Haz clic en **Añadir Filtro**. Se abrirá la ventana **Añadir filtro**.
- Configura el filtro con los valores siguientes:
 - **Categoría:** Equipo
 - **Propiedad:** Shadow Copies
 - **Operador:** Es igual a
 - **Valor:** Activado



Para más información, consulta [Configurar filtros](#) en la página 184

Capítulo 11

Configuración de la seguridad en estaciones y servidores

Advanced EDR ofrece todas las funcionalidades de protección incluidas en el producto mediante las configuraciones de seguridad para estaciones y servidores. El administrador de la red podrá proteger los activos de la empresa frente a amenazas informáticas de muy diversa índole, asignando configuraciones de seguridad a los equipos de la red.

A continuación se explican todos los parámetros incluidos en la configuración de seguridad para estaciones y servidores. También se indican algunas recomendaciones prácticas para asegurar los puestos de trabajo de la red y minimizar los inconvenientes ocasionados al usuario.

Para obtener información adicional sobre los distintos apartados del módulo Estaciones y servidores consulta las referencias siguientes:



Crear y gestionar configuraciones en la página **258**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.

Acceso, control y supervisión de la consola de administración en la página **59**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.

Contenido del capítulo

Acceso a la configuración y permisos necesarios	292
Introducción a la configuración de la seguridad	292

Configuración General	293
Protección avanzada	296
Modo auditoría	306
Modo detallado	306

Acceso a la configuración y permisos necesarios

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración de **Estaciones y servidores**.

Permisos requeridos

Permiso	Tipo de acceso
Configurar seguridad para estaciones y servidores	Crear, modificar, borrar, copiar o asignar las configuraciones de Estaciones y servidores.
Ver configuraciones de seguridad para estaciones y servidores	Visualizar las configuraciones de Estaciones y servidores.

Tabla 11.1: Permisos requeridos para acceder a la configuración Estaciones y servidores

Introducción a la configuración de la seguridad

Las configuraciones de seguridad para estaciones y servidores se dividen en varios apartados. Al hacer clic en cada uno de ellos se mostrará un desplegable con la información asociada. A continuación, se muestran las diferentes secciones con una breve explicación.

Sección	Descripción
General	Establece el comportamiento de las actualizaciones, desinstalaciones de los antivirus de otros fabricantes y los ficheros excluidos en el equipo del usuario o servidor protegido que no se analizarán.
Protección avanzada	Establece el comportamiento de la protección avanzada y de la protección anti exploit frente a APTs, amenazas dirigidas y malware avanzado o que utiliza exploits.
Modo	Monitoriza los procesos ejecutados en equipos Windows, macOS y Linux, y detecta

Sección	Descripción
auditoría	y notifica la existencia de amenazas en ellos, pero no las bloquea ni elimina. Al activar el modo auditoría en una configuración, no se modifica el estado global de las diferentes protecciones en los equipos asignados a esa configuración, ni la configuración de las protecciones en la consola web.

Tabla 11.2: Descripción de los módulos disponibles en Advanced EDR

No todas las funcionalidades se encuentran disponibles en todas las plataformas soportadas. A continuación se muestra un resumen de las funcionalidades de seguridad incluidas en Advanced EDR por plataforma compatible:

Funcionalidad	Windows	macOS	Linux
Modo auditoría	X	X	X

Tabla 11.3: Funcionalidades de seguridad por plataforma

Configuración General

La configuración general establece el comportamiento de Advanced EDR relativo a las actualizaciones, desinstalación de programas de la competencia y exclusiones de ficheros y carpetas que no se analizarán.

Alertas en los equipos

Campo	Descripción
Mostrar alertas de malware, firewall y control de dispositivos	Introduce un mensaje descriptivo para informar al usuario del motivo de la alerta. El agente Advanced EDR mostrará una ventana desplegable con el contenido del mensaje. Disponible para equipos con sistema operativo Windows, macOS o Linux.
Mostrar alertas cada vez que el control de acceso a páginas web bloquee una página	Muestra una ventana emergente en el equipo del usuario o servidor cada vez que Advanced EDR bloquea el acceso a una página web. Disponible para equipos con sistema operativo Windows o macOS.

Tabla 11.4: Campos Alertas en los equipos

Actualizaciones



Consulta **Actualización del producto** en la página **171** para obtener información acerca de los procedimientos necesarios para actualizar el agente, la protección y el fichero de firmas de software cliente instalado en el equipo del usuario.

Desinstalar otros productos de seguridad



Consulta **Visión general del despliegue de la protección** en la página **100** para establecer el comportamiento de la instalación de la protección en el caso de que otro producto de seguridad esté instalado previamente en el equipo del usuario.

Consulta **Des instaladores soportados** para obtener un listado de todos los productos de la competencia que Advanced EDR desinstala automáticamente del equipo del usuario.

Archivos y rutas excluidas del análisis

Configura los elementos del equipo que no serán bloqueados, borrados o desinfectados en busca de malware.



Esta configuración desactiva la protección avanzada. Debido a que el uso de esta configuración genera potenciales agujeros de seguridad, Cytomic recomienda limitar su uso, quedando éste restringido a evitar problemas del rendimiento.

Exclusiones establecidas por el partner

Si el partner cambia el estado de las configuraciones enviadas de editable a no editable, las exclusiones añadidas por el administrador se ocultarán y dejarán de aplicarse, de modo que solo se aplicarían las enviadas por el partner. Si el partner vuelve a establecer como editable, las exclusiones añadidas por el administrador se restaurarán y volverán a aplicarse.

Excluir los siguientes archivos en disco

Indica los ficheros en el disco de los equipos protegidos que no serán borrados o desinfectados por Advanced EDR.



Cytopic recomienda minimizar el uso de comodines en Windows y coincidencias con subcadenas en Linux / macOS con el objetivo de delimitar al máximo posible los ficheros a excluir del análisis.

Campo	Descripción
Extensiones	Extensiones de ficheros que no serán analizadas.
Carpetas	Indica las carpetas cuyo contenido no será analizado. Windows: • Permite utilizar variables de sistema y de usuario. • No permite utilizar variables creadas por el propio usuario. • No permite utilizar comodines. Linux / macOS • No permite utilizar variables de sistema ni de usuario. • Permite especificar parcialmente la ruta.
Archivos	Indica los ficheros que no serán analizados. Windows: • Permite el uso de los caracteres comodín '*' y '?' cuando no se incluye la ruta y se especifica únicamente el nombre del fichero. • No permite el uso de comodines al especificar la ruta completa de un fichero. • Si no se especifica la ruta a un fichero, éste se excluirá en todas las carpetas donde se encuentre. En caso de especificar la ruta, solo se excluirá del análisis el fichero de la carpeta indicada. Linux / macOS: • No permite el uso de los caracteres comodín '*' y '?'. • Si no se especifica la ruta a un fichero, éste se excluirá en todas las carpetas donde se encuentre. En caso de especificar la ruta, solo se excluirá del análisis el fichero de la carpeta indicada. • Permite especificar parcialmente el fichero.

Tabla 11.5: Ficheros en disco que no serán analizados por Advanced EDR



Para evitar que la protección avanzada bloquee un software de confianza, aunque sea temporalmente, pero aun así se continúe enviando la telemetría a Cytomic para poder analizar el comportamiento de las aplicaciones, se recomienda utilizar el módulo de software Autorizado en lugar de las exclusiones. Consulta [Configuración de software autorizado](#) en la página 525 para más información.

Ejemplos para excluir ficheros en Windows

Para excluir el fichero `C:\Users\mike\desktop\data.txt`:

- **Archivos** = `C:\Users\mike\desktop\data.txt` (forma recomendada).
- **Archivos** = `data.txt` (no recomendada, excluye todos los archivos `data.txt` sin importar su ruta).
- **Archivos** = `C:\Users\mike\desktop\data.*` (erróneo, no permite excluir ficheros con comodines cuando se especifica la ruta).

Ejemplos para excluir rutas en Windows

Para excluir la carpeta `C:\Users\mike\desktop\`:

- **Carpetas** = `C:\Users\mike\desktop\` (esta es la forma recomendada).
- **Carpetas** = `C:\Users\%USERNAME%\desktop\` (excluye la carpeta `desktop` de todos los usuarios del equipo).
- **Carpetas** = `C:\Users\*\desktop\` (erróneo, no permite excluir ficheros con comodines en rutas).

Ejemplos para excluir ficheros o carpetas en Linux / macOS

Para excluir el fichero `/home/mike/data.txt`:

- **Ficheros** = `/home/mike/data.txt` (forma recomendada).
- **Carpetas** = `/home/$USER/` (erróneo, no permite utilizar variables de entorno).
- **Ficheros** = `/home/mike/*.txt` (erróneo, no permite utilizar comodines).
- **Ficheros** = `mik` (no recomendada, excluye todos los ficheros que contienen en su nombre o ruta la subcadena `mik`).

Protección avanzada

Funcionalidades según el sistema operativo

La protección avanzada incluye las siguientes funcionalidades para cada sistema operativo:

Funcionalidad	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Comportamiento: modo de funcionamiento (incluye decoy files).	X		
Comportamiento: detectar actividad maliciosa	X	X	
Anti-exploit (incluye inyección de código y bloqueo de driver vulnerable)	X (No disponible en sistemas Windows ARM)		
Tecnología AMSI (Anti-Malware Scan Interface)	X		
Políticas avanzadas de seguridad (incluye bloqueo de programas)	X		
Protección contra ataques de red	X		
Privacidad	X	X	X
Uso de la red	X	X	X

Tabla 11.6: Funcionalidades de la protección avanzada según sistema operativo

Comportamiento

La protección avanzada activa la monitorización de los procesos ejecutados en equipos Windows, macOS y Linux, y el envío de toda la telemetría generada a la nube de Cytomic. Esta información se incorpora a los procesos de investigación encargados de clasificar los ficheros como goodware o malware, sin ambigüedades ni lugar para sospechosos. Gracias a esta tecnología es posible detectar malware desconocido y amenazas avanzadas como APTs en equipos Windows y Linux.

Junto a las funcionalidades de detección avanzada, Cytomic ofrece el servicio Zero-Trust Application Service para equipos Windows, que clasifica todos los ficheros encontrados en el parque informático del cliente, eliminando de esta forma la categoría de “desconocidos”.

Modo de funcionamiento (Sólo Windows)

Campo	Descripción
Audit	Permite ejecutar los programas desconocidos y las amenazas detectadas. Informa del malware conocido.
Hardening	Ejecuta los programas desconocidos ya instalados en el equipo del usuario. Bloquea los programas desconocidos que vienen de fuentes no fiables como Internet, otros equipos de la red o unidades de almacenamiento externas hasta su clasificación. Los programas clasificados como malware serán desinfectados o eliminados.
Lock	Bloquea la ejecución de todos los programas desconocidos hasta que estén clasificados. Elimina o desinfecta los programas ya clasificados como malware.

Tabla 11.7: Modos de funcionamiento de la protección avanzada para Windows

- **Crear Decoy Files para ayudar a la detección de ransomware:** Crea en el equipo del usuario ficheros de control que son permanentemente monitorizados por Advanced EDR. En caso de detectarse cambios, se clasifica al proceso que lo originó como ransomware y se finaliza para evitar el cifrado masivo del sistema de ficheros.
- **Informar a los usuarios de los equipos de los bloqueos:** muestra un mensaje en el equipo del usuario con información sobre el elemento en los casos:
 - Cuando un fichero ha sido bloqueado por el módulo de protección avanzada.
 - Cuando un fichero previamente bloqueado ha sido reclasificado como goodware y el usuario puede comenzar a utilizarlo.
- **Añadir el siguiente mensaje personalizado en las alertas (opcional):** escribe un mensaje personalizado que se mostrará al usuario con el motivo de la detección o reclasificación.
- Para dejar la decisión de ejecutar o no el elemento haz clic en el selector **Dar a los usuarios de los equipos la opción de ejecutar los programas desconocidos bloqueados (recomendado sólo para usuarios avanzados o administradores)**.

Detectar actividad maliciosa (Sólo Linux)

Advanced EDR envía la telemetría obtenida de la monitorización de actividad de equipos y servidores Linux a la nube de Cytomic. Con esta información, Advanced EDR genera reglas contextuales que permiten detener amenazas avanzadas.

Campo	Descripción
Auditar	Se informa de las amenazas detectadas mediante reglas contextuales, pero no se

Campo	Descripción
	bloquean. Las amenazas detectadas mediante otras tecnologías se bloquean o desinfectan.
Bloquear	Se informa y se bloquean las amenazas detectadas mediante reglas contextuales. Activa esta opción si estás seguro de que la actividad detectada pertenece a una amenaza.
No detectar	No se informa ni se detecta el malware descubierto mediante las reglas contextuales.

Tabla 11.8: Modos de funcionamiento de la protección para Linux

Tecnología AMSI (Anti-Malware Scan Interface)

La Interfaz de examen antimalware (AMSI) de Windows es un interfaz flexible que permite a las aplicaciones y servicios integrarse con cualquier producto antimalware existente en el equipo. AMSI proporciona protección mejorada contra el malware para los usuarios finales y sus datos, aplicaciones y tareas en ejecución.



Para mas información, consulta <https://learn.microsoft.com/es-es/windows/win32/amsi/antimalware-scan-interface-portal>



Disponible solo para equipos con sistema operativo Windows instalado.

Para activar o desactivar la tecnología AMSI, desplaza el cursor deslizante **Activar análisis avanzado con AMSI** a la posición **ON**.

Exclusiones

En el caso de programas que puedan causar problemas de rendimiento al activar la tecnología AMSI, puedes excluirlos del análisis. Para ello, escribe el nombre del programa en la caja de texto y presiona la tecla Enter. Para más información sobre el comportamiento de la consola al editar exclusiones cuando la configuración está gestionada por el partner, consulta [Exclusiones establecidas por el partner](#).

Políticas avanzadas de seguridad

Las políticas avanzadas de seguridad permiten detectar y bloquear en equipos Windows la ejecución de scripts sospechosos y programas desconocidos que utilizan técnicas avanzadas de infección. Este tipo de malware supone una amenaza creciente para la seguridad del equipo.

Para activar las políticas avanzadas de seguridad haz clic en el Botón **Activar políticas avanzadas** y configura cada una de las políticas mostradas en **Modos de funcionamiento de la protección avanzada de Advanced EDR** con una de las opciones siguientes:

- **No detectar:** la política no se detecta y no genera ningún feedback al usuario ni al administrador.
- **Auditar:** la política se detecta y genera feedback al administrador en los listados y widgets de seguridad. Consulta **Visibilidad del malware y del parque informático** en la página 607.
- **Bloquear:** Advanced EDR impide la ejecución del programa.

Las políticas avanzadas de seguridad son:

Campo	Descripción
PowerShell con parámetros ofuscados	El intérprete Powershell ha recibido parámetros sospechosos que pueden derivar en la ejecución de operaciones peligrosas en el equipo protegido. Esta opción requiere activar la protección anti-exploit.
PowerShell ejecutado por el usuario	La cuenta utilizada para ejecutar el script Powershell monitorizado es de tipo interactiva y por tanto susceptible de ejecutar operaciones peligrosas en el equipo protegido. Esta opción requiere activar la protección anti-exploit.
Scripts desconocidos	Identifica y/ o bloquea los scripts que la inteligencia de seguridad de Cytomic no ha clasificado como seguros. Esta protección permite: • Aportar visibilidad al administrador sobre los scripts ejecutados en el parque informático. • Asegurar servidores bastionados donde la ejecución de programas está fuertemente restringida. • Evitar la propagación de malware en la red del cliente si existe la sospecha de haberse producido una infección. Si consideras que la protección está generando falsos positivos, considera excluir el fichero del análisis. Consulta Archivos y rutas excluidas del análisis.
Programas compilados localmente	Programas desconocidos por la inteligencia de seguridad de Cytomic que han sido creados en el equipo del usuario.
Documentos con macros	Documentos de tipo ofimático que incorporan macros y que pueden ejecutar operaciones peligrosas para el equipo protegido.
Registro para arranque al inicio	El programa monitorizado añade una rama en el registro que le permite ganar persistencia en el equipo, cargándose junto al sistema operativo en cada

Campo	Descripción
de Windows	reinicio.

Tabla 11.9: Modos de funcionamiento de la protección avanzada de Advanced EDR

Bloquear programas

Para incrementar la seguridad de partida en los equipos Windows de la red, el administrador puede decidir prohibir completamente la ejecución de ciertos programas que previamente ha clasificado como peligrosos o no compatibles con la actividad de la empresa.

Las causas que pueden llevar a un administrador a prohibir la ejecución de un determinado programa pueden ser variadas:

- Programas que por su forma de ejecución consumen mucho ancho de banda o establecen un número de conexiones desproporcionadamente alto, poniendo en peligro el rendimiento de la conectividad de la empresa si son ejecutados por muchos usuarios concurrentes.
- Programas que permiten acceder a contenidos susceptibles de contener amenazas de seguridad.
- Programas que permiten acceder a contenidos no relacionados con la actividad de la empresa y que pueden afectar al rendimiento de los usuarios.

Para crear una nueva configuración o modificar una existente introduce la información mostrada a continuación:

Campo	Descripción
Nombres de los programas a bloquear	Nombres de los ficheros que Advanced EDR impedirá su ejecución. Puedes pegar directamente una lista de nombres de ficheros separados por retorno de carro en esta caja de texto.
Código MD5 o SHA-256 de los programas a bloquear	MD5 o SHA-256 de los ficheros que Advanced EDR impedirá su ejecución. En esta caja de texto se aceptan listas de códigos MD5 o SHA-256 copiadas / pegadas y separados por retorno de carro.

Tabla 11.10: Configuración de una política de seguridad Bloquear programas

Para mostrar un mensaje emergente en el equipo del usuario o servidor haz clic en **Informar a los usuarios de los equipos de los bloqueos**. Introduce un mensaje descriptivo para informar al usuario de que un fichero se ha bloqueado. El agente Advanced EDR mostrará una ventana desplegable con el contenido del mensaje.

Anti-exploit



La tecnología anti-exploit no está disponible en sistemas Windows ARM.

La protección anti-exploit bloquea automáticamente los intentos de explotación de vulnerabilidades en los procesos instalados en el equipo del usuario, en la mayor parte de las ocasiones sin requerir intervención por su parte.

Funcionamiento de la protección anti-exploits

Los equipos de la red pueden contener procesos de origen conocido y fiable pero con fallos de programación. Son conocidos como “procesos vulnerables” debido a que interpretan de forma incorrecta ciertas secuencias de datos que reciben del usuario o de otros procesos.

Cuando un proceso vulnerable recibe un determinado patrón de información conocido por los hackers, se produce un mal funcionamiento interno que deriva en una inyección de fragmentos de código preparados por el hacker en las regiones de memoria gestionadas por el proceso vulnerable. Un proceso así afectado recibe el nombre de “proceso comprometido”. La inyección de código provoca que el proceso comprometido ejecute acciones para las que no fue programado, generalmente peligrosas y que comprometen la seguridad del equipo.

La protección anti-exploit de Advanced EDR detecta la inyección de código malicioso en los procesos vulnerables ejecutados por el usuario, bloqueándola siguiendo cursos de acción diferentes, dependiendo del tipo de exploit encontrado:

Bloqueo del exploit

Detecta la inyección de código en el proceso vulnerable cuando todavía no se ha completado. El proceso no llega a comprometerse y el riesgo del equipo es nulo, con lo que no requiere detener el proceso afectado ni reiniciar el equipo de usuario. No implica pérdida de información por parte del proceso afectado.

El usuario puede recibir una notificación del bloqueo dependiendo de la configuración establecida por el administrador.

Detección del exploit

Detecta la inyección de código en el proceso vulnerable cuando ya se ha producido. Debido a que el proceso vulnerable ya contiene el código malicioso, es imperativo cerrarlo antes de que ejecute acciones que puedan poner en peligro la seguridad del equipo.

Independientemente del tiempo transcurrido desde la detección hasta el cierre del proceso Advanced EDR considera en riesgo el equipo, aunque su cuantificación depende del tiempo transcurrido en cerrar el proceso afectado y del diseño del malware. Advanced EDR puede cerrar el proceso de forma automática para minimizar los efectos adversos, o delegar en el usuario la decisión, pidiéndole permiso de forma explícita para descargarlo de la memoria.

Si el administrador ha configurado el cierre automático para minimizar la posibilidad de efectos adversos, el usuario puede sufrir la pérdida de información manejada por el proceso afectado. Si, por el contrario, el administrador ha delegado en el usuario la decisión, el usuario podrá retrasar el cierre de la aplicación y minimizar la posibilidad perdida de información.

En los casos en que no sea posible cerrar el proceso afectado se pedirá permiso al usuario para reiniciar el equipo completo.

Bloqueo de drivers con vulnerabilidades

Los drivers suministrados por proveedores legítimos pueden poseer vulnerabilidades aprovechables por el malware para infectar el equipo o desactivar su protección.

Estos drivers no son maliciosos por sí mismos, y de hecho pueden estar instalados en los equipos sin que ello implique una amenaza de seguridad, por lo que inicialmente no son detectados como malware.

La protección anti-exploit de Advanced EDR bloquea el uso de drivers vulnerables, excepto cuando el driver se carga en el proceso de inicio del sistema operativo.

Compatibilidad de la tecnología anti - exploit

Cyatomic sigue todas las recomendaciones de los fabricantes de sistemas operativos para asegurarse de que sus productos de seguridad coexisten en el equipo del cliente sin problemas con otras soluciones antivirus y EDR. No obstante, la implementación del módulo anti - exploit se realiza mediante hooks. Si existen varias soluciones de seguridad instaladas en el equipo que utilizan esta tecnología de interceptación, es posible que sean incompatibles. Para solucionar esta situación desactiva todas las tecnologías basadas en hooks del producto de seguridad en el equipo del usuario.

En Advanced EDR las tecnologías que utilizan hooks son:

- Anti - exploit
- Inyección avanzada de código
- IOAs avanzados. Consulta [Compatibilidad de los IOAs avanzados con soluciones de seguridad de terceros](#) en la página **558**

Configuración de la detección anti - exploits

Inyección de código

- Para activar la protección anti-exploit, desplaza el cursor deslizante a la posición **ON**.
- **Exclusiones para la inyección de código:** puedes excluir los procesos no compatibles con la protección anti-exploit. Para excluir un proceso, escribe su nombre en la caja de texto **Procesos excluidos** y presiona la tecla Enter.
- **Modo de funcionamiento (Sólo Windows):**

Campo	Descripción
Auditar	Notifica en la consola Web la detección del exploit, pero no toma acciones contra él ni informa al usuario del equipo.
Bloquear	Bloquea los ataques de tipo exploit. Puede requerir el cierre del proceso afectado por el exploit. • Informar del bloqueo al usuario del equipo: el usuario recibe una notificación, pero el proceso comprometido se cierra de forma automática si es necesario. • Pedir permiso al usuario: el usuario recibe una petición de autorización para el cierre del proceso comprometido por el exploit en caso de ser necesario. Esta opción resulta útil para que el usuario pueda salvar la información antes producirse el cierre del proceso. Si se requiere el reinicio del equipo siempre se pide confirmación al usuario, independientemente de la configuración Pedir permiso al usuario.

Tabla 11.11: Modo de funcionamiento de la protección avanzada anti-exploit en Advanced EDR



Dado que muchos exploits continúan ejecutando código malicioso hasta que no se produce el cierre del proceso, la incidencia no se marcará como resuelta en el panel de elementos maliciosos y exploit de la consola web hasta que el programa haya sido cerrado.

Driver vulnerable

- Para activar el bloqueo de drivers con vulnerabilidades, desplaza el control deslizante **Detectar drivers con vulnerabilidades** a la posición **ON**.
- **Modo de funcionamiento (Sólo Windows):**

Campo	Descripción
Auditar	Notifica la detección en la consola web de Cytomic , pero no toma acciones al respecto.
Bloquear	Notifica la detección en la consola web de Cytomic , bloquea la carga de los drivers y muestra un aviso en el equipo afectado.

Tabla 11.12: Modo de funcionamiento del bloqueo de drivers con vulnerabilidades en Advanced EDR

Protección contra ataques de red

Muchos incidentes de seguridad comienzan con ataques que explotan vulnerabilidades en servicios expuestos a Internet. Si, posteriormente, los atacantes logran su objetivo y la organización ya está infectada, también es necesario detener el ataque dentro de la red corporativa.

La Protección contra ataques de red detecta y detiene amenazas al analizar el tráfico de red en tiempo real, evitando los ataques que aprovechan las vulnerabilidades en los servicios expuestos a Internet y en la red interna.

Para más información sobre las detecciones soportadas por Protección contra ataques de red consulta <https://www.pandasecurity.com/es/support/card?id=700145>.

Campo	Descripción
Bloquear	Bloquea el tráfico que forman parte de un ataque de red. Es la opción predeterminada.
Auditar	Notifica en la consola Web la detección del ataque de red, pero no toma acciones contra él ni informa al usuario del equipo.

Tabla 11.13: Modo de funcionamiento de la protección avanzada Protección contra ataques de red en Advanced EDR

Privacidad

Advanced EDR incluye el nombre, la ruta completa de los ficheros y el usuario que inició la sesión en el equipo cuando envía los archivos a la nube de Cytomic para su análisis. Esta información se utiliza posteriormente en los informes y las herramientas de análisis forense mostrados en la consola Web. Para no enviar que esta información desactiva la casilla apropiada en la pestaña **Privacidad**.

Uso de la red

Advanced EDR comprime y envía a la nube de Cytomic los ficheros ejecutables desconocidos para su análisis en el laboratorio. El tamaño máximo del fichero comprimido que el agente puede enviar es de 50 MBytes.

El impacto en el ancho de banda de la red del cliente está configurado de forma predeterminada para pasar desapercibido:

- Se envía un máximo de 50 Mbytes por hora y agente.
- Un fichero concreto desconocido se envía una sola vez para todos los clientes que usan Advanced EDR.
- Se implementan mecanismos de gestión del ancho de banda con el objetivo de evitar un uso intensivo de los recursos de red.

Para configurar el número máximo de megabytes que un agente podrá enviar en una hora introduce el valor y haz clic en **Ok**. Para establecer transferencias ilimitadas deja el valor a 0.

Modo auditoría

El modo auditoría permite monitorizar los procesos ejecutados en equipos Windows macOS y Linux y detectar y notificar la existencia de amenazas en ellos.

Al activar el modo auditoría en una configuración, no se modifica el estado global de las diferentes protecciones en los equipos asignados a esa configuración, ni la configuración de las protecciones en la consola web. Las protecciones continúan detectando amenazas en los equipos e informando de ellas, pero no se llevan a cabo labores de bloqueo o desinfección.



Se recomienda limitar al máximo la activación del modo auditoría para minimizar el tiempo de exposición de los equipos frente a las amenazas detectadas.

Para activar el modo auditoría:

- Selecciona el menú superior **Configuración**, y después menú lateral **Estaciones y servidores**
- Haz clic en la configuración en la que quieres activar el modo auditoría. Para crear una configuración, consulta [Crear y gestionar configuraciones](#) en la página 258.
- Haz clic en **Modo auditoría**, y desplaza el control deslizante.
- Haz clic en el botón **Guardar**. En la parte superior de la ventana **Editar configuración** se mostrará un aviso indicando que el modo auditoría ha sido activado para esta configuración y el riesgo que supone.

Visualizar los equipos en modo auditoría

En el widget **Estado de protección** se muestra el número de equipos que tienen activado el modo auditoría. Al hacer clic en el texto, accederás al listado **Riesgos por equipo** filtrado por el riesgo **Modo auditoría activado**.

Para más información, consulta [Paneles/Widgets del módulo de seguridad](#) en la página 608 y [Listados del módulo Evaluación de riesgos](#) en la página 651.

Modo detallado

El modo detallado permite que un reducido número de equipos de la red generen telemetría ampliada durante un intervalo de tiempo acotado. El administrador puede analizar esta nueva información para considerar qué elementos del software de seguridad se están utilizando cuando se genera un IOA.

El modo detallado se utiliza fundamentalmente para evaluar las capacidades del software de seguridad en un entorno de pruebas donde se simulen ataques a la infraestructura IT administrada.

Para visualizar tanto la telemetría normal como la ampliada consulta [Sección Investigación \(5\)](#) en la página [238](#).

Requisitos y limitaciones del modo detallado

El modo detallado recoge y envía a la nube una gran cantidad de telemetría por cada equipo configurado en este modo. Para evitar un impacto negativo en el rendimiento, Advanced EDR implementa las siguientes limitaciones:

- Máximo número de equipos configurados en modo detallado simultáneamente: 20 equipos.
- Duración máxima del modo detallado: 7 días.
- Solo en los equipos en modo auditoría se puede activar el modo detallado.
- El modo detallado solo está disponible en equipos Windows.

Los requisitos para poder asignar a un equipo el modo detallado son:

- Permiso **Configurar seguridad para estaciones y servidores**. Consulta [Gestión de roles y permisos](#) en la página [67](#).
- Modo auditoría asignado. Consulta [Modo auditoría](#).

Activar y desactivar el modo detallado



*Comprueba que el equipo tiene asignada una configuración de **Estaciones y servidores** con el modo auditoría activado. Si el equipo no cumple con este requisito el modo detallado no estará disponible. Consulta [Modo auditoría](#).*

Para activar el modo auditoría:

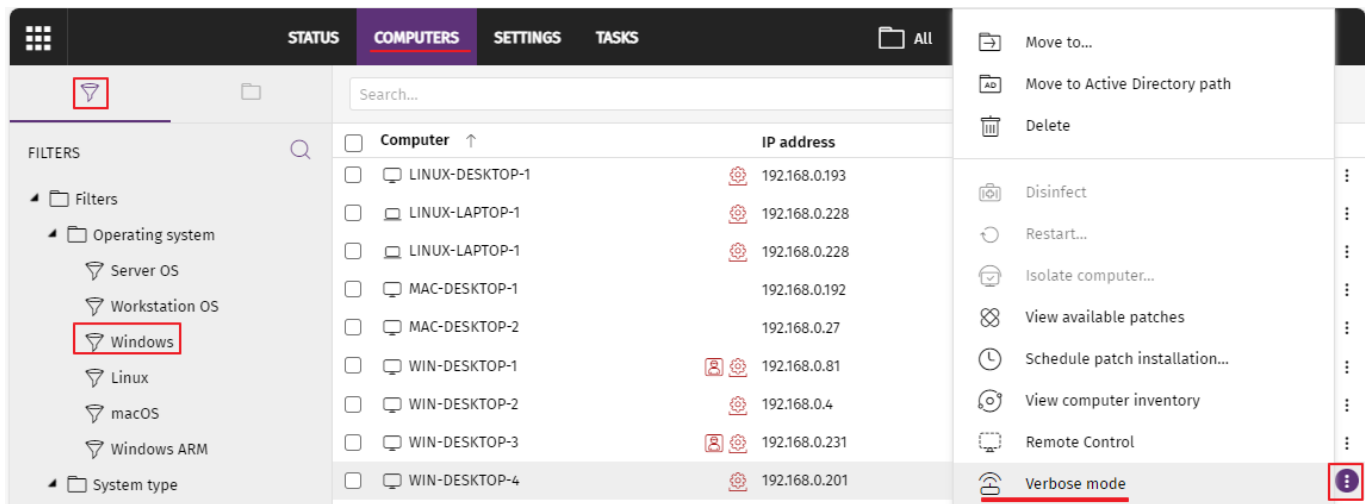


Figura 11.1: Listado de equipos filtrado por plataforma Windows

- En el menú superior haz clic en **Equipos**. Se abrirá la ventana **Equipos**.
- En el panel izquierdo haz clic en la pestaña **Filtros** . Se mostrarán los filtros configurados.
- Selecciona un filtro que muestre los equipos Windows (por ejemplo **Windows**). El listado se actualizará para mostrar todos los equipos administrados.
- Para abrir el menú de contexto del equipo donde quieres configurar el modo detallado, haz clic en el icono  asociado al equipo.
- Selecciona **Modo Detallado** . Se abrirá la ventana **Activar modo detallado**.
- En el desplegable **Introduce la duración** del modo detallado.
- Haz clic en el botón **Activar modo detallado**. Se añadirá el icono  en el listado asociado al equipo.

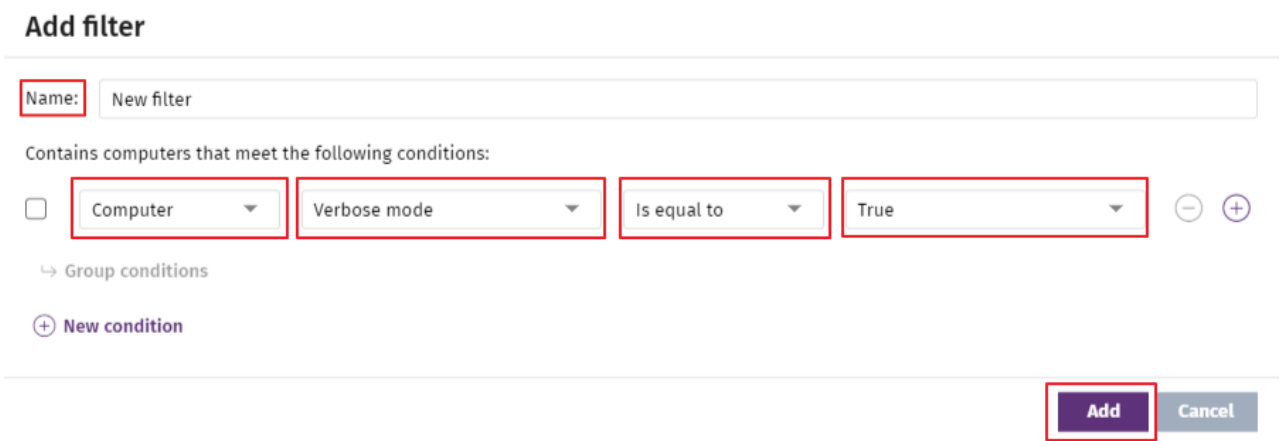
Para desactivar el modo auditoría:

- En el menú superior haz clic en **Equipos**. Se abrirá la ventana **Equipos**.
- Selecciona un filtro que muestre los equipos Windows (por ejemplo **Windows**). El listado se actualizará para mostrar todos los equipos administrados.
- Haz clic en el icono  asociado al equipo del que quieres eliminar el modo detallado. El equipo tendrá el icono .
- Selecciona **Desactivar modo Detallado** . El icono  asociado al equipo se eliminará.

Visualizar los equipos en modo detallado

Los equipos en modo detallado se muestran en el listado de equipos con el icono .

Para listar únicamente los equipos en modo detallado puedes crear un filtro:



Add filter

Name:

Contains computers that meet the following conditions:

☐ Computer Verbose mode Is equal to True − +

↳ Group conditions

+ New condition

Add **Cancel**

Figura 11.2: Listado filtrado por equipos en modo detallado

- En el menú superior haz clic en **Equipos**. Se abrirá la ventana **Equipos**.
- En el panel izquierdo haz clic en la pestaña **Filtros** . Se mostrarán los filtros configurados.
- En la carpeta **Sistema operativo** haz clic en el icono . Se abrirá un menú de contexto.
- Selecciona **Añadir filtro**. Se abrirá la ventana **Añadir filtro**.
- En la caja de texto escribe el **Nombre** del filtro.
- En el desplegable **Selecciona una categoría**, elige **Equipo**.
- En el desplegable **Selecciona una propiedad**, elige **Modo detallado**.
- En el desplegable **Selecciona un operador**, elige **Es igual A**.
- En el desplegable **Selecciona un valor** selecciona **Verdadero**.
- Haz clic en el botón **Añadir**. El filtro se creará y se aplicará en el listado de equipos, mostrando únicamente los que tienen el modo detallado activado.

Capítulo 12

Cytomic Data Watch (Supervisión de información sensible)

Los ficheros clasificados como PII (Personally Identifiable Information) son archivos sin estructura interna con información que permite identificar a personas relacionadas con la empresa (clientes, trabajadores, proveedores, etc.). Esta información es de carácter personal y su tipo es muy variado, como pueden ser números de la seguridad social, números de teléfono y direcciones de correo electrónico, entre otros.

Cytomic Data Watch es el módulo de seguridad de Advanced EDR que permite a las empresas cumplir con las regulaciones sobre protección de datos, como por ejemplo la GDPR. Además, supervisa y mejora la visibilidad de la información personal (PII) almacenada en la infraestructura IT de las organizaciones.

Para ello, Cytomic Data Watch ofrece tres funcionalidades clave:

- Genera un inventario diario y completo de ficheros PII que incluye información básica, como puede ser su nombre, extensión y el nombre del equipo donde se encontró.
- Descubre, audita y monitoriza en tiempo real el ciclo de vida de los ficheros PII: desde los datos en reposo, las operaciones efectuadas sobre ellos y su llegada y comunicación hacia el exterior.
- Ofrece herramientas de búsqueda flexible por contenido y borrado de ficheros duplicados que contienen datos personales, con el objetivo de limitar su almacenamiento y difusión en la red de la empresa.



Para obtener información adicional sobre los distintos apartados del módulo Cytomic Data Watch consulta las referencias siguientes:

Crear y gestionar configuraciones en la página **258** información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.

Acceso, control y supervisión de la consola de administración en la página **59**: gestión de cuentas de usuario y asignación de permisos.

Gestión de listados en la página **47**: información sobre como gestionar listados.



Consulta la **Guía de administración de Cytomic Data Watch** para obtener más información sobre la consola de gestión específica para este servicio.

Contenido del capítulo

Introducción al funcionamiento de Cytomic Data Watch	312
Requisitos de Cytomic Data Watch	315
El proceso de indexación	315
Inventario de ficheros PII	316
Monitorización continua de ficheros	317
Búsqueda de ficheros	317
Búsqueda de ficheros duplicados	328
Borrado y restauración de ficheros	329
Configuración de Cytomic Data Watch	332
Paneles / widgets del módulo Cytomic Data Watch	337
Listados del módulo Cytomic Data Watch	350
Extensiones de programas soportadas	370
Empaquetadores y algoritmos de compresión soportados	372
Entidades y países soportados	373

Introducción al funcionamiento de Cytomic Data Watch

Para una correcta comprensión de los procesos involucrados en el descubrimiento y seguimiento de la información personal almacenada en los equipos de la empresa, es necesario asimilar algunos conceptos relativos a las tecnologías utilizadas en Cytomic Data Watch.

Entidad

Cada pieza o grupo de palabras con significado propio referido a un tipo concreto de información personal recibe el nombre de “entidad”. Entidades comúnmente analizadas son el DNI, nombres y apellidos y

números de teléfono, entre otras.

Debido a la naturaleza ambigua y variable del lenguaje natural en sus múltiples idiomas, una misma entidad puede presentarse de formas muy diferentes, por lo que es necesario aplicar algoritmos flexibles y adaptables para su detección. De manera general, el análisis de entidades busca formatos o expresiones predefinidas, y utiliza el contexto local en torno a esa detección, o la presencia o ausencia de determinadas palabras clave, para evitar falsos positivos. Consulta [Entidades y países soportados](#) para más información.

Fichero PII

Una vez realizada la identificación de entidades se evalúa el contexto en el que aparecen para determinar si con la información que aportan es posible identificar a una persona concreta. En tal caso, el fichero será susceptible de ser protegido por protocolos específicos de tratamiento y acceso a los datos que permitan a la empresa cumplir con la normativa vigente (GDPR, PCI, etc.). Esta evaluación combina un modelo Machine learning supervisado con un modelo experto basado en ponderación de entidades y análisis del contexto global del documento, para clasificar a un fichero con entidades detectadas como un fichero PII a proteger.

Ficheros sin estructura interna y componentes IFilter

Para clasificar un fichero como PII, Cytomic Data Watch analiza archivos sin estructura (ficheros de texto en múltiples formatos, hojas de cálculo, ficheros de presentación Powerpoint etc.) en busca de entidades. Para interpretar correctamente el contenido de estos archivos se requieren algunos componentes de terceros fabricantes instalados en el equipo del usuario. Estos componentes reciben el nombre de "IFilters" y no forman parte del paquete de instalación de Advanced EDR. Microsoft Search, Microsoft Exchange Server y Microsoft Sharepoint Server, entre otros servicios del sistema operativo y productos independientes, utilizan los componentes IFilter para indexar los ficheros del usuario y habilitar búsquedas por contenido.

Cada formato de fichero compatible con Cytomic Data Watch tiene su propio componente IFilter asociado, y muchos de ellos forman parte de la instalación básica de Windows, aunque otros tienen que ser instalados o actualizados de forma manual.

Microsoft Filter Pack es un paquete de distribución gratuito que contiene todos los componentes IFilter asociados a la suite de ofimática Microsoft Office. Una vez instalado, Cytomic Data Watch será capaz de analizar el contenido de todos los formatos de fichero soportados por la suite. Consulta [Instalación del componente Microsoft Filter Pack](#) para más información.

Proceso de indexación

Es el proceso de inspección y almacenaje del contenido de todos los ficheros soportados por Cytomic Data Watch con el fin de generar un inventario de ficheros PII y permitir búsquedas de ficheros por contenido. El proceso de indexación es una tarea de bajo impacto en el rendimiento del equipo, aunque su finalización puede alargarse en el tiempo. Por esta razón el administrador puede programar su inicio o limitarla para acelerar su finalización y para mejorar el resultado de los resultados devueltos por las búsquedas. Consulta [El proceso de indexación](#) para más información.

Proceso de normalización

Al ejecutar el proceso de indexación Cytomic Data Watch aplica ciertas reglas para homogeneizar los datos recogidos. El objetivo de este proceso es almacenar de forma individual cada palabra y facilitar su posterior búsqueda, así como reducir su tiempo de ejecución. Las reglas a aplicar en el proceso de normalización varían si se trata de almacenar una entidad o texto plano. Consulta [Propiedades y requisitos de las búsquedas](#) para más información.

Inventario de ficheros PII

Una vez indexado el equipo e identificadas las entidades y los ficheros PII, Cytomic Data Watch construye un inventario accesible por el administrador de la red con los nombres de los ficheros y sus características, que se envía al servidor Advanced EDR una vez al día. Consulta [Inventario de ficheros PII](#) para más información.



Cytomic Data Watch no envía el contenido de los ficheros PII al servidor Advanced EDR. Únicamente se envían sus atributos (nombre, extensión etc.) y el número y tipo de entidades descubiertas.

Búsquedas de ficheros

Cytomic Data Watch localiza ficheros por su nombre, extensión o contenido en las unidades de almacenamiento indexadas de los equipos de la red.

Las búsquedas se ejecutan en tiempo real: tan pronto como el administrador lanza una búsqueda, ésta se despliega en los equipos de la red y comienza a reportar resultados conforme se van produciendo, sin esperar a completar la ejecución por completo. Consulta [Búsqueda de ficheros](#) para más información.

Seguimiento de las acciones sobre ficheros PII

Cytomic Data Watch monitoriza los eventos realizadas sobre los ficheros PII y los envía a la consola Cytomic Insights. Esta herramienta muestra la evolución de los ficheros PII permitiendo determinar si fueron copiados, movidos, enviados por correo, etc. Para obtener más información sobre Cytomic Insights consulta la Guía de administración de Cytomic Data Watch en <https://info.cytomicmodel.com/resources/guides/DataWatch/es/DATAWATCH-guia-ES.pdf>.

Requisitos de Cytomic Data Watch

Plataformas soportadas



A partir de la fecha 30/09/2024 no será posible añadir a la consola de administración nuevos equipos que utilicen los siguientes sistemas operativos: Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008 (no afecta a Windows Server 2008 R2). Los equipos instalados en una fecha anterior seguirán protegidos. Consulta <https://www.watchguard.com/wgrd-trust-center/end-of-life-policy>.

Cytomic Data Watch es compatible con la plataforma Microsoft Windows desde la versión XP SP3 en adelante y Windows 2003 SP1 y superiores. Otros sistemas operativos como Linux o macOS no están soportados.

Instalación del componente Microsoft Filter Pack

Microsoft Filter Pack y Microsoft Office

El componente Microsoft Filter Pack viene incluido en la suite de ofimática Office, aunque solo se instalarán de forma automática los componentes IFilter que se corresponden con los productos de la suite instalados en el equipo del usuario. Para tener la seguridad de que todos los componentes estén disponibles en el equipo en su versión 2010, consulta el punto [Instalación independiente del Microsoft Filter Pack](#).

Instalación independiente del Microsoft Filter Pack

Para instalar el Microsoft Filter Pack haz clic en la siguiente URL:

<https://www.microsoft.com/en-us/download/details.aspx?id=17062>

El paquete es compatible con Windows XP SP3, Windows 2013 SP1 y superiores, aunque en algunos casos se requerirá la instalación de la librería Microsoft Core XML Services 6.0.

El proceso de indexación

Es el proceso de inspección y almacenaje del contenido de todos los ficheros soportados por Cytomic Data Watch. Este proceso es imprescindible para poder generar el inventario de ficheros PII y también para buscar ficheros en los equipos por su contenido, y se configura de forma transparente al activar alguna de estas dos funcionalidades. La información indexada se almacena de forma local en el equipo de cada usuario en la ruta `%ProgramData%\Panda Security\Panda Security Protection\indexstore`.

Aunque el proceso de indexado es una tarea de bajo impacto en el rendimiento del equipo, puede alargarse en el tiempo. Por esta razón, Cytomic Data Watch está configurado para lanzar una única vez el proceso en

el momento en que se activa el módulo en cada equipo de la red, y cada vez que la tecnología de detección de entidades cambie para soportar mejoras.

Una vez terminada la indexación, Cytomic Data Watch comienza a monitorizar la creación de nuevos ficheros y el borrado y modificación de los ya existentes para actualizar el índice. La información con las nuevas entidades detectadas se envía al servidor Advanced EDR cada 24 horas.

Configurar el alcance, momento y tipo de indexación

Es posible excluir los resultados de ciertas carpetas o ficheros, o incluso variar la precisión de las búsquedas devueltas por Cytomic Data Watch.

- Para no devolver información de ciertas carpetas o ficheros consulta [Exclusiones](#).
- Para variar la precisión de las búsquedas consulta [Indexar el siguiente contenido](#).
- Para determinar la franja horaria en la que se ejecutará el proceso de indexado consulta [Programar períodos de indexación](#).

Inventario de ficheros PII



Cytomic Data Watch no envía el contenido de los ficheros PII al servidor Advanced EDR. Únicamente se envían sus atributos (nombre, extensión etc.) y el número y tipo de entidades descubiertas.

El inventario de ficheros PII muestra los ficheros PII que Cytomic Data Watch ha encontrado en la red del cliente.

Para activar el inventario consulta [Información personal \(inventario, búsquedas y seguimiento\)](#) para más información.

Visualizar el inventario

Cytomic Data Watch incorpora varios recursos para controlar los ficheros PII encontrados en la red y determinar el tipo de entidades que contienen.

- Para obtener estadísticas del número de ficheros PII encontrados consulta [Archivos con información personal](#) para más información.
- Para obtener estadísticas del número de equipos con ficheros PII encontrados consulta [Equipos con información personal](#) para más información.
- Para obtener un listado con el detalle de los ficheros PII encontrados consulta [Archivos con información personal](#) para más información.
- Para obtener un listado con el detalle de los equipos que contienen ficheros PII consulta [Equipos con información personal](#) para más información.

Monitorización continua de ficheros

Monitorización de ficheros PII

Cytomic Data Watch recopila todos los eventos relativos a la creación, modificación o borrado de ficheros PII para poder visualizar la actividad realizada y detectar situaciones peligrosas, tales como robo de datos, acceso no autorizada a información, etc.

Para visualizar las acciones realizadas sobre los ficheros PII accede a **Cytomic Insights** desde la parte inferior del panel lateral del menú superior **Estado**. Consulta la Guía para el usuario de Cytomic Data Watch en <https://info.cytomicmodel.com/guides/DataWatch/es/DATAWATCH-guia-ES.pdf> para obtener toda la información necesaria.

Para activar la monitorización de las acciones efectuadas sobre los ficheros PII consulta [Información personal \(inventario, búsquedas y seguimiento\)](#).

Monitorización de ficheros designados por el administrador

Además de monitorizar de forma automática los ficheros clasificados por Cytomic Data Watch como PII, el administrador puede añadir mediante reglas nuevos tipos de ficheros para monitorizar. Consulta [Monitorización de archivos por reglas](#) para más información.

Búsqueda de ficheros

Requisitos de las búsquedas

Para realizar una búsqueda de ficheros en los equipos de la red es necesario cumplir con los siguientes requisitos:

- La cuenta de usuario que lanza la búsqueda desde la consola web tiene que tener asignado un rol con el permiso **Buscar información en los equipos**. Consulta [Acceso, control y supervisión de la consola de administración](#) en la página 59 para obtener más información sobre los roles.
- Los equipos sobre los que se ejecutan las búsquedas deben de contar con una licencia de Cytomic Data Watch asignada.
- Los equipos sobre los que se ejecutan las búsquedas deben de tener asignada una configuración de Cytomic Data Watch con la opción **Permitir realizar búsquedas de información en los equipos** habilitada. Consulta [Configuración de Cytomic Data Watch](#)

Widget de búsquedas

Es el punto de entrada para toda la funcionalidad, y permite visualizar búsquedas y gestionarlas.

Para acceder al widget **Búsquedas** haz clic en el menú superior **Estado**, panel lateral **Cytomic Data Watch**

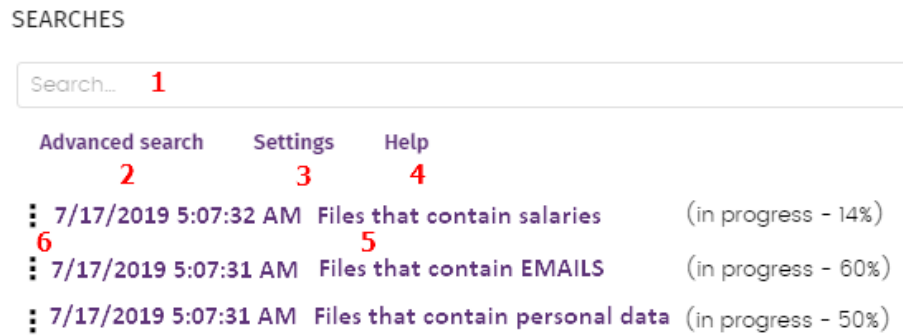


Figura 12.1: Panel Búsquedas

El widget contiene los controles mostrados a continuación:

- (1) Caja de texto para introducir los términos a buscar. Consulta [Sintaxis de las búsquedas](#) para una descripción de los comandos aceptados por Cytomic Data Watch.
- (2) **Búsqueda avanzada**: limita el ámbito de búsqueda.
- (3) **Configuración**: acceso al listado de perfiles de configuración de Cytomic Data Watch. Para más información consulta [Configuración de Cytomic Data Watch](#).
- (4) **Ayuda**: enlace a la página web de soporte de Cytomic donde se muestra la sintaxis de las búsquedas de Cytomic Data Watch actualizada con los últimos cambios introducidos.
- (5) **Búsquedas almacenadas**: búsquedas definidas anteriormente y que pueden ser relanzadas en el parque informático.
- (6) **Menú de contexto de la búsqueda**: permite editar el nombre de la búsqueda, cambiar sus parámetros, volverla a lanzar y eliminarla.

Propiedades y requisitos de las búsquedas

Para completar con éxito una búsqueda es necesario cumplir con los siguientes requisitos:

- La cuenta de usuario que lanza la búsqueda desde la consola web tiene que tener asignado un rol con el permiso **Buscar información en los equipos**. Consulta [Acceso, control y supervisión de la consola de administración](#) en la página 59 para obtener más información sobre los roles.
- Los equipos sobre los que se efectúan las búsquedas deben de contar con una licencia de Cytomic Data Watch asignada.
- Los equipos sobre los que se efectúan las búsquedas deben de tener asignada una configuración de Cytomic Data Watch con la opción **Permitir realizar búsquedas de información en los equipos** habilitada.

Propiedades de las búsquedas

- El número de búsquedas concurrentes por cada cuenta de usuario es 10. Pasado este número se mostrará un mensaje de error en la consola web.

- El número máximo de búsquedas guardadas por cuenta de usuario es 30. Pasado este número se mostrará un mensaje de error en la consola web.
- El número máximo de resultados en total por cada búsqueda es 10.000. Los resultados más allá de este número no se mostrarán en la consola web.
- El número máximo de resultados por cada equipo es 10.000 / número de equipos sobre los que se ejecuta la búsqueda. De esta forma, si se busca sobre un parque de 100 equipos, el número máximo de resultados mostrados será $10.000 / 100 = 100$ resultados por equipo.
- El número mínimo de resultados mostrados por equipo, independientemente del número de equipos de la red es 10.
- El número máximo de equipos sobre los que se ejecutan búsquedas de forma simultánea es 50. Si el número total de equipos que participaran en la búsqueda es mayor, las búsquedas más allá de este límite se mantendrán en espera hasta que las primeras se vayan completando.

Proceso de normalización



El proceso de normalización no influye en la detección de entidades.

Cytomic Data Watch aplica una serie de reglas a los datos recibidos del proceso de indexación para homogeneizarlos. Debido a que las búsquedas ejecutadas por el administrador se aplican sobre los datos ya normalizados, es necesario conocer estas reglas dado que pueden influir en los resultados mostrados en la consola web.

Transformación de las cadenas a minúsculas

Antes de almacenar una cadena en la base de datos, ésta se transforma a minúsculas.

Caracteres de separación

Cytomic Data Watch detecta un grupo de caracteres especiales que considera como separadores entre palabras y que retira completamente del índice, excepto si esos caracteres forma parte de una entidad:

- **Retorno de carro:** \r
- **Salto de línea:** \n
- **Tabulador:** \t
- **Caracteres:** " : ; ! ? - + _ * = () [] { } , . | % \ / ' "

Por ejemplo "Cytomic.Data(Watch" se almacenará como tres palabras sueltas sin los caracteres de puntuación: "cytomic", "data" y "watch".

Normalización de entidades

El proceso de normalización de entidades sigue reglas independientes:

Entidad	Caracteres de separación	Configuración de la indexación
• Cuentas bancarias • Tarjetas de crédito • Número de identidad personal • Números de teléfono • Números de carnet de conducir • Números de pasaporte • Números de la seguridad social	Se eliminan. La entidad se almacena en el índice como un único elemento.	No se tiene en cuenta
• Direcciones IP • Direcciones de correo electrónico	Se respetan. La entidad se almacena en el índice como un único elemento.	No se tiene en cuenta
• Nombres y apellidos • Direcciones físicas	Se utilizan como carácter separador. La entidad se almacena en el índice como varios elementos.	Si se tiene en cuenta

Tabla 12.1: Reglas de normalización de entidades

Ejemplos de normalización de entidades

- “1.42.67.116-C” se almacena como la entidad de tipo IDCARD “14267116C”.
- “192.168.1.1” se almacena como la entidad de tipo IP “192.168.1.1”.
- “Calle Santiago de Compostela 5 1º Izquierda” se almacenará como “calle”, “santiago”, “de”,

“compostela”, “izquierda” si el método de indexación es **Solo texto** o como “calle”, “santiago”, “de”, “compostela”, “5”, “1”, “izquierda” si el método de indexación es **Todo**.

Crear una búsqueda

Crear una búsqueda libre

- Haz clic en el menú superior **Estado**, panel lateral **Cytomic Data Watch**.
- Introduce en la caja de texto del widget **Búsquedas** los términos de búsqueda según la sintaxis mostrada en [Sintaxis de las búsquedas](#).
- Haz clic en el icono  o pulsa la tecla Enter.

Una vez introducida la búsqueda se abrirá la ventana **Resultados de la búsqueda**. Consulta [Búsquedas almacenadas](#) para editar la búsqueda introducida.

Crear una búsqueda guiada

- Haz clic en el menú superior **Estado**, panel lateral **Cytomic Data Watch**.
- Haz clic en el enlace **Búsqueda avanzada**.
- Elige en el selector **Búsqueda guiada**.
- Configura los parámetros de la búsqueda.

Parámetros de búsqueda avanzada:

Parámetro	Descripción
Nombre de la búsqueda	Establece un nombre para la búsqueda almacenada.
Buscar archivos con	Introduce el contenido a buscar. Se incluyen tres cajas de texto. • Todas estas palabras o frases exactas: busca los ficheros que contienen todas las palabras o entidades indicadas. • Alguna de estas palabras o frases exactas: busca los ficheros que contienen alguna o todas las palabras o entidades indicadas. • Ninguna de estas palabras o frases exactas: busca los ficheros que no contienen ninguna de las palabras.
Información personal	Marca las casillas de selección para indicar las entidades que deberán aparecer en los ficheros PII buscados. • Todos: todas las entidades seleccionadas deberán detectarse en el fichero PII (lógica AND) para que el fichero se incluya en la lista de

Parámetro	Descripción
	encontrados. • Alguno: algunas o todas las entidades seleccionadas deberán detectarse en el fichero PII (lógica OR) para que el fichero se incluya en la lista de encontrados.
Limitar la búsqueda a	Equipos: • Todos: busca el contenido introducido en todos los equipos que tengan una licencia de Cytomic Data Watch asignada y esté habilitada la opción de búsqueda en su configuración. • Los siguientes equipos: muestra un listado de los equipos que tengan una licencia de Cytomic Data Watch asignada. Indica con las casillas de selección los equipos en los que se buscará el contenido introducido. • Los siguientes grupos de equipos: muestra el árbol de grupos con la jerarquía de equipos configurada en Advanced EDR. Indica con la casilla de selección los grupos donde se buscará el contenido introducido.
Cancelar automáticamente la búsqueda	Indica el tiempo de espera para los equipos apagados o sin conexión antes de cancelar la búsqueda.

Tabla 12.2: Parámetros de la búsqueda avanzada

Búsquedas almacenadas

Tanto las búsquedas libres como las guiadas se almacenan para poder ser lanzadas posteriormente de forma rápida.

Una vez creada una nueva búsqueda, ésta aparecerá en el widget **Búsquedas** con la fecha y hora de su creación, junto al nombre y una leyenda indicando su estado (**En curso**, **Cancelada**) o sin estado (**Finalizada**).

Cambiar el nombre de una búsqueda almacenada

Haz clic en el menú de contexto (6 en **Panel Búsquedas**) de la búsqueda y elige **Cambiar nombre**.

Hacer una copia de una búsqueda almacenada

Para duplicar una búsqueda almacenada haz clic en el menú de contexto (6 en **Panel Búsquedas**) de la búsqueda y elige **Hacer una copia**. Se mostrará la ventana de configuración de la búsqueda y se renombrará a "Copia de ".

Volver a lanzar una búsqueda almacenada

Haz clic en el menú de contexto de la búsqueda (6 en **Panel Búsquedas**) y elige **Relanzar búsqueda**. El estado de la búsqueda cambiará e indicará el porcentaje de la tarea realizada.

Cancelar y eliminar búsquedas almacenadas

Haz clic en el menú de contexto de la búsqueda (6 en **Panel Búsquedas**) y elige **Cancelar** para interrumpir la búsqueda o en **Borrar** para cancelarla y borrarla del widget **Búsquedas**.

Editar búsquedas almacenadas

Haz clic en el menú de contexto (6 en **Panel Búsquedas**) y elige **Editar búsqueda** para abrir la ventana de búsqueda avanzada con sus parámetros cargados y modificarla.

Visualizar los resultados de una búsqueda

Para visualizar el resultado de una búsqueda accede al listado **Buscar en los equipos** de dos formas:

- Haciendo clic en una búsqueda almacenada.
- Creando una nueva búsqueda.

Este listado muestra los equipos que contienen la cadena de búsqueda introducida, junto al nombre del fichero encontrado y otra información útil.

Cabecera de listado

Configura los parámetros de la búsqueda rápida:

The screenshot shows a search results interface. At the top, there's a title bar with a back arrow, the text "Search results 'Files that contain salaries'", an edit icon, and a red number "1". Below this is a search bar containing "+salary" with a red "2" next to it. To the right of the search bar is a blue button labeled "Search on: '7 computers'" with a red "3" next to it. Below the search bar is a progress bar labeled "Searching:" with a blue progress indicator, a gear icon, the word "Cancel" with a red "4" next to it, and a link "More information". Below the progress bar is another search bar labeled "Search..." with a red "5" next to it and a magnifying glass icon. To the right of this search bar is a blue icon of a document with an arrow. Below the search bars is a table with the following columns: File, Computer ↑, Group, and Path. The table contains one row with the following data: Salaries2018, WIN_DESKTOP_1, Workstation, and C:\Data\2018\HR.

File	Computer ↑	Group	Path
Salaries2018	WIN_DESKTOP_1	Workstation	C:\Data\2018\HR

Figura 12.2: Ventana Resultados de una búsqueda

- (1) **Icono** : cambia el nombre de la búsqueda.
- (2) **Caja de texto**: contenido de la búsqueda.
- (3) **Buscar en: "x equipos"**: abre la ventana de búsqueda avanzada para refinarla.
- (4) **Buscando**: estado de la búsqueda (**En curso**, **Cancelada**). Si la búsqueda no se ha iniciado o ha terminado no se indica el estado.

- **(5) Caja de texto Buscar:** filtra los resultados mostrados en la tabla de resultados por el nombre de equipo.

Campos del listado

Campo	Comentario	Valores
Archivo	Nombre del fichero encontrado.	Cadena de caracteres
Equipo	Nombre del equipo donde se encontró el fichero.	Cadena de caracteres
Grupo	Grupo de Advanced EDR al que pertenece el equipo.	Cadena de caracteres
Ruta	Ruta dentro del dispositivo de almacenamiento donde se encuentra el fichero.	Cadena de caracteres

Tabla 12.3: Campos del listado Búsqueda de información personal en los equipos

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Archivo	Nombre del fichero encontrado.	Cadena de caracteres
Equipo	Nombre del equipo donde se encontró el fichero.	Cadena de caracteres
Grupo	Grupo de Advanced EDR al que pertenece el equipo.	Cadena de caracteres
Ruta	Ruta dentro del dispositivo de almacenamiento donde se encuentra el fichero.	Cadena de caracteres
DNIs	Indica si se detectó una o más entidades del tipo Documento Nacional de Identidad o equivalentes (Documento de identidad, Cédula de identidad / ciudadanía, Registro civil etc.) en el fichero.	Booleano
Pasaportes	Indica si se detectó una o más entidades del tipo Pasaporte en el fichero.	Booleano

Campo	Comentario	Valores
Tarjeta de crédito	Indica si se detectó una o más entidades del tipo Número de tarjeta de crédito en el fichero.	Booleano
Cuentas bancarias	Indica si se detectó una o más entidades del tipo Número de cuenta bancaria en el fichero.	Booleano
Permisos de conducir	Indica si se detectó una o más entidades del tipo Permiso de conducir en el fichero.	Booleano
Números de la Seguridad Social	Indica si se detectó una o más entidades del tipo Número de la seguridad social en el fichero.	Booleano
Direcciones de correo electrónico	Indica si se detectó una o más entidades del tipo Dirección de correo electrónico en el fichero.	Booleano
IPs	Indica si se detectó una o más entidades del tipo Dirección IP en el fichero.	Booleano
Nombres y apellidos	Indica si se detectó una o más entidades del tipo Nombre y apellidos en el fichero.	Booleano
Direcciones	Indica si se detectó una o más entidades del tipo Dirección en el fichero.	Booleano
Números de teléfono	Indica si se detectó una o más entidades de tipo Número de teléfono en el fichero.	Booleano

Tabla 12.4: Campos del fichero exportado Búsqueda de información personal en los equipos

Sintaxis de las búsquedas

Cytomic Data Watch permite búsquedas flexibles de ficheros por contenido utilizando texto plano y modificadores para acotar el ámbito de los resultados.

Sintaxis admitida en búsquedas rápidas

- **Palabra**: busca “palabra” en el contenido del documento y en los metadatos.
- **PalabraA PalabraB**: busca “palabraa” o “palabrab” (operador OR) en el contenido del documento.
- **“PalabraA PalabraB”**: busca “palabraa” y “palabrab” seguidas en el contenido del documento.
- **+PalabraA +PalabraB**: busca “palabraa” y “palabrab” en el contenido del documento.
- **+Palabraa -Palabrab**: busca “palabraa” y no “palabrab” en el contenido del documento.
- **Palabra***: busca todas las palabras que empiezan por “palabra”. El carácter “*” solo se permite al final de la cadena de caracteres a buscar.
- **Pa?abra**: busca todas las palabras que empiezan por “pa”, terminan por “abra” y tienen entre los dos grupos un único carácter alfabético. El carácter “?” puede ir colocando en cualquier punto de la cadena de caracteres a buscar.
- **Palabra~**: busca todas las palabras que contienen la cadena de caracteres “palabra”.

Sintaxis admitida en búsquedas guiadas

En las búsquedas guiadas no se utilizan los caracteres “+” y “-”. En su lugar las palabras a buscar se distribuyen en las diferentes cajas de texto presentadas en la pantalla. Si utilizas los caracteres “+” y “-”, éstos formarán parte de la búsqueda.

Entidades disponibles

Para acotar el ámbito de los resultados Cytomic Data Watch admite el uso de calificadores para indicar entidades o características del fichero en las búsquedas rápidas y avanzadas. Los calificadores disponibles son:

Calificador	Descripción
PiiType	Especifica si un tipo de entidad fue detectada en el fichero.
HasPii	Indica que el fichero contiene entidades detectadas.
Filename	Indica el nombre del fichero.
FileExtension	Indica la extensión del fichero.

Tabla 12.5: Calificadores disponibles

Los valores admitidos para los calificadores son:

Calificador	Descripción
PiiType:BANKACCOUNT	Ficheros que contienen una o más entidades de tipo Cuenta bancaria.
PiiType:CREDITCARD	Ficheros que contienen una o más entidades de tipo Tarjeta de crédito.
PiiType:IDCARD	Ficheros que contienen una o más entidades de tipo Documento de identidad (documento nacional de identidad, Cédula de identidad / ciudadanía, Registro civil etc.).
PiiType:SSN	Ficheros que contienen una o más entidades de tipo Número de la seguridad social.
PiiType:IP	Ficheros que contienen una o más entidades de tipo Dirección IP.
PiiType:EMAIL	Ficheros que contienen una o más entidades de tipo Dirección de correo electrónico.
PiiType:PHONE	Ficheros que contienen una o más entidades de tipo Teléfono.
PiiType:ADDRESS	Ficheros que contienen una o más entidades de tipo Dirección.
PiiType:FULLNAME	Ficheros que contienen una o más entidades de tipo Nombre y apellidos.
PiiType:PASSPORT	Ficheros que contienen una o más entidades de tipo Número de pasaporte.
PiiType:DRIVERLIC	Ficheros que contienen una o más entidades de tipo Numero de licencia / permiso de conducción.
HasPii:True	Ficheros que contienen alguna entidad detectada.
Filename:"nombre del fichero"	Ficheros que tienen como nombre la cadena indicada.
Fileextension:"extensión del fichero"	Ficheros que tienen como extensión la cadena indicada.

Tabla 12.6: Valores admitidos en los calificadores

Sintaxis de las búsquedas con entidades

Las entidades se pueden utilizar en todos los tipos de búsqueda (rápida o guiada) de forma individual o combinadas con otras cadenas de caracteres.

- **PiiType:IDCARD**: busca todos los ficheros con alguna entidad detectada de tipo Documento de identidad.
- **+PiiType:IDCARD +“Empresa”**: busca el fichero que contiene el listado de documentos de identidad (con alguna detección de entidad IDCARD) de la empresa (que contenga la cadena de caracteres “Empresa”).
- **+Filename:analisis* +fileextension:docx -PiiType:fullname**: busca todos los ficheros de análisis (su nombre empieza por la palabra “análisis”) en formato Word (extensión docx) y no están firmados (no se detectó ninguna entidad de tipo Fullname - Nombre y apellidos).

Consejos para construir búsquedas compatibles con la normalización

- Utiliza preferiblemente letras en minúsculas.
- Ten en cuenta la configuración establecida sobre el contenido de los ficheros a indexar y los ficheros excluidos, ya que de ello dependerá el número de resultados mostrados en las búsquedas.
- Para buscar **números de cuentas bancarias, números de tarjetas de crédito, números de identidad, números de la seguridad social, números de pasaporte, números de permiso** elimina los caracteres de separación de la búsqueda.
- Para buscar **direcciones IP y direcciones de correo electrónico** introdúcelas tal cual.
- Para buscar **números de teléfono** elimina los caracteres de separación, introduciendo el código del país si es necesario, sin el signo “+”.
- Para buscar **direcciones físicas** elimina los caracteres numéricos.

Búsqueda de ficheros duplicados

Con el objetivo de ayudar a centralizar la información sensible en un único punto, y por tanto minimizar la exposición de este tipo de datos, Cytomic Data Watch incluye la funcionalidad de búsqueda de ficheros duplicados y posterior borrado.

Definición de fichero duplicado

Se considera a dos ficheros como duplicados cuando su contenido es idéntico, independientemente del proceso de normalización descrito en [Proceso de normalización](#) ni de la configuración establecida por el administrador en [Indexar el siguiente contenido](#). En la comparación no se consideran ni el nombre ni la extensión de los ficheros.

Búsqueda de ficheros duplicados

Para buscar un fichero duplicado sigue los pasos mostrados a continuación:

- Desde el panel lateral **Mis listados**:
 - En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una ventana con todos los listados disponibles.
 - Elige el listado **Archivos con información personal**. Se mostrará el listado de ficheros PII encontrados en la red.
- Desde el widget **Archivos con información personal**:
 - En el menú superior **Estado**, panel lateral **Cytomic Data Watch**, haz clic en una serie del widget **Archivos con información personal**. Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.
- Desde el widget **Archivos por tipo de información personal**:
 - En el menú superior **Estado**, panel lateral **Cytomic Data Watch**, haz clic en una serie del widget **Archivos por tipo de información personal**. Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.
 - En el menú de contexto asociado al archivo que se quiere buscar, haz clic en la opción **Buscar copias de archivo**. Se abrirá un nuevo listado con los todos los ficheros duplicados encontrados en la red.

Borrado y restauración de ficheros

Borrar ficheros de los equipos de la red

Cytomic Data Watch permite borrar los ficheros indexados y mostrados en el inventario de los equipos de la red. El borrado de ficheros es una operación asíncrona que inicia el administrador de la red desde la consola, y se produce cuando el agente recibe una petición desde el servidor Advanced EDR y se cumplen las siguientes condiciones:

- El fichero no está en uso.
- El contenido del fichero no ha cambiado con respecto al almacenado en inventario.
- El fichero no ha sido borrado por el usuario en el periodo comprendido entre la generación del inventario y la acción de borrado por parte del administrador.
- El equipo está online. Si esta condición no se cumple, Cytomic Data Watch marcará el fichero como **Pendiente de eliminar** hasta que el equipo se conecte al servidor Advanced EDR.

Estados de la acción de borrado

Al ser una operación asíncrona, el borrado de ficheros admite los estados mostrados a continuación:

- **Eliminado:** el fichero se ha movido a la zona de backup de Advanced EDR.
- **Pendiente de eliminar:** Cytomic Data Watch está esperando a que el equipo se conecte al servidor Advanced EDR para ejecutar la tarea de borrado.
- **Error:** el fichero no se ha podido borrar por un error.

Backup de ficheros borrados por Cytomic Data Watch

Lo ficheros borrados por Cytomic Data Watch no se eliminan definitivamente del disco duro de los equipos. En su lugar se mueven a un área de backup donde residen durante 30 días, pasados los cuales el fichero es eliminado por completo.

Esta área es excluida automáticamente del inventario, de las búsquedas y de la monitorización de ficheros, y es inaccesible para el software instalado en el equipo de usuario.

Borrado de ficheros

Para borrar uno o varios ficheros sigue los pasos mostrados a continuación:

- Desde el panel lateral **Mis listados**:
 - En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una ventana con todos los listados disponibles.
 - Elige el listado **Archivos con información personal**. Se mostrará el listado de ficheros PII encontrados en la red.
- Desde el widget **Archivos con información personal**:
 - En el menú superior **Estado**, panel lateral **Cytomic Data Watch**, haz clic en una serie del widget **Archivos con información personal**. Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.
- Desde el widget **Archivos por tipo de información personal**:
 - En el menú superior **Estado**, panel lateral **Cytomic Data Watch**, haz clic en una serie del widget **Archivos por tipo de información personal**. Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.
- Para borrar varios ficheros:
 - Haz clic en las casillas de selección asociadas a los ficheros que quieres borrar.
 - Haz clic en el icono  de la parte superior de la ventana. Se mostrará una ventana pidiendo confirmación.
- Para borrar un único fichero:
 - Utiliza el menú de contexto asociado al fichero que quieres eliminar y haz clic en la opción **Eliminar**. Se mostrará una ventana pidiendo confirmación.
- Si confirmas el borrado del fichero, éste se mostrará en el listado de ficheros en rojo y con el icono  indicando que está pendiente de borrado.

Visualizar ficheros borrados

Para visualizar los ficheros borrados por el administrador sigue los pasos mostrados a continuación:

- En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una ventana con todos los listados disponibles.
- Elige el listado **Archivos eliminados por el administrador**. Se mostrará el listado de ficheros PII encontrados en la red que el administrador borró o restauró previamente.

Restaurar ficheros previamente borrados por el administrador

Cytomic Data Watch permite restaurar a su ruta original los ficheros previamente borrados por el administrador desde la consola, en tanto en cuanto estos ficheros permanezcan en el área de backup (30 días desde su borrado). La restauración de ficheros es una operación asíncrona que inicia el administrador de la red desde la consola y se produce cuando el agente recibe una petición desde el servidor Advanced EDR y se cumplen las siguientes condiciones:

- **El fichero permanece en la zona de backup**: los ficheros borrados permanecen en el área de backup durante 30 días, transcurridos los cuales se procede a eliminar el fichero definitivamente sin posibilidad de restauración.
- **No existe otro fichero en la ruta de restauración con el mismo nombre el fichero**: si existe otro fichero con el mismo nombre en la ruta de restauración Cytomic Data Watch seguirá restaurando el fichero, pero lo hará en la carpeta Perdidos.
- **La ruta de restauración existe**: si la ruta de restauración no existe, Cytomic Data Watch seguirá restaurando el fichero, pero lo hará en la carpeta Perdidos.
- **El equipo está online**: si el equipo está offline Cytomic Data Watch marcará el fichero como **Pendiente de restaurar** hasta que se conecte al servidor Advanced EDR.

Estados de la acción de restaurar

Al ser una operación asíncrona, la restauración de ficheros admite los estados mostrados a continuación:

- Restaurado
- Pendiente de restaurar
- Error

Restaurar ficheros borrados

Para restaurar los ficheros borrados por el administrador sigue los pasos mostrados a continuación:

Acceso a la funcionalidad de restauración:

- En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una ventana con todos los listados disponibles.

- Elige el listado **Archivos eliminados por el administrador**. Se mostrará el listado de ficheros PII encontrados en la red que el administrador borró o restauró previamente.

o

- En el menú superior **Estado**, panel lateral **Cytomic Data Watch** haz clic en el widget **Archivos eliminados por el administrador**. Se abrirá el listado **Archivos eliminados por el administrador** sin filtros preconfigurados.

Para restaurar varios ficheros:

- Haz clic en las casillas de selección asociadas a los ficheros que quieres recuperar.
- Haz clic en el icono  de la parte superior de la ventana. Se mostrará una ventana pidiendo confirmación.
- Si confirmas la recuperación del fichero, éste pasará al estado **Restaurando**.

Para restaurar un único fichero:

- Utiliza el menú de contexto asociado al fichero que quieres recuperar.
- Haz clic en la opción **Restaurar**. Se mostrará una ventana pidiendo confirmación.
- Si confirmas la recuperación del fichero, éste pasará al estado **Restaurando**.

Configuración de Cytomic Data Watch

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Cytomic Data Watch**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración de **Añadir configuración**.

Permisos requeridos

Permiso	Tipo de acceso
Configurar Cytomic Data Watch	Crear, modificar, borrar, copiar o asignar las configuraciones de Cytomic Data Watch.
Ver configuraciones de Cytomic Data Watch	Visualizar las configuraciones de Cytomic Data Watch.

Tabla 12.7: Permisos requeridos para acceder a la configuración Cytomic Data Watch

Requisitos para buscar y seguir documentos Microsoft Office

Para localizar los equipos que no tienen instalado alguno o ninguno de los componentes iFilter haz clic en el enlace **Comprobar ahora** de la pantalla de configuración. Se abrirá la zona **Equipos** con un listado filtrado por el criterio **Equipos sin Microsoft Filter Pack**.

Información personal (inventario, búsquedas y seguimiento)

- **Generar y mantener actualizado el inventario de información personal:** muestra los ficheros PII detectados en la red utilizando los widgets del dashboard y los listados. Consulta [Paneles / widgets del módulo Cytomic Data Watch](#) y [Listados del módulo Cytomic Data Watch](#) para más información. Para que los ficheros PII almacenados en un equipo concreto se muestren es necesario que el proceso de inventariado se haya completado para ese equipo.
- **Realizar el seguimiento de información personal en disco:** monitoriza las acciones de los procesos ejecutadas sobre ficheros PII almacenados en el equipo.
- **Realizar el seguimiento de información personal en correo:** monitoriza las acciones ejecutadas sobre la información personal almacenada en mensajes de correo electrónico.
- **Permitir realizar búsquedas de información en los equipos:** localiza ficheros por su nombre o contenido, siempre que hayan sido previamente indexados. Al hacer clic en este botón Cytomic Data Watch comenzará el proceso de indexación de los ficheros almacenados en los equipos de los usuarios. Consulta [Búsqueda de ficheros](#) para más información.

Exclusiones

El administrador puede excluir del proceso de búsqueda a aquellos ficheros almacenados en los equipos de la red cuyo contenido no considere oportuno tener en cuenta.

- **Extensiones:** excluye a los ficheros con las extensiones indicadas.
- **Archivos:** excluye del proceso a los ficheros con el nombre indicado. Se pueden utilizar los caracteres comodín * y ?.
- **Carpetas:** excluye del proceso a todos los ficheros contenidos en las carpetas indicadas. Se pueden utilizar variables del sistema y los caracteres comodín * y ?.

Monitorización de archivos por reglas

Mediante reglas definidas por el administrador, Cytomic Data Watch puede monitorizar archivos que no están clasificados como PII. El sistema almacena hasta diez reglas, que deben tener un nombre único.

Monitorizar archivos en disco

Monitoriza las acciones que se producen sobre los archivos seleccionados en **Reglas de monitorización**.

Monitorizar archivos en correo

Monitoriza las acciones que se ejecutan sobre los adjuntos en mensajes de correo, que cumplan las reglas indicadas en **Reglas de monitorización**.

Reglas de monitorización

Muestra la lista de extensiones predeterminadas sobre las que se aplica la monitorización. Se pueden añadir otras extensiones a la lista o eliminar las que ya están. Esta lista es común para todas las reglas que se han creado.



Cuando se asigna una propiedad de tipo “extensión del archivo” a una regla, la monitorización se producirá únicamente sobre los archivos que coincidan con la extensión, y no sobre el listado completo de extensiones.

Para crear una regla de monitorización haz clic en el icono +, se abrirá la ventana **Añadir reglas de monitorización** donde introducir los criterios de configuración de la regla.

- Introduce los campos de nombre y descripción.
- Completa los términos de la condición.

Propiedad	Operador	Valor
Nombre de archivo	Igual a / No es igual a	• Cadena de caracteres con comodines "*" y "?". • La cadena de caracteres nunca puede comenzar con un comodín.
Ruta del archivo	Igual / No es igual a	• Cadena de caracteres con comodines "*" y "?". • Cuando se especifica una ruta del sistema de ficheros el separador es por defecto "\". • Es necesario incluir un comodín "*" al definir una regla con el campo Ruta del archivo. • La cadena de caracteres nunca puede comenzar con un comodín.
Contenido del archivo	Igual a / No es igual a	• Cadena de caracteres con comodines "*" y "?". • La cadena de caracteres nunca puede comenzar con un comodín.
Extensión del archivo	Igual a / No es igual a	• Cadena de caracteres sin comodines. • Las extensiones de ficheros se deben poner sin punto delante.

Tabla 12.8: Campos para configurar una condición

Nueva condición:

añade más condiciones a la regla. Se aplicarán los operadores lógicos Y/O.

Operadores lógicos

Para combinar dos condiciones o más en una misma regla se utilizan los operadores lógicos Y y O. Al añadir una segunda condición y sucesivas a una regla, se mostrará de forma automática un desplegable con los operadores lógicos disponibles, que se aplicarán a las condiciones adyacentes.

Agrupaciones de condiciones de regla

Los paréntesis en una expresión lógica se utilizan para variar el orden de evaluación de los operadores que relacionan las condiciones de las reglas introducidas.

Para encerrar dos o más condiciones en un paréntesis crea una agrupación marcando con las casillas de selección las condiciones consecutivas que formarán parte del grupo y haz clic en el botón **Agrupar condiciones**. Se mostrará una línea delgada que abarcará las reglas de reglas de monitorización que forman parte de la agrupación.

Mediante el uso de paréntesis se definen agrupaciones de varios niveles para poder anidar grupos de operandos en una expresión lógica.

Ejemplos de reglas de monitorización

Propiedad	Contenido	Búsqueda
Ruta del archivo	c:\ruta*	Busca en todos los archivos y carpetas que se encuentran en c:\ruta\
Ruta del archivo	c:\ruta\ c:\ruta	Configuración errónea. No devuelve ningún resultado.
Extensión del archivo	txt	Busca los archivos con extensión "txt"
Extensión del archivo	.txt	Configuración errónea. No devuelve ningún resultado.
Nombre del archivo	NombreFichero	Devuelve todos los ficheros cuyo nombre es "NombreFichero".
Nombre del archivo	NombreFichero*	Devuelve todos los ficheros cuyo nombre comienza por "NombreFichero".

Propiedad	Contenido	Búsqueda
Nombre del archivo	?NombreFichero *NombreFichero	Configuración errónea. No devuelve ningún resultado.

Tabla 12.9: Ejemplos de reglas de monitorización

Opciones avanzadas de indexación

Para ver el estado de la indexación haz clic en el enlace **Ver estado de indexación de los equipos**. Se abrirá el **Estado de Cytomic Data Watch**.

Indexar el siguiente contenido

Establece el tipo de contenido que se considerará a la hora de generar el inventario y que se devolverá como resultado de las búsquedas.



Los equipos que ya tengan un índice generado y reciban un cambio de configuración borrarán el índice y reiniciarán el proceso de indexado desde el principio.

Selecciona el tipo de indexación dependiendo de si únicamente quieres generar un inventario de ficheros PII o, por el contrario, también deseas lanzar búsquedas por contenido:

- **Indexar solo el texto:** se indexa solo el texto a no ser que forme parte de una entidad reconocida por Cytomic Data Watch. Las búsquedas por contenido producidas con este tipo de índice serán más limitadas, por lo tanto, está recomendado si el administrador únicamente quiere generar el inventario de ficheros PII.
- **Indexar todo el contenido:** se indexan tanto los textos como los caracteres numéricos. Se recomienda cuando el administrador además de mantener el inventario de ficheros PII quiere realizar búsquedas precisas por contenido.



*Cytomic Data Watch buscará sobre los contenidos del fichero según la configuración **Contenido del índice en los equipos** asignada. Si los equipos tienen configuraciones de indexación distintas, el resultado de las búsquedas pueden no ser homogéneo.*

Programar períodos de indexación

Configura la franja horaria en la que el proceso de indexación se iniciará en caso de ser necesario:

- **Siempre activado:** no se indica una franja horaria y el proceso de indexación se iniciará en el momento que sea necesario.
- **Activar sólo durante las siguientes horas:** indica mediante un calendario mensual los días y horas en los que el proceso de indexación podrá iniciarse.
- Utiliza los botones **Vaciar** y **Seleccionar todo** para limpiar el calendario o marcarlo por completo (equivalente a **Siempre activado**).

Escritura en unidades de almacenamiento extraíbles

Limita el acceso a la escritura de medios de almacenamiento externos USB.

- Permitir escritura sólo en unidades extraíbles cifradas: al activar esta opción, el usuario solo puede escribir en medios de almacenamiento externo USB que estén previamente cifrados con Cytomic Encryption o BitLocker.



Las configuraciones de **Control de dispositivos** en **Estaciones y servidores** tienen precedencia sobre las configuraciones establecidas en **Cytomic Data Watch**. De esta manera, si **Control de dispositivos** está activado y no permite la lectura y escritura de la unidad USB, no será posible su escritura, independientemente de que esté o no cifrada. Consulta **Control de dispositivos (Equipos Windows)** para obtener más información acerca de esta configuración.

Paneles / widgets del módulo Cytomic Data Watch

Acceso al panel de control

Para acceder al panel de control haz clic en el menú superior **Estado**, panel lateral **Cytomic Data Watch**.

Permisos requeridos

Permiso	Acceso a Widgets
Sin permisos	• Estado del despliegue • Equipos sin conexión • Estado de la actualización • Estado de la indexación • Características activadas en los equipos • Archivos eliminados por el administrador

Permiso	Acceso a Widgets
Visualizar inventario de información personal	- Archivos con información personal - Archivos por tipo de información personal - Equipos con información personal
Buscar información en los equipos	Búsquedas

Tabla 12.10: Permisos requeridos para el acceso a los widgets de Cytomic Data Watch

Estado del despliegue

Muestra los equipos donde Cytomic Data Watch está funcionando correctamente y aquellos que presentan algún tipo de error. El estado de los equipos se representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

DEPLOYMENT STATUS



Figura 12.3: Panel Estado del despliegue

Significado de las series

Serie	Descripción
Ok	Equipos con Cytomic Data Watch instalado, licenciado y funcionando correctamente.
Error	Equipos con Cytomic Data Watch instalado donde el módulo no responde a las peticiones enviadas desde los servidores de Cytomic.
Sin licencia	Equipos compatibles con Cytomic Data Watch pero sin licencia de Advanced EDR

Serie	Descripción
	asignada.
Error instalando	Equipos cuya instalación no se pudo completar.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con un agente sin actualizar.
Parte central	Suma de todos equipos compatibles con Cytomic Data Watch.

Tabla 12.11: Descripción de la serie Estado del despliegue

Filtros preestablecidos desde el panel

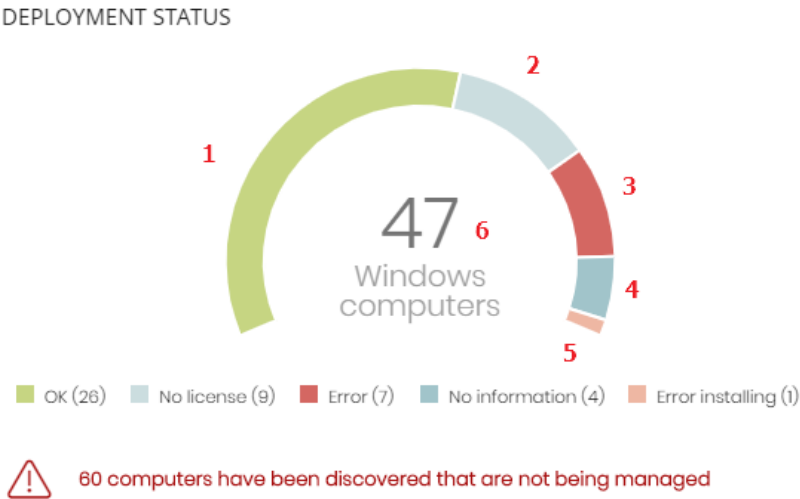


Figura 12.4: Zonas activas del panel Estado del despliegue

Al hacer clic en las zonas indicadas en **Zonas activas del panel Estado del despliegue** se abre el listado **Estado de Cytomic Data Watch** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de Cytomic Data Watch = Correcto.
(2)	Estado de Cytomic Data Watch = Sin licencia. El equipo no tiene asignada licencia de Advanced EDR.
(3)	Estado de Cytomic Data Watch = Error.
(4)	Estado de Cytomic Data Watch = Sin información.

Zona activa	Filtro
(5)	Estado de Cytomic Data Watch = Error instalando.
(6)	Sin filtros.

Tabla 12.12: Definición de filtros del listado Estado de Cytomic Data Watch

Equipos sin conexión

Muestra los equipos de la red que no han conectado con la nube de Cytomicen un determinado periodo de tiempo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

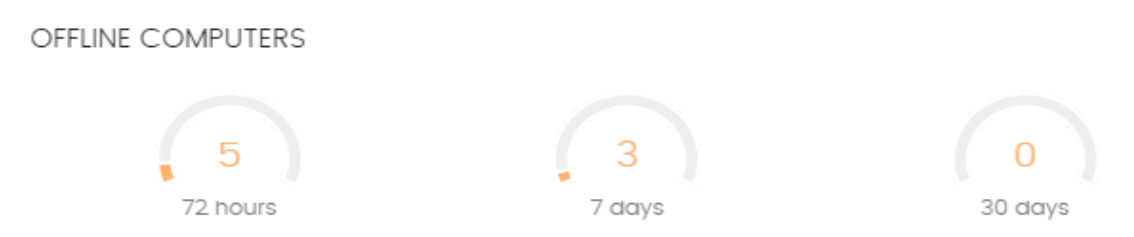


Figura 12.5: Panel Equipos sin conexión

Significado de las series

Serie	Descripción
72 horas	Número de equipos que no enviaron su estado en las últimas 72 horas.
7 días	Número de equipos que no enviaron su estado en las últimas 7 días.
30 días	Número de equipos que no enviaron su estado en las últimas 30 días.

Tabla 12.13: Descripción de la serie Equipos sin conexión

Filtros preestablecidos desde el panel

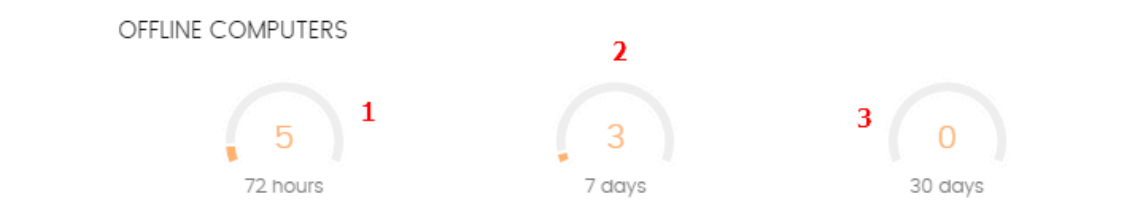


Figura 12.6: Zonas activas del panel Equipos sin conexión

Al hacer clic en las zonas indicadas en **Zonas activas del panel Equipos sin conexión** se abre el listado **Estado de Cytomic Data Watch** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 72 horas.
(2)	Última conexión = Hace más de 7 días.
(3)	Última conexión = Hace más de 30 días.

Tabla 12.14: Definición de filtros del listado Estado de Cytomic Data Watch

Estado de la actualización

Muestra el estado de los equipos con respecto a la actualización del motor de Cytomic Data Watch.

UPDATE STATUS



Figura 12.7: Panel Estado de la actualización

Significado de las series

Serie	Descripción
Actualizados	Número de equipos con el motor Cytomic Data Watch actualizado.
Desactualizados	Número de equipos con el motor Cytomic Data Watch desactualizado.
Pendientes de reinicio	Número de equipos que han descargado el motor Cytomic Data Watch pero todavía no se han reiniciado, con lo que todavía no se ha actualizado.

Tabla 12.15: Descripción de la serie Estado de la actualización

Filtros preestablecidos desde el panel

UPDATE STATUS

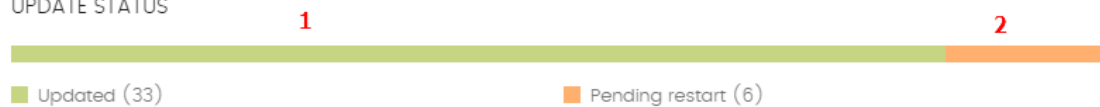


Figura 12.8: Zonas activas del panel Estado de la actualización

Al hacer clic en las zonas indicadas en **Zonas activas del panel Estado de la actualización** se abre el listado **Estado de Cytomic Data Watch** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Protección actualizada = Si.
(2)	Protección actualizada = Pendiente de reinicio.
(3)	Protección actualizada = No.

Tabla 12.16: Definición de filtros del listado Estado de Cytomic Data Watch

Estado de la indexación

Muestra el estado de los equipos con respecto al estado de indexación de las unidades de almacenamiento conectadas.

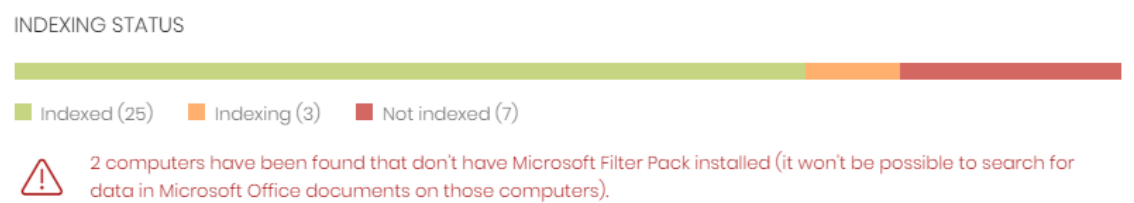


Figura 12.9: Panel Estado de la indexación

Significado de las series

Serie	Descripción
Indexado	Número de equipos con los contenidos de las unidades de almacenamiento completamente indexados. Requiere que las búsquedas y/o el inventario estén activados. Consulta Configuración de Cytomic Data Watch .
No indexado	Número de equipos con los contenidos de las unidades de almacenamiento sin indexar. Requiere que las búsquedas y/o el inventario estén activados. Consulta Configuración de Cytomic Data Watch
Indexando	Número de equipos con contenidos en proceso de indexación. Requiere que las búsquedas y/o el inventario estén activados. Consulta Configuración de Cytomic Data Watch

Tabla 12.17: Descripción de la serie Estado de la indexación

Filtros preestablecidos desde el panel

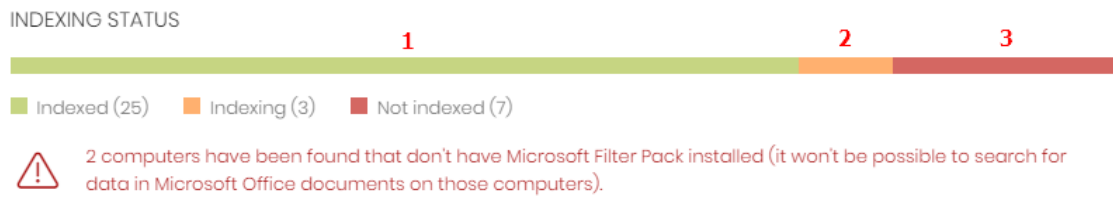


Figura 12.10: Zonas activas del panel Estado de la indexación

Al hacer clic en las zonas indicadas en **Zonas activas del panel Estado de la indexación** se abre el listado **Estado de Cytomic Data Watch** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de indexación = Indexado.
(2)	Estado de indexación = Indexando.
(3)	Estado de indexación = No indexado.

Tabla 12.18: Definición de filtros del listado Estado de Cytomic Data Watch

Características activadas en los equipos

Refleja el número total de equipos en la red que tienen instalado y correctamente licenciado Cytomic Data Watch, y que han reportado el estado **Activado** para cada una de las tres funcionalidades.

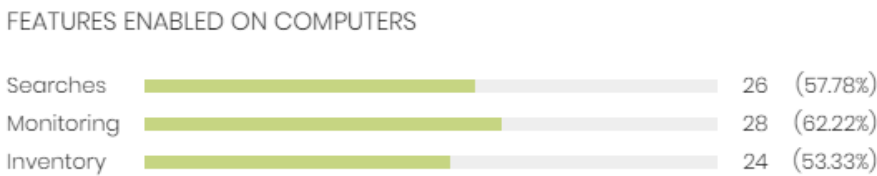


Figura 12.11: Panel Características activadas en los equipos

Significado de las series

Serie	Descripción
Búsquedas	Muestra el número de equipos que reportan como activada la funcionalidad de búsqueda por contenido de ficheros PII.
Seguimiento	Muestra el número de equipos que reportan como activada la funcionalidad de monitorización de ficheros PII.

Serie	Descripción
Inventario	Muestra el número de equipos que reportan como activada la funcionalidad de inventario de ficheros PII.

Tabla 12.19: Descripción de la serie Características activadas en los equipos

Filtros preestablecidos desde el panel

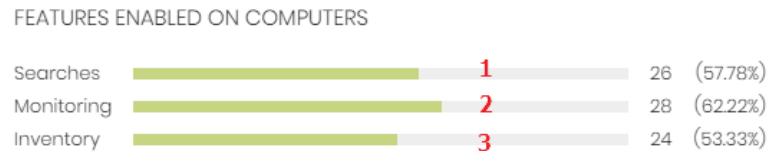


Figura 12.12: Zonas activas del panel Características activadas en los equipos

Al hacer clic en las zonas indicadas en **Zonas activas del panel Características activadas en los equipos** se abre el listado **Estado de Cytomic Data Watch** con los filtros preestablecidos mostrados a continuación.

Zona activa	Filtro
(1)	Búsqueda de información en los equipos activada = Si.
(2)	Seguimiento de información personal activada = Si.
(3)	Inventario de información personal activado= Si.

Tabla 12.20: Definición de filtros del listado Estado de Cytomic Data Watch

Archivos eliminados por el administrador

Muestra los distintos estados por los que pasan los ficheros eliminados por el administrador.

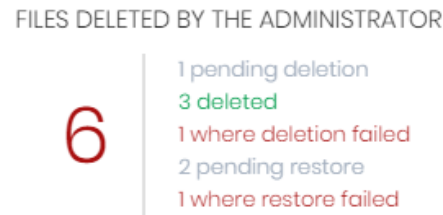


Figura 12.13: Panel Archivos eliminados por el administrador

Significado de las series

Serie	Descripción
Pendientes de eliminar	Archivos marcados para borrar pero que todavía no se ha ejecutado la

Serie	Descripción
	tarea.
Eliminados	Archivos borrados que permanecen en el área de backup de Advanced EDR.
Con error al eliminar	Archivos sobre los que no fue posible ejecutar la tarea de borrado.
Pendientes de restaurar	Archivos marcados para restaurar pero que todavía no se ha ejecutado la tarea.
Restaurados	Archivos que han sido movidos desde el área de backup a su ubicación original.

Tabla 12.21: Descripción de la serie Archivos eliminados por el administrador

Filtros preestablecidos desde el panel

FILES DELETED BY THE ADMINISTRATOR

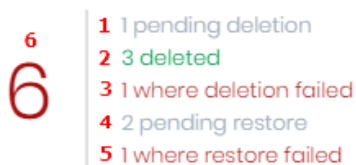


Figura 12.14: Zonas activas del panel Archivos eliminados por el administrador

Al hacer clic en las zonas indicadas en **Zonas activas del panel Archivos eliminados por el administrador** se abre un listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Archivos con información personal.	Pendiente de eliminar.
(2)	Archivos eliminados por el administrador.	Estado = Eliminado.
(3)	Archivos con información personal.	Error eliminando.
(4)	Archivos eliminados por el administrador.	Estado = Pendiente de restaurar.
(5)	Archivos eliminados por el	Estado = Error restaurando.

Zona activa	Listado	Filtro
	administrador.	
(6)	Archivos eliminados por el administrador.	Estado = todos.

Tabla 12.22: Definición de filtros del listado Archivos eliminados por el administrador

Archivos con información personal

Muestra el número de ficheros con información personal encontrados en la red y el total de ficheros encontrados en el último inventario diario generado.

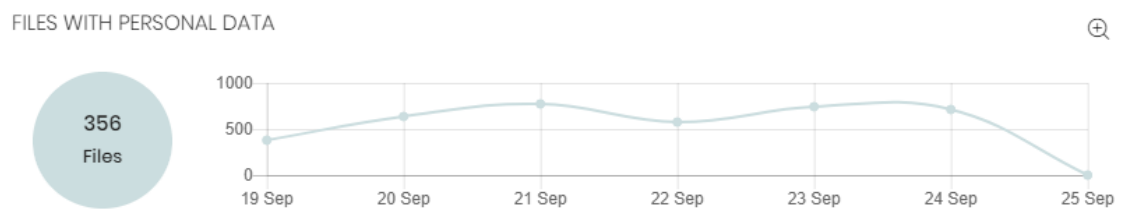


Figura 12.15: Panel Archivos con información personal

Significado de las series

Serie	Descripción
Burbuja	Número total de ficheros PII encontrados según el último inventario enviado por cada equipo.
Linea	Número de ficheros PII encontrados en los inventarios diarios generados en las fechas indicadas en el eje de las Xs, y en todos los equipos de la red.

Tabla 12.23: Descripción de la serie Archivos con información personal

Filtros preestablecidos desde el panel

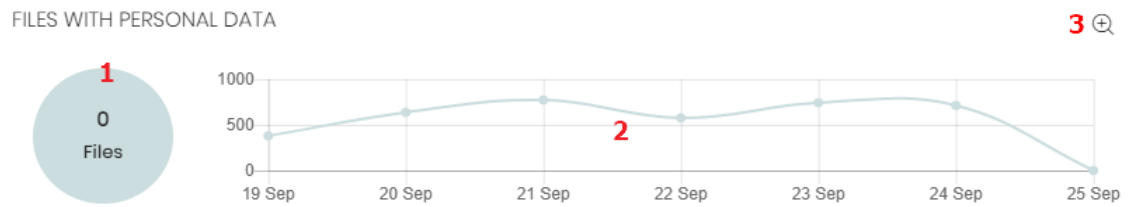


Figura 12.16: Zonas activas del panel Archivos con información personal

Al hacer clic en las zonas indicadas en **Zonas activas del panel Archivos con información personal** se abre el listado **Archivos con información personal** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.
(2)	Fecha 1 = fecha elegida y Fecha 2 = fecha actual.
(3)	Se abre una nueva ventana con una ampliación del widget.

Tabla 12.24: Definición de filtros del listado Archivos con información personal

Ampliación de la gráfica Archivos con información personal

Al hacer clic sobre el icono  se abre una ventana con una ampliación del widget **Archivos con información personal** representando mediante una serie independiente el número de ficheros PII que contienen cada una de las entidades soportadas.

- Para configurar el widget:
- Haz clic en la leyenda para activar o desactivar una serie.
- Haz clic en el enlace **Ocultar todos los datos** para mostrar el número de ficheros PII que contienen cualquier tipo de entidad.
- Haz clic en **Mostrar todos los datos** para mostrar el número de ficheros PII que contienen cada tipo de entidad por separado.

Equipos con información personal

Muestra el número de equipos de usuario y servidores que contienen ficheros con información personal en el último inventario diario generado.

COMPUTERS WITH PERSONAL DATA



Figura 12.17: Panel Archivos con información personal

Significado de las series

Serie	Descripción
Burbuja	Número de equipos con ficheros PII encontrados según los últimos datos enviados por cada equipo.

Serie	Descripción
Línea	Número total de equipos con ficheros PII encontrados en los inventarios diarios generados en las fechas indicadas en el eje de las Xs.

Tabla 12.25: Descripción de la serie Equipos con información personal

Filtros preestablecidos desde el panel



Figura 12.18: Zonas activas del panel Archivos con información personal

Al hacer clic en las zonas indicadas en **Zonas activas del panel Archivos con información personal** se abre el listado **Archivos con información personal** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.
(2)	Fecha 1 = fecha elegida y Fecha 2 = fecha actual.

Tabla 12.26: Definición de filtros del listado Archivos con información personal

Archivos por tipo de información personal

Muestra el número de archivos PII encontrados por cada tipo de entidad soportada en el último inventario diario generado.

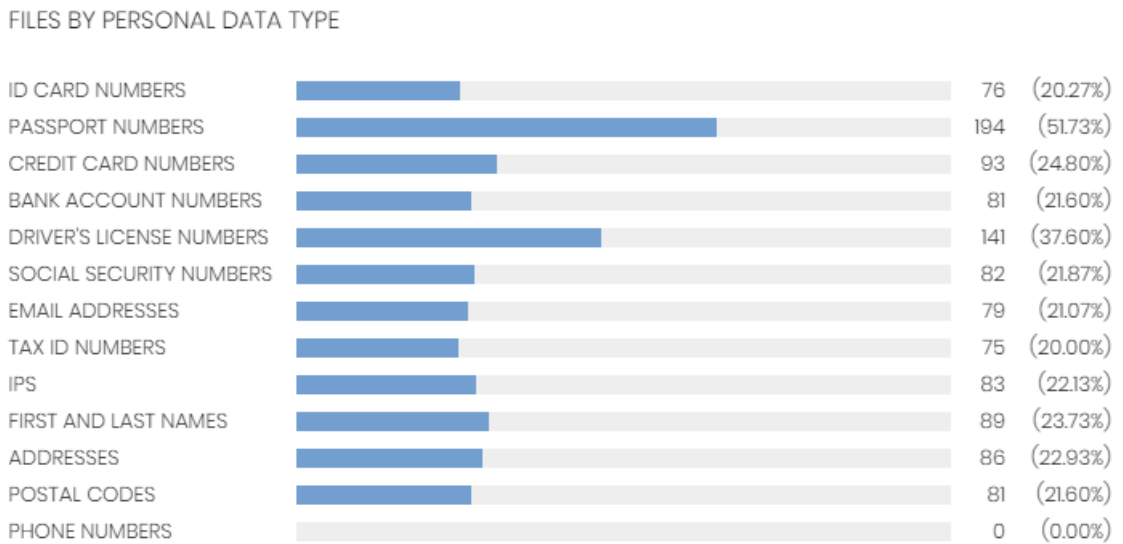


Figura 12.19: Panel Archivos por tipo de información personal

Significado de las series

Serie		Descripción
Serie		
		Número total de ficheros PII encontrados en el último inventario diario generado por cada tipo de entidad soportada, y porcentaje de ficheros sobre el total de ficheros PII detectados.

Tabla 12.27: Descripción de la serie Archivos por tipo de información personal

Filtros preestablecidos desde el panel

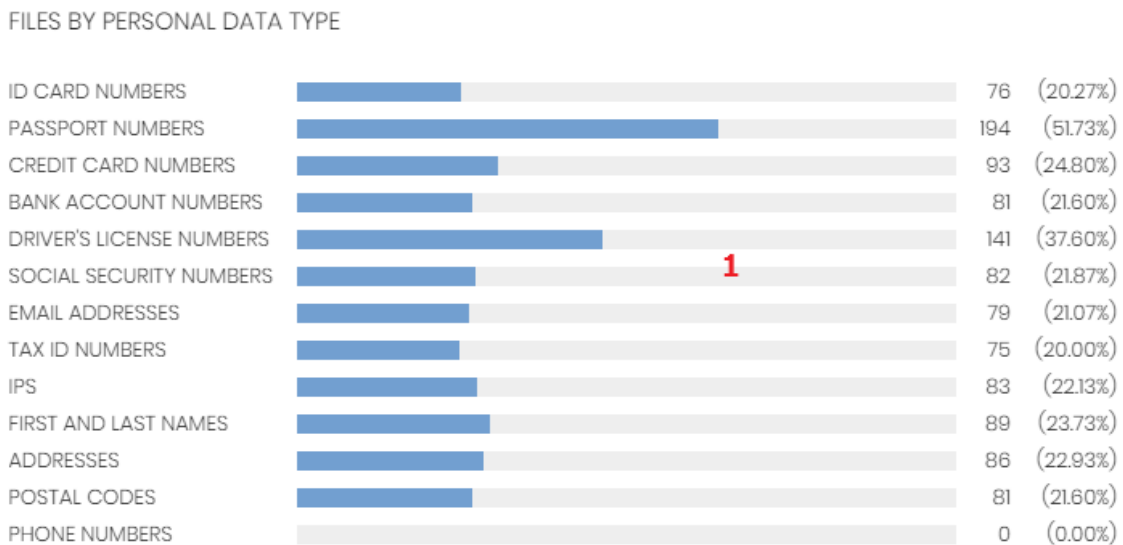


Figura 12.20: Zonas activas del panel Archivos por tipo de información personal

Haz clic en el widget para abrir el listado **Archivos con información personal** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Información personal = tipo de entidad seleccionada.

Tabla 12.28: Definición de filtros del listado Archivos con información personal

Listados del módulo Cytomic Data Watch

Acceso a los listados

El acceso a los listados se puede hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Cytomic Data Watch** y en el widget relacionado.

ó

- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.
- Selecciona un listado de la sección **Protección de datos** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

Permiso	Acceso a listados
Sin permisos	Estado de Cytomic Data Watch
Visualizar inventario de información personal	- Archivos con información personal - Equipos con información personal - Archivos eliminados por el administrador

Tabla 12.29: Permisos requeridos para acceder a los listados de Cytomic Data Watch

Estado de Cytomic Data Watch

Muestra todos los equipos de la red e incorpora filtros relativos al estado del módulo Cytomic Data Watch para localizar aquellos puestos de trabajo o dispositivos móviles que cumplen los criterios establecidos en el panel.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres

Campo	Comentario	Valores
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Estado del equipo	Reinstalación del agente:  Reinstalando agente.  Error en la reinstalación del agente. Reinstalación de la protección:  Reinstalando la protección.  Error en la reinstalación de la protección.  Pendiente de reinicio. Estado de aislamiento del equipo:  Equipo en proceso de entrar en aislamiento.  Equipo aislado.  Equipo en proceso de salir del aislamiento. Modo Contención de ataque RDP:  Equipo en modo contención de ataque RDP.  Finalizando modo de contención de ataque RDP.	Icono
Seguimiento de información personal	Indica si Cytomic Data Watch puede realizar un seguimiento de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	 Error instalando y Error  Desactivado  Activado  Sin licencia  Sin información

Campo	Comentario	Valores
Inventario	Indica si Cytomic Data Watch puede generar un inventario de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	 Error instalando y Error  Desactivado  Activado  Sin licencia  Sin información
Búsquedas	Indica si Cytomic Data Watch puede buscar ficheros en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	 Error instalando y Error  Desactivado  Instalando  Activado  Sin licencia  Sin información
Actualizado	Indica si el módulo de Cytomic Data Watch instalado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se indica la versión de la protección instalada.	 Actualizado  Pendiente de reinicio  No actualizado
Microsoft Filter	Indica si todos los componentes necesarios del paquete	 Instalado

Campo	Comentario	Valores
Pack	Microsoft Filter Pack están instalados o no en el equipo.	 No instalado  Información no disponible
Estado de indexación	Indica el estado del proceso de indexación de ficheros.	 Indexando  Indexado (Solo texto o Todo el contenido)  No indexado  No disponible
Última conexión	Fecha del último envío del estado de Advanced EDR a la nube de Cytomic.	Fecha

Tabla 12.30: Campos del listado Estado de Cytomic Data Watch



Para visualizar los datos del listado gráficamente accede a uno de los siguientes widgets: *Estado del despliegue, Equipos sin conexión, Estado de la actualización, Características activadas en los equipos, o Estado de la indexación.*

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil - Servidor

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el Software Advanced EDR se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha del último envío del estado del equipo a la nube de Cytomic.	Fecha
Fecha de la última actualización	Fecha de la última actualización del agente.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada.	Binario
Versión de la	Versión interna del módulo de protección.	Cadena de

Campo	Comentario	Valores
protección		caracteres
Conocimiento actualizado	Indica si el fichero de firmas descargado en el equipo es la última versión publicada.	Binario
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Seguimiento de información personal	Indica si Cytomic Data Watch puede realizar un seguimiento de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	• Error instalando • Error • Desactivado • Correcto • Sin licencia • Sin información
Inventario de información	Indica si Cytomic Data Watch puede generar un inventario de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	• Error instalando • Error • Desactivado • Correcto • Sin licencia • Sin información
Búsquedas	Indica si Cytomic Data Watch puede buscar ficheros en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	• Error instalando • Error • Desactivado • Correcto • Sin licencia • Sin información
Microsoft Filter Pack	Indica si todos los componentes necesarios del paquete Microsoft Filter Pack están instalados o no en el equipo.	• Instalado • No instalado • No disponible
Estado de	Indica el estado del proceso de indexación de ficheros.	• Indexando

Campo	Comentario	Valores
indexación		• Indexado • No indexado • No disponible
Tipo de indexación	Muestra el tipo de indexación configurado en el equipo.	• Solo el texto • Todo el contenido
Estado de aislamiento	Indica si el equipo ha sido aislado de la red o se comunica con sus equipos vecinos de forma normal.	• Aislado • No aislado
Fecha error instalación	Fecha en la que se intentó la instalación del módulo Cytomic Data Watch y se produjo el error.	Fecha
Error instalación	Motivo del error de instalación.	Cadena de caracteres

Tabla 12.31: Campos del fichero exportado Estado de Cytomic Data Watch

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil • Dispositivo móvil • Servidor
Buscar equipo	Filtra los equipos según su nombre.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Cytomic Data Watch a la nube de Cytomic.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días

Campo	Comentario	Valores
		- Hace menos de 30 días - Hace más de 3 días - Hace más de 7 días - Hace más de 30 días
Protección actualizada	Filtra los equipos según la versión de la protección instalada.	- Todos - Si - No - Pendiente de reinicio
Estado de indexación	Filtra los equipos según el estado del proceso de indexación de ficheros.	- Todos - Indexando - Indexado - No indexado - No disponible
Tipo de indexación	Muestra los equipos que tienen configurado un tipo concreto de indexación.	- Todos - Solo el texto - Todo el contenido
Microsoft Filter Pack	Filtra los equipos si tienen o no instalados todos los componentes necesarios del paquete Microsoft Filter Pack.	- Todos - Falso - Verdadero
Estado de Cytomic Data Watch	Filtra los equipos según el estado del módulo Cytomic Data Watch.	- Instalando... - Sin información - Correcto - Seguimiento de información personal desactivado - Búsqueda de información en el

Campo	Comentario	Valores
		equipo desactivado • Error • Error Instalando • Sin licencia • Seguimiento de información personal activada • Búsqueda de información en los equipos activada • Inventario de información personal activado • Inventario de información personal desactivado

Tabla 12.32: Campos de filtrado para el listado Estado de Cytomic Data Watch

Archivos con información personal

Muestra todos los ficheros PII encontrados, así como su tipo, localización y otra información relevante.

Dado que Cytomic Data Watch solo retiene el último inventario completo de cada equipo, aquellos que estuvieran apagados en el momento de su generación solo mostrarán información en el listado **Archivos con información personal** si el campo **Última vez visto** abarca la fecha en la que se generó el inventario de esos equipos.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Cadena de caracteres
Ruta	Ruta completa de la carpeta donde se almacena el fichero dentro del equipo.	Cadena de caracteres

Campo	Comentario	Valores
Información personal	Tipo de información personal contenida en el fichero.	•  Entidad documento de identidad •  Entidad Pasaporte •  Entidad Tarjeta de crédito •  Entidad Cuenta bancaria •  Entidad Número de la seguridad social •  Entidad Permiso de conducir •  Entidad Dirección de correo electrónico •  Entidad Dirección IP •  Entidad Nombre y Apellido •  Entidad Direcciones •  Entidad Teléfono móvil
Última vez visto	Fecha en la que se tomó la última fotografía del sistema de ficheros del equipo.	Fecha

Tabla 12.33: Campos del listado Archivos con información personal



Para visualizar los datos del listado gráficamente accede al widget **Archivos por tipo de información personal**.

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Cadena de caracteres
Ruta	Ruta completa de la carpeta donde se almacena el fichero dentro del equipo.	Cadena de caracteres
DNIs	Entidad Documento de identidad.	Booleano
Pasaportes	Entidad Número de pasaporte.	Booleano
Tarjetas de crédito	Entidad Número de tarjeta de crédito.	Booleano
Cuentas bancarias	Entidad Numero de cuenta bancaria.	Booleano
Permisos de conducir	Entidad Permiso de conducir.	Booleano
Números de la Seguridad Social	Entidad Número de la seguridad social.	Booleano
Direcciones de correo electrónico	Entidad Dirección de correo electrónico.	Booleano
IPs	Entidad Dirección IP.	Booleano
Nombres y apellidos	Entidad Nombre y apellidos.	Booleano

Campo	Comentario	Valores
Direcciones	Entidad Dirección física.	Booleano
Números de teléfono	Entidad Número de teléfono.	Booleano
Última vez visto	Fecha en la que el fichero fue incluido por última vez en el inventario diario.	Fecha
Estado	Estado del fichero.	• Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando
Error	• El fichero está en uso. • El contenido del fichero ha cambiado con respecto al almacenado en el inventario. • El fichero ha sido borrado por el usuario desde que se generó el inventario y la acción de borrado por parte del administrador. • Error al intentar eliminar el fichero.	Cadena de caracteres

Tabla 12.34: Campos del fichero exportado Archivos con información personal

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil • Servidor
Última vez visto	Muestra el inventario de los equipos que fueron vistos por última vez dentro del rango de fechas especificado.	• Todos • Últimas 24

Campo	Comentario	Valores
		horas • Últimos 7 días • Último mes • Último año
Información personal	Especifica el tipo de entidad que se buscará en el fichero PII.	• DNIs • Tarjetas de crédito • Permisos de conducir • Direcciones de correo electrónico • IPs • Direcciones • Números de teléfonos • Pasaportes • Cuentas bancarias • Números de la seguridad social • NIFs • Nombres y apellidos

Tabla 12.35: Campos de filtrado para el listado Archivos con información personal

Equipos con información personal

Muestra el número de ficheros PII encontrados en cada uno de los equipos de la red. Dependiendo de la configuración de los filtros **Fecha 1** y **Fecha 2** el listado puede utilizarse para mostrar información de varios tipos:

- Si los campos **Fecha 1** y **Fecha 2** están establecidos, el listado muestra la variación en el número de ficheros PII encontrados en cada uno de los equipos de la red entre las dos fechas. Por lo tanto, el listado presenta una evolución en el número de ficheros PII encontrados en cada equipo de la red.
- Si los campos **Fecha 1** y **Fecha 2** están vacíos, el listado muestra los ficheros PII encontrados en cada equipo de la red, según haya sido el resultado del último inventario completo generado.
- Si el campo **Fecha 1** está establecido, el listado muestra los ficheros PII encontrados en cada equipo de la red, según haya sido el resultado del inventario completo creado en la fecha indicada.

Para ver el listado de ficheros PII encontrado en un equipo haz clic en el nombre del equipo. Se abrirá el listado **Archivos con información personal** filtrado por el nombre del equipo elegido.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Archivos (fecha)	Nombre del archivo.	Cadena de caracteres
Variación	Muestra la diferencia en el número de ficheros PII encontrados entre las fechas establecidas en Fecha 1 y Fecha 2. Si el número es positivo se mostrará el icono  . Si el número es negativo se muestra el icono  .	Numérico

Tabla 12.36: Campos del listado Equipos con información personal



Para visualizar los datos del listado gráficamente accede al widget **Equipos con información personal**.

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que	Cadena de

Campo	Comentario	Valores
	pertenece el equipo.	caracteres
Fecha 1	Fecha inicial utilizada en la evolución de ficheros PII.	Fecha
Fecha de inventario	Fecha en la que se generó el inventario completo del equipo.	Fecha
Archivos con información personal	Número de ficheros PII encontrados en la fecha indicada en Fecha 1.	Numérico
Pasaportes	Número de ficheros PII que contienen la entidad Pasaporte encontrada en la fecha indicada en Fecha 1.	Numérico
Tarjetas de crédito	Número de ficheros que contienen la entidad Tarjeta de crédito encontrada en la fecha indicada en Fecha 1.	Numérico
Cuentas bancarias	Número de ficheros que contienen la entidad Cuentas bancarias encontrada en la fecha indicada en Fecha 1.	Numérico
Permisos de conducir	Número de ficheros que contienen la entidad Permisos de conducir encontrada en la fecha indicada en Fecha 1.	Booleano
Números de la Seguridad Social	Número de ficheros que contienen la entidad Números de la Seguridad social encontrada en la fecha indicada en Fecha 1.	Numérico
Direcciones de correo electrónico	Número de ficheros que contienen la entidad Direcciones de correo electrónico encontrada en la fecha indicada en Fecha 1.	Numérico
NIFs	Número de ficheros que contienen la entidad NIF encontrada en la fecha indicada en Fecha 1.	Numérico
IPs	Número de ficheros que contienen la entidad IP encontrada en la fecha indicada en Fecha 1.	Numérico
Nombres y apellidos	Número de ficheros que contienen la entidad Nombre y apellidos encontrada en la fecha indicada en Fecha 1.	Numérico

Campo	Comentario	Valores
Direcciones	Número de ficheros que contienen la entidad Dirección encontrada en la fecha indicada en Fecha 1.	Numérico
Números de teléfono	Número de ficheros que contienen la entidad Número de teléfono encontrada en la fecha indicada en Fecha 1.	Numérico
Fecha 2	Fecha inicial utilizada en la evolución de ficheros PII.	Fecha
Fecha de inventario	Fecha en la que se generó el inventario completo del equipo.	Fecha
Archivos con información personal	Número de ficheros PII encontrados en la fecha indicada en Fecha 2.	Numérico
Pasaportes	Número de ficheros que contienen la entidad Pasaporte encontrada en la fecha indicada en Fecha 2.	Numérico
Tarjetas de crédito	Número de ficheros que contienen la entidad Tarjeta de crédito encontrada en la fecha indicada en Fecha 2.	Numérico
Cuentas bancarias	Número de ficheros que contienen la entidad Cuentas bancarias encontrada en la fecha indicada en Fecha 2.	Numérico
Permisos de conducir	Número de ficheros que contienen la entidad Permisos de conducir encontrada en la fecha indicada en Fecha 2.	Booleano
Números de la Seguridad Social	Número de ficheros que contienen la entidad Números de la Seguridad social encontrada en la fecha indicada en Fecha 2.	Numérico
Direcciones de correo electrónico	Número de ficheros que contienen la entidad Direcciones de correo electrónico encontrada en la fecha indicada en Fecha 2.	Numérico
NIFs	Número de ficheros que contienen la entidad NIF encontrada en la fecha indicada en Fecha 2.	Numérico
IPs	Número de ficheros que contienen la entidad IP encontrada en	Numérico

Campo	Comentario	Valores
	la fecha indicada en Fecha 2.	
Nombres y apellidos	Número de ficheros que contienen la entidad Nombre y apellidos encontrada en la fecha indicada en Fecha 2.	Numérico
Direcciones	Número de ficheros que contienen la entidad Dirección encontrada en la fecha indicada en Fecha 2.	Numérico
Números de teléfono	Número de ficheros que contienen la entidad Número de teléfono encontrada en la fecha indicada en Fecha 2.	Numérico

Tabla 12.37: Campos del fichero exportado Equipos con información personal

Herramienta de filtrado

Campo	Comentario	Valores
Buscar	Filtra el listado por el nombre del equipo.	Cadena de caracteres
Fecha 1	Primera fecha a comparar.	Fecha
Fecha 2	Segunda fecha comparar.	Fecha
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil • Servidor
Información personal	Especifica el tipo de entidad que se buscará en el fichero PII.	• DNIs • Tarjetas de crédito • Permisos de conducir • Direcciones de correo electrónico • IPs • Direcciones • Números de teléfonos • Pasaportes • Cuentas bancarias

Campo	Comentario	Valores
		- Números de la seguridad social - NIFs - Nombres y apellidos
Variación	Muestra los equipos cuya variación en el número de ficheros es positiva o negativa.	Positivo: el número de ficheros encontrados en Fecha 2 es superior a Fecha 1. Negativo: el número de ficheros encontrados en Fecha 2 es inferior a Fecha 1. Todos

Tabla 12.38: Campos de filtrado para el listado Equipos con información personal

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta [Información de equipo](#) en la página 218 para obtener más información.

Archivos eliminados por el administrador

Muestra el estado de los ficheros que han recibido en el pasado tareas de borrado o restauración y que todavía permanecen en los equipos de la red, de forma accesible o en la zona de backup.

Campo	Comentario	Valores
Fecha	Fecha en la que el fichero cambió de estado.	Fecha
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Archivos con información personal
Ruta	Localización del archivo dentro del sistema de ficheros del equipo.	Cadena de caracteres
Efectuado por	Cuenta de la consola de administración que originó el cambio de estado del fichero.	Cadena de caracteres

Campo	Comentario	Valores
Estado	Estado del fichero.	• Todos • Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando

Tabla 12.39: Campos del listado Archivos eliminados por el administrador



Para visualizar los datos del listado gráficamente accede al widget **Archivos eliminados por el administrador**.

Campos mostrados en fichero exportado (historial)

Incluye las acciones de borrado y restauración que el administrador ejecutó sobre los ficheros de la red.

Campo	Comentario	Valores
Fecha	Fecha en la que el fichero cambió de estado.	Fecha
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Archivos con información personal
Ruta	Localización del archivo dentro del sistema de ficheros del equipo.	Cadena de caracteres
Efectuado por	Cuenta de la consola de administración que originó el cambio de estado del fichero.	Cadena de caracteres
Estado	Estado del fichero.	• Todos

Campo	Comentario	Valores
		• Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando

Tabla 12.40: Campos del listado Archivos eliminados por el administrador

Campos mostrados en fichero exportado (historial detallado)

Incluye todas las acciones de borrado y restauración que el administrador ejecutó sobre los ficheros de la red a lo largo del tiempo.

Campo	Comentario	Valores
Fecha	Fecha en la que el fichero cambió de estado.	Fecha
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Archivos con información personal
Ruta	Localización del archivo dentro del sistema de ficheros del equipo.	Cadena de caracteres
Efectuado por	Cuenta de la consola de administración que originó el cambio de estado del fichero.	Cadena de caracteres
Estado	Estado del fichero.	• Todos • Eliminado • Pendiente de eliminar • Restaurado

Campo	Comentario	Valores
		- Pendiente de restaurar - Error restaurando

Tabla 12.41: Campos del listado Archivos eliminados por el administrador

Herramienta de filtrado

Campo	Comentario	Valores
Estado	Estado del fichero.	- Todos - Eliminado - Pendiente de eliminar - Restaurado - Pendiente de restaurar - Error restaurando

Tabla 12.42: Campos de filtrado para el listado Archivos eliminados por el administrador

Extensiones de programas soportadas

Nombre de la suite	Producto	Extensiones
Office	Word	- DOC - DOT - DOCX - DOCM - RTF
	Excel	- XLS - XLSM - XLSX - XLSB - CSV

Nombre de la suite	Producto	Extensiones
OpenOffice	PowerPoint	• PPT • PPS • PPSX • PPSM • SLDX • SLDM • POTX • PPTM • PPTX • POTM
	Writer	• ODM • ODT • OTT • OXT • STW • SXG • SXW
	Draw	• ODG • OTG • STD
	Math	• ODF • SXM
	Base	• ODB
	Impress	• OTP • ODP • STI • SXI

Nombre de la suite	Producto	Extensiones
	Calc	• OTS • ODS • SXC
Texto plano		• TXT
Navegadores web	Internet Explorer Chrome Opera Otros	• HTM • HTML • MHT • OTH
Cliente de correo	Outlook Outlook Express	• EML
Otros	Adobe Acrobat Reader	• PDF
	Extensible Markup Language	• XML
	Contribute	• STC
	ArcGIS Desktop	• SXD

Tabla 12.43: Listado de extensiones de programas soportadas

Empaquetadores y algoritmos de compresión soportados

Nombre del compresor / empaquetador / algoritmo	Extensiones
7-ZIP	7Z
bzip2	BZ2
gzip	GZ
Binhex	HQX

Nombre del compresor / empaquetador / algoritmo	Extensiones
LHARC	• LHA • LZH
Lempel-Ziv & Haruyasu	LZH
Lempel-Ziv-Oberhumer / Izop	LZO
Multi-Purpose Internet Mail	MME
Lotus Notes Traveler	NTS
Winrar	RAR
Tar	TAR
Tar & Gzip	TGZ
Uuencode	• UU • UUE
XXEncoding	• XX • XXE
PkZip / PKWare	ZIP

Tabla 12.44: Listado de extensiones de empaquetadores / compresores soportados

Entidades y países soportados

Cytomic Data Watch soporta las entidades mostradas a continuación:

- Cuentas bancarias.
- Tarjetas de crédito.
- Número de identidad personal.
- Direcciones IP.
- Direcciones de correo electrónico.
- Números de teléfono.

- Números de carnet de conducir.
- Números de pasaporte.
- Números de la seguridad social.
- Nombres y apellidos.
- Direcciones físicas.

Países soportados

El formato de las distintas entidades reconocidas varía dependiendo del país. Cytomic Data Watch soporta la detección de entidades de los países mostrados a continuación:

- Alemania
- Austria
- Bélgica
- Dinamarca
- España
- Finlandia
- Francia
- Hungría
- Irlanda
- Italia
- Noruega
- Países Bajos
- Portugal
- Reino Unido
- Suecia
- Suiza

Capítulo 13

Cytomic Patch (Actualización de programas vulnerables)

Cytomic Patches es un módulo integrado en la plataforma Cytomic que localiza los equipos de la red que contienen software con vulnerabilidades conocidas, y los actualiza de forma automática y centralizada. De esta forma minimiza la superficie de ataque, evitando que el malware aproveche fallos del software instalado en los equipos de los usuarios y servidores para infectarlos.

Cytomic Patch es compatible con sistemas operativos Windows, macOS y Linux y detecta aplicaciones de terceros pendientes de actualizar o en EoL (End of Life), así como los parches y actualizaciones publicados por Microsoft para todos sus productos (sistemas operativos, bases de datos, suites ofimáticas, etc.).



Para más información sobre los proveedores y aplicaciones incluidas en Cytomic Patch, consulta <https://info.pandasecurity.com/patchmanagementapp/?type=windows>



Cytomic Patch no es compatible con actualizaciones de seguridad extendidas (licencias ESU). Las licencias ESU (Extended Security Update) permiten ejecutar productos de Microsoft una vez finalizado el plazo de soporte técnico oficial para ellos. Para más información sobre las licencias ESU, su disponibilidad y fechas de finalización, consulta <https://learn.microsoft.com/es-es/lifecycle/faq/extended-security-updates>

Para obtener información adicional sobre los distintos apartados del módulo Cytomic Patch consulta las referencias siguientes:



Crear y gestionar configuraciones en la página **258**: información sobre cómo crear, modificar, borrar o asignar configuraciones a los equipos de la red.

Acceso, control y supervisión de la consola de administración en la página **59**: gestión de cuentas de usuario y asignación de permisos.

Gestión de listados en la página **47**: información sobre cómo gestionar listados.

Contenido del capítulo

Funcionalidades de Cytomic Patch	376
Requisitos mínimos de Cytomic Patch	378
Flujo general de trabajo	380
Configuración del descubrimiento de parches sin aplicar	396
Paneles/widgets en Cytomic Patch	398
Listados del módulo Cytomic Patch	416

Funcionalidades de Cytomic Patch

Toda la funcionalidad de Cytomic Patch se concentra en los puntos de la consola de administración mostrados a continuación:

- **Configuración del descubrimiento de parches a aplicar**: a través del perfil de configuración **Gestión de parches**, accesible desde el panel lateral en el menú superior **Configuración**. Consulta **Configuración del descubrimiento de parches sin aplicar** para más información.
- **Configuración de las exclusiones de parches**: desde el listado **Parches disponibles**. Consulta **Excluir parches en todos o en algunos equipos** para más información.
- **Visibilidad del estado de actualización del parque IT**: mediante widgets en un panel de control independiente, accesible desde el menú superior **Estado**, panel lateral **Cytomic Patch**. Consulta **Estado de gestión de parches** para más información.
- **Listados de parches pendientes de aplicar**: desde los listados **Estado de gestión de parches**, **Parches disponibles** y **Programas "End of Life"** accesibles desde el menú superior **Estado**, panel lateral **Mis listados**, **Añadir**. Consulta **Listados del módulo Cytomic Patch** para más información.
- **Histórico de parches instalados**: desde el listado **Historial de instalaciones**, accesible desde el menú superior **Estado**, panel lateral **Mis listados**, **Añadir**. Consulta **Historial de instalaciones** para más información.

- **Parcheo de equipos:** desde el menú superior **Tareas** y creando una tarea programada de tipo **Instalar parches**. También se pueden parchear los equipos desde los menús de contexto del árbol de grupos en el menú superior **Equipos**, de los listados y desde **Detalle de equipo**. Consulta [Descargar e instalar parches](#) para más información.
- **Excluir equipos de las tareas de instalación de parches.** Es posible excluir equipos o grupos de equipos a la hora de ejecutar tareas de instalación de parches. La exclusión de equipos de las tareas de instalación de parches es una funcionalidad dirigida a los partners que utilizan CYTOMIC Nexus y que gestionan a varios clientes con una única consola de administración CYTOMIC Nexus.

Para más información, consulta el Configuraciones para los productos de seguridadde la [guía de administración de CYTOMIC Nexus](#).
- **Parcheo de equipos de prueba:** al configurar Cytomic Patch es posible designar equipos de prueba en los que instalar parches y comprobar los resultados de la instalación antes de aplicar los parches al resto de equipos de la red. Para designar equipos de pruebas:
 - Crea una configuración de Cytomic Patch, selecciona la opción **Designar como equipos de prueba e instalar parches** en el desplegable **Instalación de parches** y asignala a los equipos de prueba. Para más información consulta [Instalación de parches](#).
 - Crea una tarea de Cytomic Patch y activa el selector **Ejecutar la tarea sólo en equipos de prueba**. Para más información consulta [Configuración de una tarea de instalación de parches](#).
- **Desinstalación de parches:** elige una de las opciones siguientes:
 - Desde el widget **Últimas tareas de instalación de parches**, haz clic en el link **Ver historial de instalaciones**. Consulta [Últimas tareas de instalación de parches](#) para más información.
 - Desde el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona el listado **Historial de instalaciones**. Consulta [Historial de instalaciones](#) para más información.
 - Desde en el menú superior **Tareas**, selecciona la tarea que instaló el parche a desinstalar y haz clic en **Ver parches instalados**.
- Al hacer clic en el parche se muestra su información asociada y el botón **Desinstalar** si es compatible con su desinstalación. Consulta [Desinstalar un parche ya instalado](#) para más información.

Requisitos mínimos de Cytomic Patch



A partir de la fecha 30/09/2024 no será posible añadir a la consola de administración nuevos equipos que utilicen los siguientes sistemas operativos: Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008 (no afecta a Windows Server 2008 R2). Los equipos instalados en una fecha anterior seguirán protegidos. Consulta <https://www.watchguard.com/wgrd-trust-center/end-of-life-policy>.

Versiones de sistemas operativos Windows compatibles

Estaciones

- Windows 7 (32 y 64 bits)
- Windows 8 (32 y 64 bits)
- Windows 8.1 (32 y 64 bits)
- Windows 10 (32 y 64 bits)
- Windows 11 (64 bits)

Servidores

- Windows 2008 (32 y 64 bits) y 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2 y 2016
- Windows Server 2022

Compatibilidad con equipos de arquitectura Windows ARM

Cytomic Patch es parcialmente compatible con equipos Windows que implementan un microprocesador ARM:

- Detecta parches de terceros en sistemas 32 y 64 bits.
- Instala únicamente parches de 32 bits de terceros.
- No detecta ningún parche del sistema operativo

Estas limitaciones no aplican a equipos con sistemas operativos macOS o Linux.

Versiones de sistemas operativos macOS compatibles

- macOS 10.15 Catalina
- macOS 11 Big Sur
- macOS 12 Monterey
- macOS Ventura.
- macOS Sonoma

Instalación de parches de sistema operativo en equipos macOS con arquitectura Apple Silicon

Para instalar parches de sistema operativo en estos equipos, se solicitará al usuario sus credenciales, con un límite de tres intentos. Una vez instalado el parche, el equipo se reiniciará automáticamente.

Si en la tarea de instalación existen otros parches que no necesitan credenciales, su instalación se llevará a cabo con normalidad. Consulta [Instalación de parches de sistema operativo en equipos macOS](#).

Versiones de sistemas operativos Linux compatibles

Distribuciones de 64 bits compatibles:

- **Red Hat:** Versión 7.0 y superiores; 8.0 y superiores.
- **CentOS:** Versión 7.0 y superiores.
- **SuSE Linux Enterprise:** Versión 12.0 y superiores; 15.0 y superiores.



Para una correcta instalación de los parches, es necesario que la configuración del repositorio del equipo no haya sido modificada y apunte a los servidores del proveedor de la distribución.

Comportamiento en equipos no compatibles

Para equipos no compatibles con Cytomic Patch, el comportamiento será el siguiente:

- No se instalará en ellos Cytomic Patch
- Los equipos conservarán las configuraciones y tareas de Cytomic Patch que tenían asignadas, pero no les serán aplicadas.
- En el listado **Parches disponibles** no se incluirá información sobre estos equipos ni el estado de los parches instalados.
- Los equipos no computarán a los efectos de licencias consumidas de Cytomic Patch
- En el historial de instalaciones, las instalaciones anteriores de Cytomic Patch se mostrarán como **No disponible**.

URLs necesarias

- <https://content.ivanti.com>
- <https://application.ivanti.com>
- <https://stlicense.ivanti.com>
- <https://help.ivanti.com>
- <https://license.shavlik.com>

Flujo general de trabajo

Cytomic Patch es una herramienta integral que gestiona el parcheo y actualización de los sistemas operativos y programas instalados en los equipos de la red. Para conseguir reducir de forma eficiente la superficie de ataque de los equipos, es necesario seguir los pasos mostrados a continuación:

- Comprobar que Cytomic Patch funciona correctamente en los equipos instalados.
- Comprobar que los parches publicados están instalados.
- Aislar los equipos con vulnerabilidades conocidas sin parchear.
- Instalar los parches seleccionados.
- Desinstalación (Rollback) de los parches que muestran un mal funcionamiento.
- Excluir parches en todos o en algunos equipos.
- Comprobar que los programas instalados en los equipos no han entrado en EoL.
- Comprobar puntualmente el histórico de instalaciones de parches y actualizaciones.
- Comprobar puntualmente el estado del parcheo de equipos con incidencias.

Comprobar que Cytomic Patch funciona correctamente

Sigue los pasos mostrados a continuación:

- Comprueba que los equipos de la red tienen una licencia asignada de Cytomic Patch y que el módulo está instalado y en funcionamiento. Utiliza el widget **Estado de gestión de parches**
- Comprueba que los equipos con una licencia de Cytomic Patch asignada se comunican con la nube de Cytomic. Utiliza el widget **Tiempo desde la última comprobación**
- Comprueba que los equipos donde se instalarán los parches tienen el servicio Windows Update en ejecución con las actualizaciones automáticas desactivadas.



Activa la configuración **Desactivar Windows Update en los equipos** en el perfil de configuración de **Gestión de parches** para que Advanced EDR pueda gestionar correctamente el servicio. Para más información, consulta **Configuración general**.

En el caso de Windows 10 y posteriores, el sistema operativo permite posponer las actualizaciones de parches de calidad pero no desactivarlas, por lo que estas actualizaciones se lanzarán transcurridos 30 días aunque la configuración **Desactivar Windows Update en los equipos** esté activada.

Comprobar que los parches publicados están instalados

Los parches y actualizaciones se publican de forma constante según los proveedores del software instalado en la red detectan vulnerabilidades y las corrigen. Estos parches tienen asociada una criticidad y un tipo.

- Para obtener una visión general de los parches pendientes de instalar según su tipo y criticidad utiliza el widget **Criticidad de los parches**
- Para ver los parches pendientes de instalación en un equipo o grupo de equipos:
 - En el árbol de equipos (menú superior **Equipos**, pestaña **Carpeta** en el panel lateral) haz clic en el menú de contexto de un grupo y selecciona **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el grupo.
- ó
- En el panel de equipos (menú superior **Equipos**, panel derecho) haz clic en el menú de contexto de un equipo y selecciona **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el equipo.
- Para obtener una visión global detallada de los parches pendientes de instalar:
 - En el menú superior **Estado** haz clic en el panel lateral **Mis listados, Añadir** y selecciona el listado **Parches disponibles**.
 - Utiliza la herramienta de filtrado para acotar la búsqueda.
- Para buscar los equipos que no tienen instalado un parche concreto:
 - En el menú superior **Estado** haz clic en el panel lateral **Mis listados, Añadir** y selecciona el listado **Parches disponibles**.
 - Utiliza la herramienta de filtrado para acotar la búsqueda.
 - Haz clic en el menú de contexto del equipo - parche a buscar y selecciona el menú **Visualizar equipos** con el parche disponible para su instalación.

Aislar los equipos con vulnerabilidades conocidas sin parchear

Para aislar un equipo que todavía no ha recibido un parche ya publicado que corrige una vulnerabilidad conocida:

- En el menú superior **Estado** haz clic en el link **Añadir** del panel lateral y selecciona el listado **Parches disponibles**.
- Haz clic en el menú de contexto de un parche y elige en el menú desplegable la opción **Aislar equipo**.

Descargar e instalar parches

Para instalar los parches y actualizaciones, Cytomic Patch utiliza la infraestructura de tareas implementada en Advanced EDR.

Requisitos de funcionamiento

La instalación de parches publicados por Microsoft utiliza el servicio Windows Update en el equipo del usuario o servidor. Sin embargo, para no solapar la actividad de Cytomic Patch con la del servicio Windows Updates, es recomendable que la configuración de éste se establezca de forma que no tenga actividad en el equipo. Consulta **Configuración general**

Permisos necesarios

La cuenta de usuario utilizada para acceder a la consola web tiene que tener asignado el permiso **Instalar, desinstalar y excluir parches** a su rol. Para obtener más información sobre el sistema de permisos consulta **Gestión de roles y permisos** en la página 67.

Descarga de parches y ahorro de ancho de banda

Antes de la instalación de un parche, es necesaria su descarga desde los servidores del proveedor de software. Esta descarga se produce de forma transparente e independiente en cada equipo cuando se lanza la tarea de instalación. Para minimizar el ancho de banda consumido se puede aprovechar la infraestructura de equipos caché instalada en la red del cliente.

Limitación de la descarga de parches a través de equipos caché y proxy

La descarga de los parches puede realizarse directamente desde Internet o también a través de un equipo caché o proxy de Advanced EDR. Consulta **Configuración de las descargas mediante equipos caché** en la página 279 y **Configuración de listas de acceso a través de proxy** en la página 277.

Según el sistema operativo instalado en el equipo, hay limitaciones a la hora de utilizar un método de descarga u otro;

- **Equipos con sistema operativo Windows o macOS:** pueden descargar parches a través de equipos caché e Internet. No pueden descargar parches a través de proxy de Advanced EDR
- **Equipos con sistema operativo Linux:** utilizan el gestor de paquetes propio de la distribución para

hacer la descarga de los parches desde Internet. No pueden descargar parches a través de equipos caché ni proxy de Advanced EDR.

Los equipos caché almacenan los parches durante un periodo máximo de 30 días, transcurrido el cual se eliminarán. Si un equipo solicita a un equipo caché la descarga de un parche y éste no lo tiene en su repositorio, el equipo solicitante dará un tiempo al equipo caché para que lo descargue. Este tiempo depende del tamaño del parche a descargar. Si no es posible la descarga, el equipo solicitante la iniciará de forma directa.

Una vez aplicados los parches en los equipos, éstos se borrarán del medio de almacenamiento donde residen.

Tipos de tareas de instalación parches

- **Inmediatas (opción Instalar):** instala el parche en el momento sin necesidad de completar toda la configuración de la tarea, pero no reinicia el equipo del usuario, aunque sea requisito para completar la instalación. Las tareas inmediatas inician la descarga de los parches necesarios en el momento en que éstas se crean, de forma que puede darse un alto consumo de ancho de banda si afectan a muchos equipos, o el volumen de la descarga es alto.
- **Programadas (programar instalación):** permite configurar todos los parámetros de la actualización de parches. Si varias tareas coinciden en el mismo momento de inicio se introduce un retardo aleatorio de hasta un máximo de 2 minutos para evitar el solapamiento de descargas y minimizar el consumo de ancho de banda.

Interrupción de las tareas de instalación de parches

Las tareas de instalación de parches pueden cancelarse si el proceso de instalación en el equipo no se ha iniciado todavía. Si la instalación ya ha comenzado no se podrá cancelar la tarea, ya que podría causar errores en los equipos.

Envío de parches según el sistema operativo del equipo

Aunque el administrador establezca como destinatario un equipo incompatible con el tipo de parche a instalar, el equipo solo recibirá los parches correspondientes a su sistema operativo.

Instalación de parches de sistema operativo en equipos macOS

Algunos parches de sistema operativo para equipos macOS fuerzan el reinicio del equipo para finalizar su instalación, independientemente de las opciones de reinicio seleccionadas en la configuración de las tareas de instalación de parches.

Estos parches incorporan soluciones, arreglos y mejoras del sistema operativo instalado, pero no suponen la actualización total del mismo a una versión mayor superior. Se distinguen porque incluyen el texto *SoftwareUpdate* en su nombre, visible en la ventana **Parche detectado** y en el listado **Parches disponibles**.

Mensajes de advertencia

Dado que la instalación de estos parches conlleva un reinicio automático imprescindible, el usuario y el administrador son advertidos de ello en los siguientes supuestos:

- Si el administrador selecciona alguno de estos parches en el listado de parches disponibles para crear una tarea rápida o una tarea programada, se mostrará un mensaje de advertencia. Si lo acepta, se lanzará la instalación (tarea rápida) o se accederá a la configuración de la tarea (tarea programada). Consulta [Desde el listado Parches disponibles](#).
- Si el administrador al configurar la tarea selecciona **macOS** en **Instalar parches de los siguientes productos** se mostrará un mensaje advirtiendo del reinicio y preguntando si quiere incluir estos parches en la tarea. Por defecto, esta opción está desactivada. Consulta [Configuración de una tarea de instalación de parches](#).
- En los equipos destinatarios de la tarea, se le mostrará al usuario un mensaje advirtiendo de que la instalación está en curso y que implica reinicio.

Instalación en equipos macOS con arquitectura Apple

En el caso de los equipos macOS con arquitectura Apple, para instalar parches de sistema operativo es necesario escribir las credenciales de *Volume Owner*.

- **Si las credenciales son correctas:** en la columna **Instalación** del listado **Parches disponibles** se mostrará **Pendiente de reinicio**. Cuando se complete la instalación del parche, el equipo se reiniciará automáticamente y el parche desaparecerá del listado.
- **Si el usuario cancela la instalación:** el equipo se mostrará junto a un código de error en la ventana de resultado de la tarea. Consulta [Resultados de una tarea](#) en la página **836**



Si la tarea de instalación para equipos macOS con arquitectura Apple incluye otros parches para cuya instalación no son necesarias credenciales, su instalación se llevará a cabo con normalidad.

Instalación en equipos macOS con arquitectura Intel

En este caso no es necesario escribir credenciales. En el equipo destinatario de la tarea se mostrará un mensaje advirtiendo de que la instalación del parche está en curso y de que cuando finalice se reiniciará el equipo.



Dado que no es posible posponer el reinicio automático, es muy recomendable salvar y cerrar los archivos que se están utilizando.

Acceso a la instalación de parches en la consola

Desde el listado Parches disponibles

- Selecciona el menú superior **Estado**.
- En la sección **Mis listados** del panel lateral, haz clic en **Añadir** y selecciona el listado **Parches disponibles**
- Utiliza las herramientas de filtrado para acotar la búsqueda.
- Selecciona las casillas de los equipos - parches a instalar.
- Para crear una tarea rápida, haz clic en **Instalar** en la barra superior de herramientas. Para crear una tarea programada, haz clic en **Programar instalación**. Para configurar una tarea programada consulta [Configuración de una tarea de instalación de parches](#).



Si entre los parches elegidos para su instalación hay alguno de tipo sistema operativo para macOS que requiera reinicio automático, se mostrará un mensaje advirtiéndolo.

Consulta [Instalación de parches de sistema operativo en equipos macOS](#)

Desde el listado Parches disponibles por equipo

- Selecciona el menú superior **Estado**.
- En la sección **Mis listados** del panel lateral, haz clic en **Añadir** y selecciona el listado **Parches disponibles por equipos**
- Utiliza las herramientas de filtrado para acotar la búsqueda.
- Haz clic en el menú contextual asociado al parche. Se mostrará el listado **Parches disponibles**. Consulta [Desde el listado Parches disponibles](#).

Desde el árbol de equipos

- Selecciona el menú superior **Equipos** y haz clic en la pestaña **Carpets** del árbol de equipos situado en el panel izquierdo.
- Para instalar parches en un grupo de equipos haz clic en el menú de contexto del grupo y selecciona **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles**. Consulta [Desde el listado Parches disponibles](#).
- Para programar la instalación de parches en un grupo de equipos haz clic en el menú de contexto del grupo y selecciona **Programar instalación de parches**. Se creará una nueva tarea de instalación de parches. Para configurarla consulta [Configuración de una tarea de instalación de parches](#).

Desde el listado del árbol de equipos

- Selecciona el menú superior **Equipos** y haz clic en la pestaña **Carpeta** del árbol de equipos situado en el panel izquierdo.
- Selecciona el grupo de equipos y haz clic en las casillas de selección del listado de equipos.
- Para instalar parches, si has seleccionado un solo equipo haz clic en el menú de contexto asociado al equipo y selecciona **Visualizar parches disponibles**. Si has seleccionado varios, haz clic en **Visualizar parches disponibles** en la barra superior de herramientas. Se mostrará el listado **Parches disponibles**. Consulta [Desde el listado Parches disponibles](#).
- Para programar la instalación de grupos de parches, si has seleccionado un solo equipo haz clic en el menú de contexto asociado al equipo y selecciona **Programar instalación de parches**. Si has seleccionado varios, haz clic en **Programar instalación de parches** en la barra superior de herramientas. Se creará una nueva tarea de instalación de parches. Para configurarla consulta [Configuración de una tarea de instalación de parches](#).

Desde el menú superior Tareas

En el menú superior selecciona **Tareas**, haz clic en **Añadir tarea** y selecciona **Instalar parches**.

Configuración de una tarea de instalación de parches

- Escribe la información general de la tarea en los campos **Nombre** y **Descripción**.
- Si la tarea no tiene destinatarios activados, haz clic en el enlace **Destinatarios (No se ha asignado a ningún equipo)** para abrir una ventana nueva donde seleccionar los equipos que recibirán la tarea configurada.



Para acceder a la ventana de selección de equipos, es necesario guardar previamente la tarea. Si la tarea no ha sido guardada, se mostrará una ventana de advertencia.

- Si quieres enviar la tarea de instalación de parches solo a los equipos de prueba que has designado en la red, desplaza el cursor deslizante **Ejecutar la tarea solo en equipos de prueba**. El rol de equipo de prueba se asigna en la configuración de Cytomic Patch asignada al equipo. Consulta [Funcionalidades de Cytomic Patch](#).
- Selecciona el tipo de equipos que recibirán la tarea: **Estación**, **Portátil** o **Servidor**.
- Haz clic en el botón para agregar equipos individuales o grupos de equipos, y en el botón para eliminarlos.
- En la ventana **Editar tarea**, haz clic en el botón **Ver equipos** para verificar los equipos que recibirán la tarea.
- Indica la programación horaria de la tarea. Se establece mediante dos parámetros:

- **Empieza:** marca el inicio de la tarea.

Valor	Descripción
Lo antes posible (activado)	La tarea se lanza en el momento si el equipo está disponible (encendido y accesible desde la nube), o cuando se encuentre disponible dentro del margen definido en el desplegable Equipo apagado .
Lo antes posible (desactivado)	La tarea se lanza en la fecha seleccionada en el calendario, indicando si se tiene en cuenta la hora del equipo o la hora del servidor Advanced EDR.
Equipo apagado	Si el equipo está apagado o inaccesible, la tarea no se podrá lanzar. El sistema de programación de tareas permite establecer la caducidad de la tarea en función del intervalo de tiempo definido por el administrador, desde 0 (la tarea caduca de forma inmediata si el equipo no está disponible) a infinito (la tarea siempre está activa y se espera a que el equipo esté disponible de forma indefinida): • No ejecutar: la tarea se cancela si en el momento del lanzamiento el equipo no está encendido o no es accesible. • Dar un margen de: define un intervalo de tiempo dentro del cual, si el equipo inicialmente no estaba disponible y vuelve a estarlo, la tarea será lanzada. • Ejecutar cuando se encienda: no establece ningún intervalo de tiempo sino que se espera de forma indefinida a que el equipo esté accesible para lanzar la tarea.

Tabla 13.1: Comportamiento del inicio de la tarea si el equipo no está disponible

- **Frecuencia:** establece un intervalo de repetición cada día, semana, mes o año tomando como referencia la fecha indicada en el campo **Empieza:**

Valor	Descripción
Ejecución única	La tarea se ejecuta de forma puntual a la hora indicada en el campo Empieza .
Diaria	La tarea se ejecuta todos los días a la hora indicada en el campo Empieza .

Valor	Descripción
Semanal	Haz clic en las casillas de selección para establecer la ejecución de la tarea en los días de la semana elegidos, a la hora indicada en el campo Empieza .
Mensual	Elige una de las opciones: - Ejecutar la tarea un día concreto de cada mes. Si se eligen los días 29, 30 o 31 y el mes no tiene esos días, la tarea se ejecuta el último día del mes. - Ejecutar la tarea el primer, segundo, tercer, cuarto o ultima día de la semana de cada mes.

Tabla 13.2: Configuración de la frecuencia de la tarea

- En **Parches de seguridad** indica el nivel de criticidad de los parches a instalar.
- En **Instalar parches de los siguiente productos**, el árbol de productos aparece ordenado por sistemas operativos. Cada sistema operativo contiene los parches disponibles para él. Indica qué productos recibirán parches utilizando las casillas de selección en el árbol de productos.



Si entre los parches elegidos para su instalación hay alguno de tipo sistema operativo para macOS que requiera reinicio automático, se mostrará un mensaje para que selecciones si deseas incluir este tipo de parches en la tarea. Consulta [Instalación de parches de sistema operativo en equipos macOS](#)

Dado que el árbol de productos es un recurso vivo que cambia a lo largo del tiempo, ten en cuenta las siguientes reglas al seleccionar los elementos del árbol:

- Al seleccionar un nodo se marcarán todos sus nodos hijos y sus descendientes. Por ejemplo, al seleccionar Adobe se seleccionarán todos los nodos que quedan por debajo de este nodo.
- Si seleccionas un nodo y posteriormente Cytomic Patch agrega de forma automática un nuevo nodo hijo en la rama seleccionada, este nodo también quedará seleccionado de forma automática. Por ejemplo, si seleccionas el nodo Adobe se seleccionarán todos sus nodos hijos, y si posteriormente dentro de Adobe Cytomic Patch agrega un nuevo nodo (un nuevo programa o familia de programas), éste quedará seleccionado de forma automática. Por el contrario, si se seleccionan manualmente algunos nodos hijo individuales de Adobe y Cytomic Patch añade un nuevo nodo hijo, éste no se seleccionará de forma automática.

- Los programas a parchear se evalúan en el momento en que se ejecuta la tarea, no en el momento de su creación o configuración. Esto implica que si Cytomic Patch agrega una nueva entrada en el árbol después de que el administrador haya configurado una tarea de parcheo, y esta entrada es seleccionada de forma automática según la regla del punto anterior, se instalarán los parches asociados a ese nuevo programa en el momento en que se ejecute la tarea.
- Establece las opciones de reinicio en el caso de que sea un requisito reiniciar el puesto de trabajo o servidor para completar la instalación del parche:
 - **No reiniciar automáticamente:** al terminar la tarea de instalación de parches se le muestra al usuario del equipo una ventana con las opciones **Reiniciar ahora** y **Recordar más tarde**. En caso de elegir ésta última, se volverá a mostrar a las 24 horas siguientes.



A los equipos con sistema operativo Linux sin entorno gráfico, se les enviará un mensaje informando de la necesidad de reiniciar para completar la instalación del parche.

- **Reiniciar automáticamente solo las estaciones de trabajo:** elige el intervalo en el que se reiniciarán los equipos de tipo estación de trabajo. Al cumplirse el tiempo establecido, el agente mostrará al usuario del equipo una ventana de aviso con el botón **Reiniciar ahora** y una cuenta atrás indicando el tiempo restante para el reinicio.



A los equipos con sistema operativo Linux sin entorno gráfico, se les enviará un mensaje concretando el tiempo restante para el reinicio.

Conforme el momento de reinicio se vaya acercando, el usuario dejará de poder cerrar la ventana de aviso. Cada 30 minutos, la pantalla se mostrará en primer plano para recordarle al usuario la necesidad del reinicio. Cuando la cuenta atrás se haya completado, el equipo se reiniciará automáticamente.

- **Reiniciar automáticamente solo los servidores:** el comportamiento es idéntico a la opción **Reiniciar automáticamente solo las estaciones de trabajo** pero aplica solo a equipos de tipo servidor.
- **Reiniciar automáticamente tanto las estaciones de trabajo como los servidores:** el comportamiento es idéntico a la opción **Reiniciar automáticamente solo las estaciones de trabajo** pero aplica tanto a estaciones de trabajo como a servidores.
- Haz clic en **Guardar**. La tarea aparecerá en el listado de tareas configuradas, pero mostrará la etiqueta **Sin publicar**, indicando que no está activa.

- Haz clic en el enlace **Publicar** para introducir la tarea en el programador de Advanced EDR, encargado de marcar el momento en que se lanzan las tareas según su configuración.



Cuando dos o más tareas de instalación de parches que requieren reinicio se solapan en el tiempo, Advanced EDR sigue la estrategia de reiniciar el equipo cuando así lo indique la tarea que tenga establecido el intervalo de reinicio más cercano en el tiempo. De esta forma se evita posponer el reinicio del equipo indefinidamente si se encadenan sucesivas tareas de instalación de parches.

Conversión automática de la frecuencia de ejecución e intervalo de reinicio

Las versiones anteriores de Advanced EDR que no soporten la característica de determinar el intervalo de reinicio, lo establecen de forma automática en 4 horas.

Si alguno de los equipos del parque informático tiene instalada una versión anterior del software de seguridad, es posible que no sea capaz de interpretar correctamente las configuraciones de frecuencia establecidas por el administrador en la consola web. En este caso, cada equipo establecerá las siguientes correspondencias para la configuración de la frecuencia en las tareas a ejecutar:

- **Tareas diarias:** sin cambios.
- **Tareas semanales:** se omiten los días elegidos por el administrador. La primera ejecución se realiza en la fecha indicada en **Empieza** y, a partir de este punto, se ejecutará nuevamente cada 7 días.
- **Tareas mensuales:** se omiten los días elegidos por el administrador. La primera ejecución se realiza en la fecha indicada en **Empieza** y, a partir de este punto, se ejecutará nuevamente cada 30 días.

Descargar los parches de forma manual

En algunos casos Cytomic Patch no puede obtener una URL de descarga para iniciar la instalación del parche de forma automática. El motivo de este escenario es diverso:

- El parche puede ser de pago, o no ser un parche público y requerir el registro previo del usuario, entre otras razones.
- Los parches protegidos por EULAs no pueden ser descargados y redistribuidos por Cytomic

En estos casos Cytomic Patch mostrará un enlace que el administrador podrá tomar como referencia para localizar la descarga del parche. Si el enlace no resulta de utilidad será necesario contactar con el proveedor del software a parchear.

Cytomic Patch implementa un mecanismo mediante el cual integra estas descargas manuales en la consola web para que el administrador pueda añadir los parches descargados manualmente.



Los sistemas operativos Linux y macOS no so compatibles con el procedimiento de descarga manual de parches.

Para añadir un parche de forma manual al repositorio es necesario disponer la URL de descarga del parche proporcionada por el proveedor del producto a actualizar. Una vez tengas la URL sigue los pasos mostrados a continuación:

- Identifica los parches que requieren una descarga manual.
- Obtén la URL de descarga del proveedor.
- Integra el parche descargado en el repositorio de parches.
- Habilita el parche descargado para su instalación.
- Opcional: deshabilita un parche ya habilitado para su instalación

Identifica los parches que requieren una descarga manual

- Desde el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una lista con todos los listados disponibles.
- Elige el listado **Parches disponibles** y configura los siguientes filtros:
 - **Instalación**: Requiere descarga manual.
 - **Mostrar parches no descargables**: Si.
- Haz clic en el botón **Filtrar**. El listado mostrará todos los parches reportados por Cytomic Patch como necesarios para actualizar los equipos de la red y que no son descargables de forma automática.

Obtén la URL de descarga

- Con el listado de parches no descargables que se indica en **Identifica los parches que requieren una descarga manual** haz clic en un parche concreto. Se mostrarán los detalles del parche.
- Haz clic en el campo **URL de descarga** para iniciar la descarga del parche y guarda el nombre del fichero que aparece en el campo **Nombre del archivo**.

Integra el parche descargado en el repositorio de parches

- Localiza en la red un equipo con Advanced EDR instalado y el rol de caché asignado y copia el fichero descargado en la ruta siguiente:

```
c:\Programdata\Panda Security\Panda Aether  
Agent\Repository\ManuallyDeploy.
```



Si la unidad de almacenamiento del equipo ha cambiado a otra diferente de la establecida por defecto en el proceso de instalación del software Advanced EDR, accede a la siguiente ruta:

*x:\Panda Security\Panda Aether
Agent\Repository\ManuallyDeploy*

*Siendo x la unidad donde reside el repositorio del equipo. Consulta **Establecer la unidad de almacenamiento** en la página 275 para mas información.*

- Si la carpeta **ManuallyDeploy** no existe, créala con permisos de administrador para lectura y escritura.
- Si es necesario, renombra el parche recién copiado con el nombre obtenido en el campo **Nombre de archivo** indicado en **Obtén la URL de descarga**.

Habilita el parche descargado para su instalación

- Una vez copiado el parche en el repositorio vuelve al listado **Parches disponibles** y haz clic en el menú de contexto asociado al parche descargado manualmente.
- Elige la opción **Marcar como descargado manualmente**  del menú desplegable. A partir de este momento el parche pasará del estado previo **Requiere descarga manual** al estado **Pendiente (descargado manualmente)** para todos los equipos que requieran su instalación. Una vez en estado **Pendiente (descargado manualmente)** se habilitarán todas las opciones necesarias en el menú de contexto del parche para poder instalarse de la misma forma que un parche descargado automáticamente. Consulta **Descargar e instalar parches** para más información.



Cytomic Patch no comprueba que un parche en estado Pendiente (descargado manualmente) realmente exista en algún equipo con el rol de caché asignado. De igual manera, tampoco comprueba que todos los equipos de la red que deberían recibir el parche tienen asignado un equipo caché con el parche copiado en su repositorio. Es responsabilidad del administrador asegurarse de que los equipos caché que se utilizarán en la descarga de parches tienen en la carpeta ManuallyDeploy los parches necesarios descargables de forma manual.

Deshabilita un parche para su instalación

Para retirar del repositorio un parche previamente integrado sigue los pasos mostrados a continuación:

- En el listado **Parches disponibles** configura un filtro de las siguientes características:
 - **Instalación:** Pendiente (descargado manualmente).
 - **Mostrar parches no descargables:** Si.

- Haz clic en el botón **Filtrar**. El listado mostrará todos los parches descargados de forma manual y habilitados para su instalación.
- Haz clic en el menú de contexto asociado al parche habilitado para su instalación y elige la opción **Marcar como "Requiere descarga manual"** . A partir de este momento el parche dejará de pertenecer al repositorio de parche instalables y perderá las opciones de su menú de contexto.

Desinstalar los parches defectuosos

En alguna ocasión puede suceder que los parches publicados por los proveedores del software no funcionen correctamente. Aunque se recomienda seleccionar un reducido grupo de equipos de prueba previo al despliegue en toda la red, Cytomic Patch también soporta la desinstalación de parches (Rollback).



La desinstalación de parches no es compatible con Linux y macOS.

Requisitos para desinstalar un parche instalado

- El rol del administrador tiene el permiso **Instalar / desinstalar** parche habilitado. Consulta **Instalar / desinstalar y excluir parches** en la página **74** para obtener más información.
- La instalación del parche a desinstalar finalizó completamente.
- El parche se puede desinstalar. No todos los parches soportan esta funcionalidad.

Desinstalar un parche ya instalado

- Accede a la pantalla de desinstalación del parche:
 - En el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona **Historial de instalaciones**.
 - Accede al listado de parches instalados en el menú superior **Tareas**, selecciona la tarea que instaló el parche a desinstalar y haz clic en el link **Ver parches instalados**, situado en la parte superior derecha de la ventana de la tarea.
 - Accede al widget **Últimas tareas de instalación de parches** el menú superior **Estado**, menú lateral **Cytomic Patch** y haz clic en el link **Historial de instalaciones**.
- Selecciona de la lista el parche a desinstalar.
- Si el parche se puede desinstalar, se mostrará el botón **Desinstalar el parche**. Haz clic en el botón para mostrar la ventana de selección de equipos:
 - Selecciona **Desinstalar en todos los equipos** para eliminar el parche de todos los equipos de la red.
 - Selecciona **Desinstalar solo en...** para eliminar el parche del equipo indicado.

- Cytomic Patch creará una tarea de ejecución inmediata que desinstalará el parche.
- Si el parche requiere el reinicio del equipo de usuario para completar su desinstalación, se esperará a que el usuario lo reinicie de forma manual.



*Un parche desinstalado volverá a mostrarse en los listados de parches disponibles a no ser que haya sido excluido. Si has configurado una tarea programada de instalación de parches y el parche no ha sido excluido, éste se volverá a instalar en su próxima ejecución. Si el parche ha sido retirado por el proveedor, no se volverá a mostrar ni a instalar. Consulta **Excluir parches en todos o en algunos equipos** para más información.*

Comprobar el resultado de las tareas de instalación / desinstalación de parches

Para consultar las tareas de instalación / desinstalación, haz clic en el menú superior **Tareas** se puede consultar aquellas que han instalado o desinstalado parches en los equipos. Ambas ofrecen la posibilidad de Ver resultados para ver en detalle sobre qué equipos se ha realizado cada una de las acciones y qué parches se han instalado/desinstalado. Consulta **Resultados tarea de instalación / desinstalación de parches** y **Ver parches instalados / desinstalados** para más información.

Excluir parches en todos o en algunos equipos

Para evitar la instalación de los parches que han tenido un mal funcionamiento o que cambian de forma importante las características del programa que los recibe, el administrador de la red puede excluirlos a discreción. Para ello sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Estado** y en el panel lateral **Añadir** en la zona **Mis listados**. Elige el listado **Parches disponibles**. Este listado muestra una línea por cada par equipo - parche disponible. Un parche disponible es aquel que no ha sido instalado en algún equipo de la red o que ha sido desinstalado.
- Para excluir un único parche haz clic en el menú de contexto asociado al parche  y elige la opción **Excluir** . Se mostrará una ventana emergente para seleccionar el tipo de exclusión.
 - **Excluir solo para el equipo X:** excluye el parche elegido en el equipo indicado en el listado.
 - **Excluir para todos los equipos:** el parche elegido se excluirá de todos los equipos de la red.
- Para excluir varios parches y/o un único parche de varios equipos selecciónalos con las casillas de selección, haz clic en la barra de acciones y elige la opción **Excluir** . Se mostrará una ventana emergente para seleccionar el tipo de exclusión:
 - **Excluir solo para los equipos seleccionados:** excluye los parches elegidos en los equipos indicados en el listado.

- **Excluir para todos los equipos:** los parches elegidos se excluirán de todos los equipos de la red.



Los parches excluidos hacen referencia a una versión concreta del parche, de forma que si se excluye un determinado parche y posteriormente el proveedor del software publica otro posterior, éste último no se excluirá automáticamente.

Comprobar que los programas no han entrado en EoL

Los programas que han entrado en EoL no reciben ningún tipo de actualización por parte de los proveedores de software, de forma que se recomienda sustituirlos por alternativas equivalentes o por versiones más avanzadas.

Para localizar los programas actualmente en EOL o que entrarán en EOL en breve:

- Haz clic en el menú superior **Estado**, panel lateral **Cytomic Patch**:
- En el widget **Programas "End of life"** se muestra la información dividida en tres series:
 - **Actualmente en EOL:** programas instalados en la red que ya no reciben actualizaciones de sus respectivos proveedores.
 - **Actualmente o en 1 año en EOL:** programas instalados en la red que ya están en EOL o que entrarán en EOL en el plazo de un año.
 - **Con fecha EOL conocida:** programas instalados en la red que tienen fecha EOL conocida.

Para localizar todos los programas con información de EOL conocida:

- Haz clic en el menú superior **Estado**, panel lateral **Mis listados, Añadir**.
- Selecciona el **Programas "End of Life"**

El listado contiene una entrada por cada par equipo - programa en EoL.

Comprobar el histórico de instalaciones de parches y actualizaciones

Para determinar si un parche concreto está instalado en los equipos de la red:

- Haz clic en el menú superior **Estado**, panel lateral **Mis listados, Añadir**.
- Selecciona **Historial de instalaciones**.

El listado contiene una entrada por cada par equipo - parche instalado, junto con información sobre su nombre, versión, programa o sistema operativo al que afecta y criticidad / tipo del parche.

Al hacer clic en el menú de contexto de un equipo se muestran las opciones que permiten:

- Ver tareas asociadas a la instalación o desinstalación del parche.
- Ver todos los parches instalados en el equipo.
- Ver todos los equipos que tienen instalados el parche elegido.

Comprobar el nivel de parcheo de los equipos con incidencias

Cytomic Patch relaciona los equipos que tienen incidencias detectadas con su nivel de parcheo, de forma que es posible determinar si un equipo infectado o con amenazas detectadas tiene o no aplicados todos los parches que se han publicado.

Para comprobar si un equipo con una incidencia detectada tiene parches pendientes de instalación:

- En el menú superior **Estado**, widgets **Actividad del malware**, **Actividad de PUPs**, **Actividad de Exploits** o **Programas actualmente bloqueados en clasificación** haz clic en una amenaza - equipo. Se mostrará la información de la amenaza detectada en el equipo.
- En la sección **Equipo afectado** haz clic en el botón **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el equipo.
- Selecciona todos los parches disponibles para este equipo y haz clic en la barra de acciones **Instalar** para crear una tarea inmediata que parcheará el equipo.



Debido a que este proceso puede implicar descargas de parches desde los servidores del proveedor del software a parchear, y por lo tanto retrasar su aplicación en el tiempo, se recomienda aislar el equipo de la red si el equipo ha sido infectado y muestra tráfico de red en su ciclo de vida. De esta forma se minimiza el riesgo de propagación de la infección en la red del cliente mientras el proceso de parcheo se completa. Consulta [Análisis forense](#) en la página 739 para obtener más información acerca del ciclo de vida del malware y [Aislar uno o varios equipos de la red de la organización](#) en la página 805 para más información.

Configuración del descubrimiento de parches sin aplicar

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Gestión de parches**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración.

Permisos requeridos

Permiso	Tipo de acceso
Gestión de parches	Crear, modificar, borrar, copiar o asignar las configuraciones de Gestión de parches.
Ver configuraciones de parches	Visualizar las configuraciones de Gestión de parches.

Tabla 13.3: Permisos requeridos para acceder a la configuración Gestión de parches

Configuración general

- Escribe el nombre y la descripción para la configuración.
- Para que Cytomic Patch gestione las actualizaciones de forma exclusiva y sin interferencias con la configuración local de Windows Update, haz clic en **Desactivar Windows Update en los equipos**.



*En el caso de Windows 10 y posteriores, el sistema operativo permite posponer las actualizaciones de parches de calidad pero no desactivarlas, por lo que estas actualizaciones se lanzarán transcurridos 30 días aunque la configuración **Desactivar Windows Update en los equipos** esté activada.*

- Haz clic en el botón **Guardar**.
- En la lista de configuraciones, haz clic en la configuración que has creado. Se mostrara la ventana **Editar configuración**. Para seleccionar los equipos a los que se asignará la configuración, haz clic en el enlace **Destinatarios (No se ha asignado a ningún equipo)**.
- Para agregar equipos individuales, utiliza . Para eliminarlos, haz clic en .
- En la ventana **Editar configuración**, haz clic en el selector **Buscar parches automáticamente** para activar la búsqueda de parches. Si el selector no está activado los parches pendientes de instalación no se mostrarán en los listados, aunque las tareas de instalación de parches podrán aplicarlos de forma independiente.

Instalación de parches

Al configurar Cytomic Patch se pueden seleccionar diferentes opciones de instalación de parches, que se aplicarán a los equipos y grupos de equipos destinatarios:

- **Instalar parches** los parches se instalarán en los equipos y grupos de equipos destinatarios.
- **Designar como equipos de prueba e instalar parches:** los equipos o grupos destinatarios serán identificados como equipos de prueba para la instalación de parches. Para más información, consulta [Funcionalidades de Cytomic Patch](#)
- **No instalar parches:** los parches no se instalarán en los equipos o grupos de equipos destinatarios. Esta opción es aplicable a proveedores de servicios que tengan contratado Cytomic Patch. Para más información, consulta el capítulo **Configuraciones para los productos de seguridad** de la Guía de administración de CYTOMIC Nexus.

Frecuencia de la búsqueda

Buscar parches con la siguiente frecuencia establece cada cuanto tiempo Cytomic Patch consulta los parches instalados en los equipos y los compara con las bases de datos de parches disponibles.

Criticidad de los parches

Establece la criticidad de los parches que Cytomic Patch busca en las bases de datos de parches disponibles.

En el caso de los equipos y dispositivos con sistema operativo macOS o Linux, no se aplican parches de tipo Windows Service Pack.

La criticidad de cada parche está establecida por cada proveedor del software afectado por la vulnerabilidad. Este criterio de clasificación no es uniforme y se recomienda comprobar previamente la descripción del parche para aquellos que no estén clasificados como “críticos”, con el objetivo de evitar su instalación si no se padecen los síntomas descritos.



*Las criticidades relacionadas con parches de resolución de bugs y mejoras para macOS y Linux, se incluyen dentro de la categoría **Otros parches (no de seguridad)**.*

Paneles/widgets en Cytomic Patch

Acceso al panel de control

Para acceder al panel de control haz clic en el menú superior **Estado**, panel lateral **Cytomic Patch**.

Permisos requeridos

Permisos	Acceso al widget
Sin permisos	• Estado de gestión de parches • Tiempo desde la última comprobación

Permisos	Acceso al widget
Instalar, desinstalar y excluir parches	- Programas “End Of Life” - Parches disponibles - Últimas tareas de instalación de parches
Visualizar parches disponibles	- Programas “End Of Life” - Parches disponibles - Últimas tareas de instalación de parches

Tabla 13.4: Permisos requeridos para los widgets de Gestión de parches

Estado de gestión de parches

Muestra los equipos donde Cytomic Patch está funcionando correctamente y aquellos con errores o problemas en la instalación o en la ejecución del módulo. El estado del módulo se representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

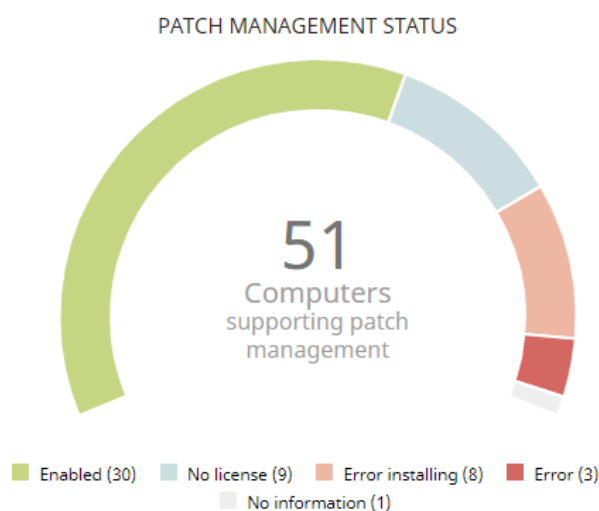


Figura 13.1: Panel de Estado de gestión de parches

Significado de las series

Serie	Descripción
Activado	Indica el porcentaje de equipos en los que Cytomic Patch se instaló sin errores, su ejecución no presenta problemas y la configuración asignada permite buscar parches automáticamente.

Serie	Descripción
Desactivado	Indica el porcentaje de equipos en los que Cytomic Patch se instaló sin errores, su ejecución no presenta problemas y la configuración asignada no permite buscar parches automáticamente.
Sin licencia	Equipos compatibles con Cytomic Patch pero sin licencia de Advanced EDR asignada.
Error instalando	Indica los equipos donde el módulo no se pudo instalar.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con el agente sin actualizar.
Error	El módulo Cytomic Patch no responde a las peticiones del servidor y su configuración difiere de la establecida en la consola web.
Parte central	Refleja el número de total de equipos compatibles con el módulo Cytomic Patch.
Pendiente de reinicio	Indica el número de equipos que están pendientes de reinicio para completar la instalación o desinstalación de parches.

Tabla 13.5: Descripción de la serie Estado de gestión de parches

Filtros preestablecidos desde el panel

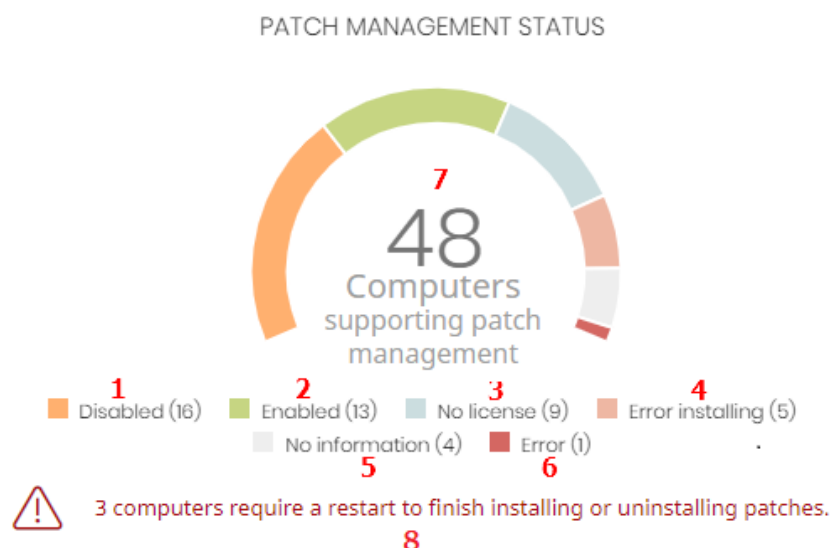


Figura 13.2: Zonas activas del panel Estado de gestión de parches

Al hacer clic en las zonas indicadas en **Zonas activas del panel Estado de gestión de parches** se abre el listado **Estado de gestión de parches** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de gestión de parches = Desactivado.
(2)	Estado de gestión de parches = Activado.
(3)	Estado de gestión de parches = Sin licencia. El equipo no tiene asignada licencia de Advanced EDR.
(4)	Estado de gestión de parches = Error instalando.
(5)	Estado de gestión de parches = Sin información.
(6)	Estado de gestión de parches = Error.
(7)	Sin filtro.
(8)	Estado de gestión de parches = Pendiente de reinicio.

Tabla 13.6: Definición de filtros del listado Estado de gestión de parches

Tiempo desde la última comprobación

Muestra los equipos de la red que no han conectado con la nube de Cytomic en un determinado periodo de tiempo para comprobar su estado de parcheo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

TIME SINCE LAST CHECK



Figura 13.3: Panel Tiempo desde la última comprobación

Significado de las series

Serie	Descripción
72 horas	Número de equipos que no comprobaron su estado de parcheo en las últimas 72 horas.
7 días	Número de equipos que no comprobaron su estado de parcheo en las últimas 7 días.

Serie	Descripción
30 días	Número de equipos que no comprobaron su estado de parcheo en los últimas 30 días.

Tabla 13.7: Descripción de la serie Tiempo desde la última comprobación

Filtros preestablecidos desde el panel



Figura 13.4: Zonas activas del panel Tiempo desde la ultima comprobación

Al hacer clic en las zonas indicadas en **Zonas activas del panel Tiempo desde la ultima comprobación** se abre el listado **Estado de gestión de parches** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 3 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.
(2)	Última conexión = Hace más de 7 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.
(3)	Última conexión = Hace más de 30 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.

Tabla 13.8: Definición de filtros del listado Estado de gestión de parches

Programas “End of life”

Muestra la información relativa al “end of life” de los programas instalados en los equipos de la red, agrupados según el plazo restante.

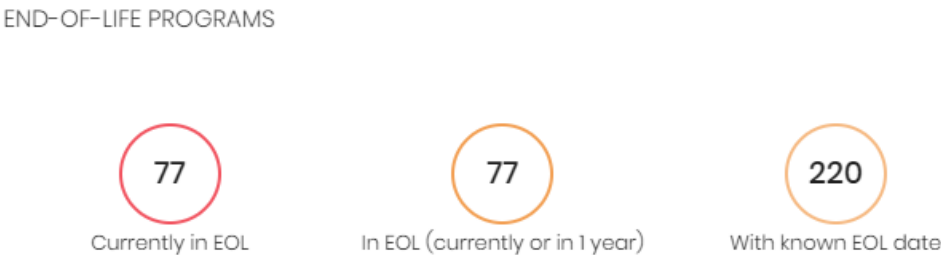


Figura 13.5: Panel Programas “End of life”

Significado de las series

Serie	Descripción
Actualmente en EOL	Programas instalados en el parque informático que ya entraron en EOL.
Actualmente o en 1 año en EOL	Programas instalados en el parque informático que ya han entrado en EOL o entrarán dentro de un año.
Con fecha EOL conocida	Programas instalados en el parque informático cuya fecha de EOL es conocida.

Tabla 13.9: Descripción de la serie Programas “End of life”

Filtros preestablecidos desde el panel



Figura 13.6: Zonas activas del panel Programas “End of life”

Al hacer clic en las zonas indicadas en **Zonas activas del panel Programas “End of life”** se abre el listado **Programas “End Of Life”** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Actualmente en EOL.
(2)	Actualmente o en 1 año en EOL.
(3)	Con fecha EOL conocida.

Tabla 13.10: Definición de filtros del listado Programas “End Of Life”

Últimas tareas de instalación de parches



Consulta **Gestionar tareas** en la página **832** para obtener más información sobre como modificar una tarea ya creada.

Muestra un listado de las últimas tareas de instalación de parches y actualizaciones creadas. Este widget está formado por varios enlaces que permiten gestionar las tareas de instalación de parches:

LAST PATCH INSTALLATION TASKS

- ⋮  **Install Internet Explorer 11 patch on 6 computers** In progress
- ⋮  **New task (Install patches): Install patches with the following criticality** In progress

[View all](#) [View installation history](#)

Figura 13.7: Panel de Últimas tareas de instalación de parches

- Haz clic en una tarea para editar su configuración.
- Haz clic en el enlace **Ver todas** para acceder directamente al menú superior **Tareas** donde se muestran todas las tareas creadas.
- Haz clic en el enlace **Ver historial de instalaciones** para acceder al listado **Historial de instalaciones** con todas las tareas de instalación de parches terminadas con éxito o con error.
- Haz clic en el menú de contexto asociado a una tarea para mostrar una lista desplegable con las opciones siguientes:
 - **Cancelar:** interrumpe la tarea antes de iniciar el proceso de instalación de parches en el equipo.
 - **Ver resultados:** muestra los resultados de la tarea.

Evolución de los parches disponibles

Muestra la evolución de los parches pendientes de instalar en los equipos de la red según su criticidad.

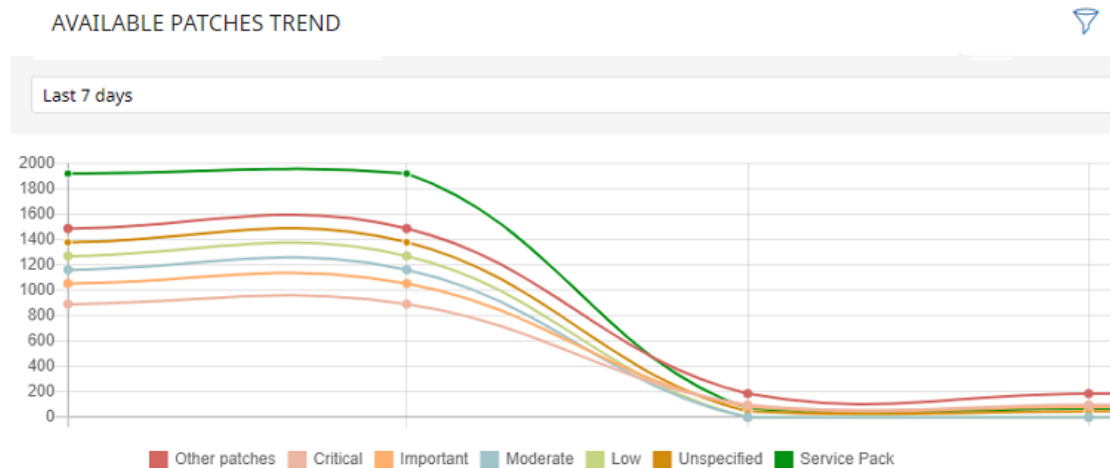


Figura 13.8: Gráfico de Evolución de parches disponibles

Significado de las series

Serie	Descripción
Parches de seguridad - Críticos	Número de parches clasificados como de importancia crítica relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos seguridad - Importantes	Número de parches clasificados de importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - Baja	Número de parches clasificados como de importancia baja relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - No clasificados	Número de parches sin determinar su importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Otros parches (no de seguridad)	Número de parches no relativos a la seguridad del sistema y que no han sido aplicados todavía.
Service Packs	Número de paquetes de parches y actualizaciones que no han sido aplicados todavía. No aplicable a equipos con sistema operativo Linux o macOS.

Tabla 13.11: Descripción de la serie Parches disponibles

Al situar el cursor del ratón sobre uno de los nodos se muestra un tooltip con la siguiente información:

- Fecha
- Tipo
- Número de parches

Filtros preestablecidos desde el panel

Haz clic sobre los elementos de la leyenda debajo de la gráfica para acceder al listado **Parches disponibles** con el filtro correspondiente al tipo seleccionado. Haz clic sobre la gráfica, para acceder al listado completo de **Parches disponibles** sin aplicar ningún filtro.

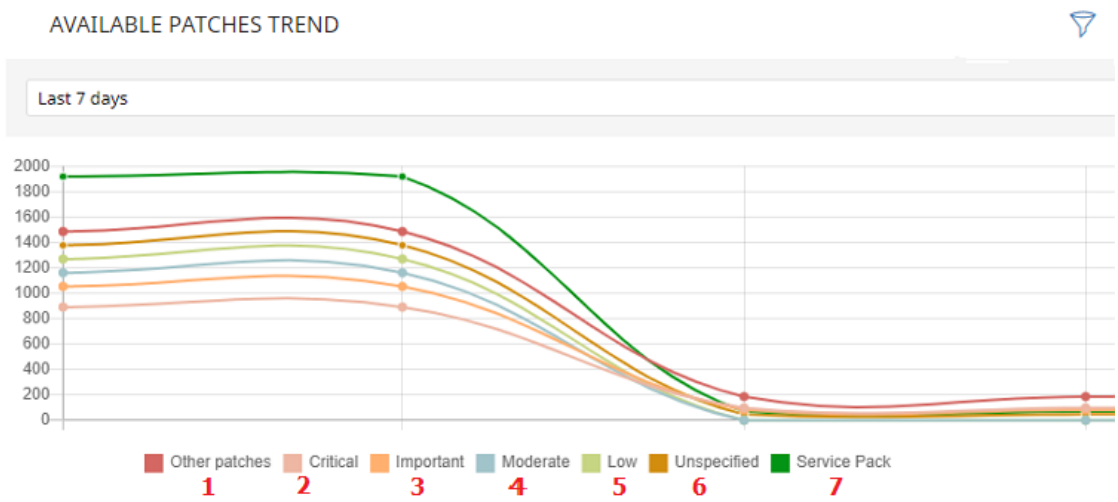


Figura 13.9: Series mostradas en el gráfico Evolución de parches disponibles

Zona activa	Filtro
(1)	Criticidad = Otros parches (no de seguridad).
(2)	Criticidad = Critica (de seguridad).
(3)	Criticidad = Importante (de seguridad).
(4)	Criticidad = Moderada (de seguridad).
(5)	Criticidad = Baja (de seguridad).
(6)	Criticidad=No clasificado (de seguridad)
(9)	Criticidad = Service Pack.

Tabla 13.12: Definición de filtros del listado Parches disponibles

Filtros disponibles sobre el widget

Al hacer clic en el icono  se muestran los filtros disponibles, que se aplican sobre la información mostrada en el propio widget:

Filtro	Definición
Tipo de equipo	- Estación - Portátil - Servidor

Filtro	Definición
Plataforma	Sistema operativo instalado en el equipo.
Parches de sistema operativo	Parches disponibles para sistemas operativos.
Parches de aplicaciones	Parches disponibles para las aplicaciones . Para ver el listado completo de aplicaciones soportadas por Cytomic Patch, consulta https://info.pandasecurity.com/patchmanagementapp/. Para obtener más información acerca de cómo seleccionar las aplicaciones a parchear consulta Configuración de una tarea de instalación de parches.

Tabla 13.13: Filtros disponibles para el widget Evolución de parches disponibles

Parches disponibles

Muestra un recuento de parejas parche - equipo sin aplicar, distribuido por la categoría del parche. Cada parche no aplicado se contabiliza tantas veces como equipos no lo tengan instalado.

AVAILABLE PATCHES



Figura 13.10: Panel Parches disponibles

Significado de las series

Serie	Descripción
Parches de seguridad - Críticos	Número de parches clasificados como de importancia crítica relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos seguridad - Importantes	Número de parches clasificados de importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - Baja	Número de parches clasificados como de importancia baja relativos a la seguridad del sistema y que no han sido aplicados todavía.

Serie	Descripción
Parches críticos de seguridad - No clasificados	Número de parches sin determinar su importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Otros parches (no de seguridad)	Número de parches no relativos a la seguridad del sistema y que no han sido aplicados todavía.
Service Packs	Número de paquetes de parches y actualizaciones que no han sido aplicados todavía.
Ver todos los parches disponibles	Número de parches de cualquier importancia relativos o no a la seguridad del sistema y que no han sido aplicados todavía.
Ver parches excluidos	Número de parches excluidos de su instalación.

Tabla 13.14: Descripción de la serie Parches disponibles

Filtros preestablecidos desde el panel

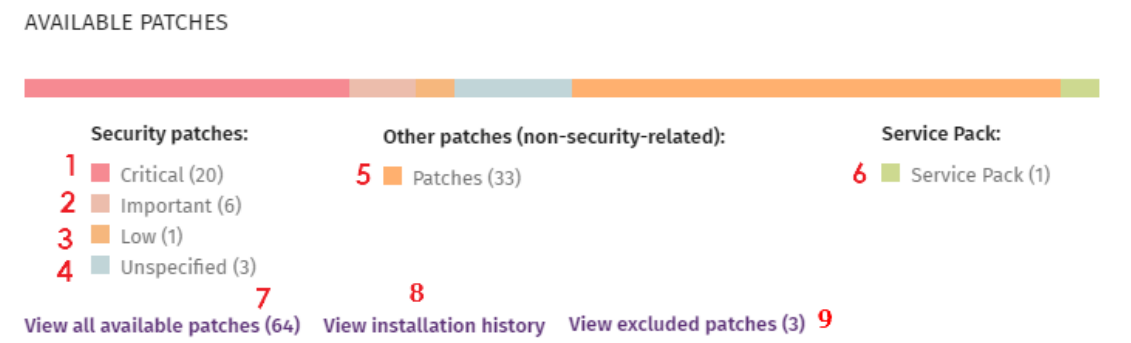


Figura 13.11: Zonas activas del panel Parches disponibles

Al hacer clic en las zonas indicadas en **Descripción de la serie Parches disponibles** se abre un listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Parches disponibles	Criticidad = Crítica (de seguridad).
(2)	Parches disponibles	Criticidad = Importante (de seguridad).
(3)	Parches disponibles	Criticidad = Baja (de seguridad).
(4)	Parches disponibles	Criticidad = No clasificado (de seguridad).

Zona activa	Listado	Filtro
(5)	Parches disponibles	Criticidad = Otros parches (no de seguridad).
(6)	Parches disponibles	Criticidad = Service Pack.
(7)	Parches disponibles	Sin filtros.
(8)	Historial de instalaciones	Sin filtros.
(9)	Parches excluidos	Sin filtros.

Tabla 13.15: Definición de filtros del listado Parches disponibles

Filtros disponibles sobre el widget

Al hacer clic en el icono  se muestran los filtros disponibles, que se aplican sobre la información mostrada en el propio widget:

Filtro	Definición
Tipo de equipo	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.
Parches de sistema operativo	Parches disponibles para sistemas operativos.
Parches de aplicaciones	Parches disponibles para las aplicaciones . Para ver el listado completo de aplicaciones soportadas por Cytomic Patch, consulta https://info.pandasecurity.com/patchmanagementapp/. Para obtener más información acerca de cómo seleccionar las aplicaciones a parchear consulta Configuración de una tarea de instalación de parches.

Tabla 13.16: Filtros disponibles para el widget Evolución de parches disponibles

Parches disponibles en más equipos

Muestra el número de equipos afectados por cada parche disponible en estado **Pendiente** o **Pendiente de reinicio** .

MOST AVAILABLE PATCHES FOR COMPUTERS



The .NET Framework...	Cumulative Sec...	SQL Se...	Vulne...	Notep...	Java 8...	Micro...	Notep...
18	16	10	9	9	9	9	9
Microsoft .NET Fram...	Microsoft .NET F...	Network I...	Micro...	Secur...	Java 8...	Sec...	Tim...
18	14	8	7	7	7	6	6
Microsoft security a...	Microsoft .NET F...	Security O...	Securit...	Securit...	Sec...	Q...	S...
16	14	8	6	4	4	3	3
Cumulative Security ...	Vulnerability in ...	Firefox 61...	Securit...	Securit...	Octo...	Se...	Hy...
16	13	7	5	4	3	3	3
Google Chrome 67.0...	Firefox 61.0 x64	Compatibi...	Update...	Update...	Cum...	Se...	Vul...
16	12	7	5	4	3	3	3
		Java 8 Upd...	Securit...	Stop er...	Secur...		
			5	4	3	2	2

Figura 13.12: Panel Parches disponibles en más equipos

Significado de las series

Serie	Descripción
Nombre	Nombre del parche disponible.
Número	Número de equipos con el parche disponible en estado Pendiente o Pendiente de reinicio .
Enlace Ver todos los parches disponibles	Acceso al listado completo de parches disponibles por equipos.

Tabla 13.17: Descripción de las series de Parches disponibles en más equipos

Al situar el cursor del ratón sobre un cuadro, se muestra un tooltip con la siguiente información:

- Nombre del parche.
- Número de equipos que tienen disponible el parche.
- Programa (o familia del sistema operativo).
- Criticidad.
- Fecha de publicación
- Número CVE (Common Vulnerabilities and Exposures).

Filtros preestablecidos desde el panel

Al hacer clic en cualquiera de los cuadros del panel, se abre el listado **Parches disponibles**.

Microsoft .NET Fram... 1	Google Chrome... 16
18	16
The .NET Framework...	Microsoft .NET F...
18	14

Figura 13.13: Zonas activas del panel Parches disponibles en más equipos

Zona activa	Filtro
(1)	Parche = Nombre del parche seleccionado

Tabla 13.18: Definición de filtros del listado Parches disponibles en más equipos

Filtros disponibles sobre el widget

Haz clic en el icono  para mostrar los filtros disponibles que se aplican sobre la información mostrada en el propio widget:

Filtro	Descripción	Valores
Criticidad	Importancia de la actualización y tipo.	- Otros parches (no de seguridad) - Crítica (de seguridad) - Importante (de seguridad) - Moderada (de seguridad) - Baja (de seguridad) - No clasificado (de seguridad) - Service Pack
Tipo de equipo	Clase de dispositivo al que se aplica el parche.	- Estación - Portátil - Servidor
Plataforma	Sistema operativo instalado en el equipo.	- Todos - Windows - Linux

Filtro	Descripción	Valores
		macOS
Tipo de parche	Tipo de software al que se aplicará el parche.	- Parches de aplicaciones - Parches de sistema operativo

Tabla 13.19: Filtros del panel Parches disponibles en más equipos

Equipos con más parches disponibles

Muestra los equipos de la red que tienen más parches disponibles para instalar, y su número.

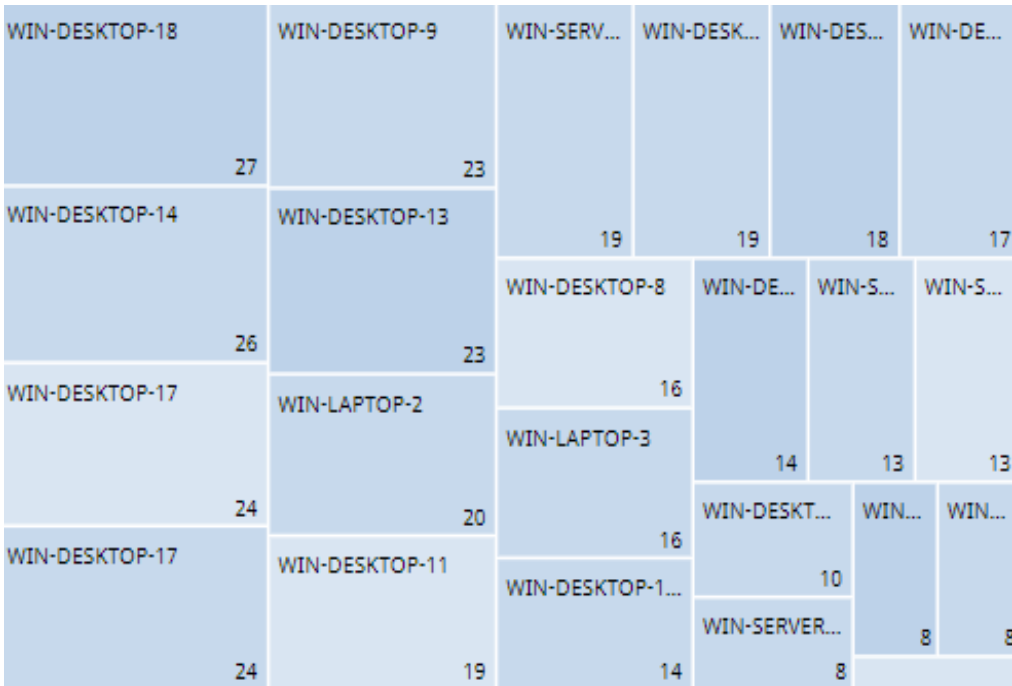


Figura 13.14: Panel Equipos con más parches disponibles

Significado de las series

Serie	Descripción
Nombre	Nombre del equipo con más parches disponibles.
Número	Número de parches disponibles en el equipo.

Tabla 13.20: Descripción de las series del panel Parches disponibles en más equipos

Al situar el cursor del ratón sobre un cuadro, se muestra una etiqueta con la siguiente información:

- Nombre del equipo.
- Número de parches tiene disponible el equipo.

Filtros preestablecidos desde el panel

Al hacer clic en cualquiera de los cuadros del panel, se abre el listado **Parches disponibles**.

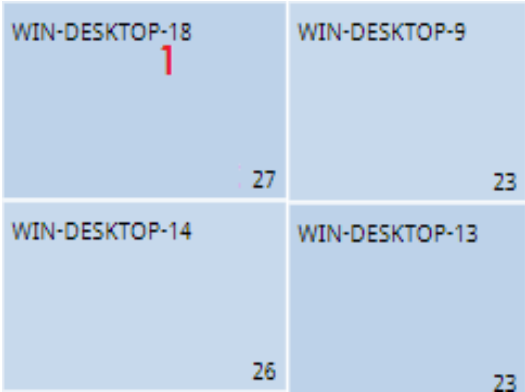


Figura 13.15: Zonas activas del panel Equipos con más parches disponibles

Zona activa	Filtro
(1)	Equipo = Nombre del equipo seleccionado

Tabla 13.21: Definición de filtros del listado Parches disponibles

Filtros disponibles sobre el widget

Haz clic en el icono  para mostrar los filtros disponibles:

Filtro	Descripción	Valores
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Tipo de equipo	Clase de dispositivo al que se aplica el	• Estación

Filtro	Descripción	Valores
	parche.	• Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de parche	Tipo de software al que se aplicará el parche.	• Parches de aplicaciones. • Parches de sistema operativo.

Tabla 13.22: Definición de filtros del panel Equipos con más parches disponibles

Programas con más parches disponibles

Muestra los programas que tienen más parches disponibles para instalar, y su número.

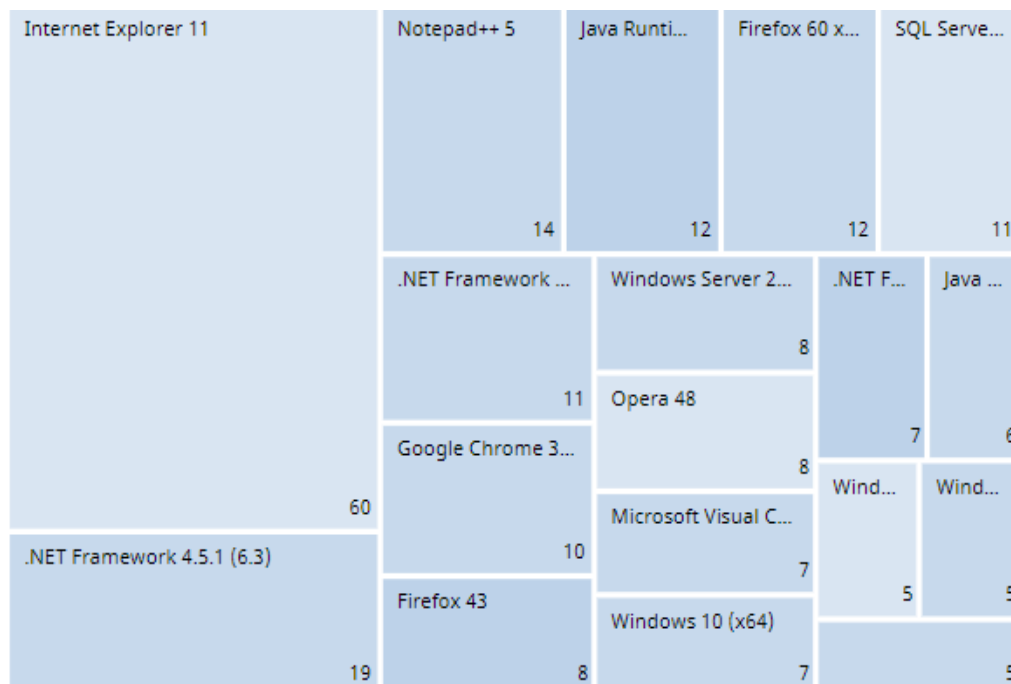


Figura 13.16: Panel Programas con más parches disponibles

Significado de las series

Serie	Descripción
Nombre	Nombre del programa.
Número	Número de parches del programa disponibles.

Tabla 13.23: Descripción de las series del panel Programas con más parches disponibles

Al situar el cursor del ratón sobre un cuadro, se muestra una etiqueta con la siguiente información:

- Nombre del programa.
- Número de parches disponibles del programa.

Filtros preestablecidos desde el panel

Al hacer clic en cualquiera de los cuadros del panel, se abre el listado **Parches disponibles**.



Figura 13.17: Zonas activas del panel Programas con más parches disponibles

Zona activa	Filtro
(1)	Programa = Nombre del programa seleccionado

Tabla 13.24: Definición de filtros del listado Parches disponibles

Filtros disponibles sobre el widget

Haz clic en el icono  para mostrar los filtros disponibles:

Filtro	Descripción	Valores
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad)

Filtro	Descripción	Valores
		• Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Tipo de equipo	Clase de dispositivo al que se aplica el parche.	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de parche	Tipo de software al que se aplicará el parche.	• Parches de aplicaciones. • Parches de sistema operativo.

Tabla 13.25: Definición de filtros del panel Programas con más parches disponibles

Listados del módulo Cytomic Patch

Acceso a los listados

El acceso a los listados se podrá hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Cytomic Patch** y en el widget relacionado.
ó
- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se abrirá una ventana emergente con los listados disponibles.
- Selecciona un listado de la sección **Gestión de parches** para ver su plantilla asociada. Modificala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Los listados de instalación o desinstalación de parches se pueden consultar desde el widget **Historial de instalaciones**, haciendo clic en **Ver historial de instalaciones**.

Los listados **Resultados tarea de instalación / desinstalación de parches** y **Ver parches instalados / desinstalados** se pueden consultar desde el menú superior **Tareas**, haciendo clic en **Ver resultados** en una tarea de instalación o desinstalación.

Permisos requeridos

Permisos	Acceso a listados
Sin permisos	Estado de gestión de parches
Instalar, desinstalar y excluir parches	Acceso a los listados y a los menús de contexto para instalar y desinstalar parches: - Parches disponibles - Historial de instalaciones - Programas "End Of Life" - Parches excluidos - Resultados tarea de instalación / desinstalación de parches - Ver parches instalados / desinstalados
Visualizar parches disponibles	Acceso de solo lectura a los listados: - Parches disponibles - Historial de instalaciones - Programas "End Of Life" - Parches Exclusivos - Resultados tarea de instalación / desinstalación de parches - Ver parches instalados / desinstalados - Evolución de los parches disponibles - Parches disponibles en más equipos - Equipos con más parches disponibles - Programas con más parches disponibles

Tabla 13.26: Permisos requeridos para los listados de Gestión de parches

Estado de gestión de parches

Este listado muestra en detalle todos los equipos de la red compatibles con Cytomic Patch, incorporando filtros que permiten localizar aquellos puestos de trabajo y servidores que no estén recibiendo el servicio por alguno de los conceptos mostrados en el panel asociado.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Estado del equipo	Reinstalación del agente:  Reinstalando agente.  Error en la reinstalación del agente Reinstalación de la protección:  Reinstalando la protección.  Error en la reinstalación de la protección.  Pendiente de reinicio. Estado de aislamiento del equipo:  Equipo en proceso de entrar en aislamiento.  Equipo aislado.  Equipo en proceso de salir del aislamiento. Modo Contención de ataque RDP:  Equipo en modo contención de ataque RDP.  Finalizando modo de contención: de ataque RDP. Instalación de parches  No instalar parches.  Designar como equipos de prueba e instalar parches.	Icono
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres

Campo	Comentario	Valores
Gestión de parches	Estado del módulo.	•  Activado •  Desactivado •  Error instalando (motivo del error) •  Sin licencia •  Sin información •  Error
Última comprobación	Fecha en la que Cytomic Patch consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Última conexión	Fecha del último envío del estado de Advanced EDR a la nube de Cytomic.	Fecha

Tabla 13.27: Campos del listado Estado de gestión de parches

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres

Campo	Comentario	Valores
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Instalación de parches	Opción de instalación de parches aplicada al equipo: • Instalar parches: el equipo tiene Cytomic Patch activado. Los parches se instalarán en el equipo. • Equipo de prueba: el equipo tiene Cytomic Patch activado y ha sido designado "equipo de prueba" para la instalación de parches. • No instalar parches: el equipo tiene Cytomic Patch desactivado. Los parches no se instalarán en el equipo.	Enumeración
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el módulo Cytomic Patch se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha de la última vez que el agente se conectó con la nube de Cytomic.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada.	Booleano

Campo	Comentario	Valores
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Estado de gestión de parches	Estado del módulo.	• Activado • Desactivado • Error instalando • Sin licencia • Sin información • Error
Requiere reinicio	El equipo no se ha reiniciado para completar la instalación o desinstalación de uno o más parches descargados.	Booleano
Fecha de la última comprobación	Fecha en la que Cytomic Patch consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Estado de aislamiento	Indica si el equipo ha sido aislado de la red o se comunica con sus equipos vecinos de forma normal.	• Aislado • No aislado
Fecha error instalación	Fecha en la que se intentó la instalación del módulo Cytomic Patch y se produjo el error.	Fecha
Error instalación	Motivo del error de instalación.	• Error en la descarga • Error en la ejecución

Tabla 13.28: Campos del fichero exportado Estado de gestión de parches

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo	• Todos

Campo	Comentario	Valores
	instalado en el equipo.	- Windows - Linux - macOS
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil - Servidor
Última comprobación	Fecha en la que Cytomic Patch consultó a la nube para comprobar si se han publicado nuevos parches.	- Todos - Hace más de 3 días - Hace más de 7 días - Hace más de 30 días
Última conexión	Fecha de la última vez que el agente se conectó con la nube de Cytomic.	Fecha
Pendiente de reinicio para completar la instalación o desinstalación de parches	El equipo no se ha reiniciado para completar la instalación o desinstalación de uno o más parches.	Booleano
Instalación de parches	Opciones de instalación de parches.	- Instalación de parches activada - Equipo de prueba para la instalación de parches - Instalación de parches desactivada
Estado de gestión de parches	Estado del módulo.	- Activado - Desactivado - Error

Campo	Comentario	Valores
		- Error instalando - Sin licencia - Sin información

Tabla 13.29: Campos de filtrado para el listado Estado de gestión de parches

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se abrirá la ventana de detalle del equipo. Consulta [Información de equipo](#) en la página 218 para obtener más información.

Parches disponibles

Muestra el detalle de los parches disponibles y la información sobre los parches que están en proceso de instalación. Cada línea del listado refleja un par parche - equipo de la red.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software desactualizado y opción de instalación de parches asignada al equipo en la configuración de Cytomic Patch:  No instalar parches.  Designar como equipos de prueba e instalar parches.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Criticidad	Importancia de la actualización y tipo.	Otros parches (no de

Campo	Comentario	Valores
		seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Instalación	Indica el estado de la instalación del parche: • Pendiente: el parche está disponible para el equipo y no ha completado su instalación. • Requiere descarga manual: el parche requiere que el administrador descargue de forma manual el parche y lo copie en un equipo con el rol de cache asignado. Consulta Descargar los parches de forma manual para más información. • Pendiente (descargado manualmente): el parche ya fue descargado de forma manual y forma parte del repositorio de parches. Consulta Descargar los parches de forma manual para más información. • Pendiente de reinicio: el parche ha sido instalado pero el equipo no ha sido reiniciado. Algunos parches pueden no aplicarse hasta realizar este proceso.	Enumeración
Menú de contexto	Despliega un menú de acciones: • Instalar: crea una tarea inmediata de instalación del parche en el equipo elegido. • Programar instalación: crea una tarea configurable de instalación del parche elegido. • Excluir: permite elegir de qué equipo se quiere excluir el	Enumeración

Campo	Comentario	Valores
	parche. • Aislar equipo: aísla el equipo de la red. No disponible para equipos Linux. • Visualizar parches disponibles del equipo: filtra el listado por el equipo elegido para mostrar todos los parches disponibles que aun no se han instalado. • Visualizar equipos con el parche disponible: muestra todos los equipos que tienen disponible el parche elegido para su aplicación.	

Tabla 13.30: Campos del listado Parches disponibles

Campos mostrados en fichero exportado

Utiliza el menú de contexto para exportar los datos. La exportación puede incluir todos los datos del listado de parches disponibles o una versión más reducida que muestra los datos correspondientes a la evolución de los parches disponibles durante los últimos 7 días, último mes o el último año.

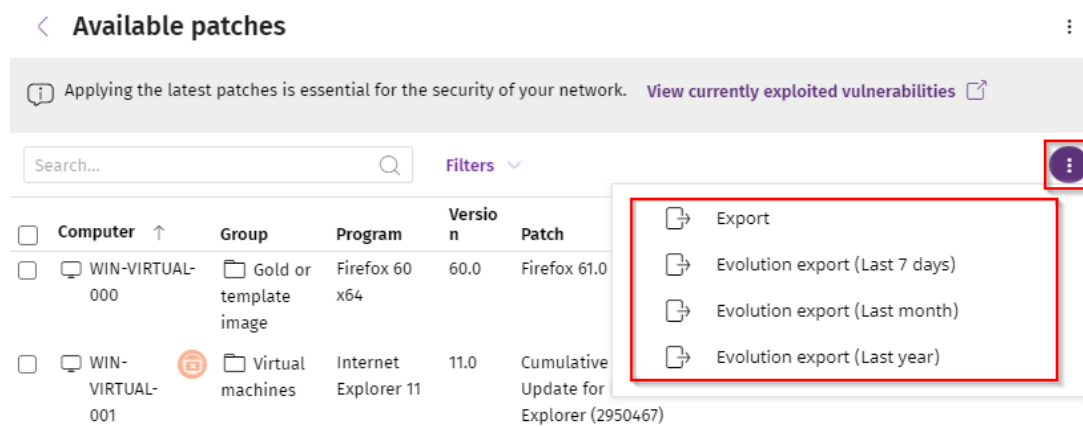


Figura 13.18: Menú de contexto para exportación

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo con software desactualizado.	Cadena de

Campo	Comentario	Valores
		caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Instalación de parches	Opción de instalación de parches aplicada al equipo.	• Instalación de parches activada • Equipo de prueba para la instalación de parches • Instalación de parches desactivada
Vendor	Compañía creadora del programa desactualizado.	Cadena de caracteres
Familia de producto	Nombre de producto con parches pendientes de aplicar o reiniciar.	Cadena de caracteres

Campo	Comentario	Valores
Versión de programa	Número de versión del programa desactualizado.	Numérico
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha

Campo	Comentario	Valores
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha
Es descargable	Indica si el parche está disponible para su descarga o requiere un contrato adicional con el proveedor del software para acceder a aquel.	Booleano
Tamaño de la descarga (KB)	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Estado	Indica el estado de la instalación del parche: • Pendiente: el parche está disponible para el equipo y no ha completado su instalación. • Pendiente (descargado manualmente): el parche ya fue descargado de forma manual y forma parte del repositorio de parches. Consulta Descargar los parches de forma manual para más información. • Requiere descarga manual: el parche requiere que el administrador descargue de forma manual el parche y lo copie en un equipo con el rol de cache asignado. Consulta Descargar los parches de forma manual para más información.	Enumeración
Nombre del archivo	Nombre del archivo que contiene el parche.	Cadena de caracteres
URL de descarga	Recurso HTTP en la infraestructura del proveedor del software para descargar el parche.	Cadena de caracteres

Tabla 13.31: Campos del fichero exportado Parches disponibles

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows

Campo	Comentario	Valores
		- Linux - macOS
Publicación del parche	Fecha en la que el parche se publica y está disponible para su descarga.	- Todos - Hace menos de 7 días - Hace menos de 14 días - Hace menos de un mes - Hace menos de dos meses - Hace más de 7 días - Hace más de 14 días - Hace más de un mes - Hace más de dos meses
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil - Servidor
Tipo de parche	Clase de parche disponible.	- Parches de aplicaciones - Parches de sistema operativo
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres

Campo	Comentario	Valores
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Programa, familia o vendor	La búsqueda se aplicará al programa, familia de productos o compañía seleccionada.	Cadena de caracteres
Instalación de parches	Opción de instalación de parches.	• Instalación de parches activada • Equipo de prueba para la instalación de parches • Instalación de parches desactivada
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack

Campo	Comentario	Valores
Instalación	Muestra los parches que se encuentran en proceso de instalación filtrándolos por la etapa en la que se encuentran.	• Pendiente • Requiere descarga manual • Pendiente (descargado manualmente) • Pendiente de reinicio
Mostrar parches no descargables	Indica los parches que no son descargables directamente por Cytomic Patch debido a requisitos adicionales del proveedor (aceptación de EULA, introducción de credenciales, captchas etc.).	Booleano

Tabla 13.32: Campos de filtrado para el listado Parches disponibles

Ventana Parche detectado

Al hacer clic en una de las filas del listado se abrirá la ventana **Parche detectado**, en la que se muestra información detallada sobre el parche. Los datos pueden variar según el sistema operativo instalado en los equipos.

Esta ventana puede tener el siguiente contenido:

- Información sobre el parche disponible, así como el botón **Instalar el parche**.
- Información sobre el parche en proceso de instalación. El texto **Pendiente de reinicio** aparecerá junto al botón **Instalar el parche**.

Haz clic en el botón **Instalar el parche**. Aparecerá una ventana emergente en la que podrás seleccionar los destinatarios de la tarea de instalación del parche:

- **Instalar solo en el equipo actual:** La tarea se realiza en el equipo seleccionado en la lista.
- **Instalar en todos los equipos del filtro seleccionado:** Selecciona un filtro del árbol de filtros mostrado. El parche se instala en todos los equipos del filtro seleccionado.
- **Instalar en todos los equipos:** El parche se instala en todos los equipos de la red.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base, etc.).	Cadena de caracteres

Campo	Comentario	Valores
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión de programa	Número de versión del programa desactualizado. No disponible para parches de macOS o Linux.	Cadena de caracteres
Familia	Nombre de producto con parches pendientes de aplicar o reiniciar. No disponible para parches de macOS o Linux.	Cadena de caracteres
Vendor	Compañía creadora del programa desactualizado. No disponible para parches de macOS o Linux.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Estado de la instalación	Estado de la instalación del parche o actualización.	• Pendiente • Requiere descarga manual

Campo	Comentario	Valores
		- Pendiente (descargado manualmente) - Pendiente de reinicio
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera. No disponible para parches de macOS o Linux.	Cadena de caracteres
URL de la descarga	URL para descargar el parche de forma individual.	Cadena de caracteres
Nombre del archivo	Nombre del archivo que contiene el parche.	Cadena de caracteres
Descripción	Información sobre el impacto que la vulnerabilidad podría tener en los equipos. No disponible para parches de macOS o Linux.	Cadena de caracteres

Tabla 13.33: Campos de la ventana Parche detectado

Parches disponibles por equipos

Este listado muestra los parches disponibles y el número de equipos donde el parche está disponible para su instalación.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Equipos	Número de equipos en los que está disponible el parche.	Numérico
Menú de contexto	Visualizar equipos con el parche disponible: muestra todos los equipos que tienen disponible el parche elegido para su aplicación.	

Tabla 13.34: Campos del listado Parches disponibles por equipos

Campos mostrados en fichero exportado

Utiliza el menú de contexto para exportar los datos. La exportación puede incluir todos los datos del listado de parches disponibles o una versión más reducida que muestra los datos correspondientes a la evolución de los parches disponibles durante los últimos 7 días, último mes o el último año.

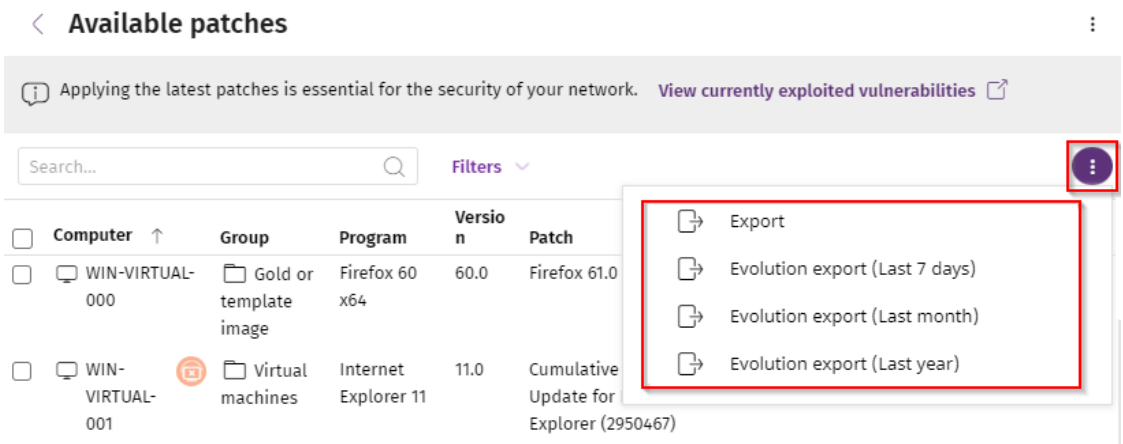


Figura 13.19: Menú de contexto para exportación

Campo	Comentario	Valores
Vendor	Compañía creadora del programa desactualizado.	Cadena de caracteres
Familia de producto	Nombre de producto con parches pendientes de aplicar o reiniciar.	Cadena de caracteres
Versión de programa	Número de versión del programa desactualizado.	Numérico
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Criticidad	Importancia de la actualización y tipo.	- Otros parches (no de seguridad) - Crítica (de seguridad) - Importante (de seguridad) - Moderada (de seguridad)

Campo	Comentario	Valores
		- Baja (de seguridad) - No clasificado (de seguridad) - Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador de KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Equipos	Número de equipos en los que está disponible el parche	Numérico
Plataforma	Sistema operativo instalado en el equipo.	- Windows - macOS - Linux

Tabla 13.35: Campos del fichero exportado Parches disponibles por equipos

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	- Todos - Windows - Linux - macOS
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil

Campo	Comentario	Valores
		• Servidor
Tipo de parche	Clase de parche disponible.	• Parches de aplicaciones • Parches de sistema operativo
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Selecciona versión de programa, familia o vendor	La búsqueda se aplicará al programa, familia de productos o compañía seleccionada.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de

Campo	Comentario	Valores
		seguridad) • Service Pack
Mostrar parches no descargables	Indica los parches que no son descargables directamente por Cytomic Patch debido a requisitos adicionales del proveedor (aceptación de EULA, introducción de credenciales, captchas etc.).	Booleano

Tabla 13.36: Campos de filtrado para el listado Parches disponibles por equipos

Ventana Parche detectado

Al hacer clic en una de las filas del listado se abrirá la ventana **Parche detectado**, en la que se muestra información detallada sobre el parche. Consulta [Ventana Parche detectado](#).

Historial de instalaciones

Muestra las operaciones que Cytomic Patch ha ejecutado a lo largo del tiempo en los equipos de la red.

Campo	Comentario	Valores
Fecha	Fecha en la que se registró la operación.	Fecha
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa o versión del sistema operativo.	Cadena de caracteres
Versión	Versión del programa o sistema operativo.	Cadena de caracteres
Parche	Nombre del parche.	Cadena de caracteres
Criticidad	Importancia del parche.	• Otros parches • Crítica • Importante

Campo	Comentario	Valores
		- Moderada - Baja - No clasificado - Service Pack
Instalación	Estado de la operación registrada.	- Instalado - Requiere reinicio - El parche ya no es requerido - Desinstalado (requiere reinicio) - Error
Menú de contexto ⋮	Muestra un desplegable con opciones.	Ver tarea: muestra la configuración de la tarea asociada a la operación registrada. Visualizar parches instalados del equipo: filtra el listado por el equipo elegido para mostrar todos los parches instalados en él. Visualizar equipos con el parche instalado: muestra todos los equipos que tienen instalado el parche elegido.

Tabla 13.37: Campos del listado Historial de instalaciones

Campos mostrados en fichero exportado

Utiliza el menú de contexto para exportar los datos. La exportación puede ser detallada e incluir todos los datos del listado de historial de instalaciones de parches, o una versión más reducida. En ambos casos, se muestran los datos correspondientes a la instalación de parches durante el tiempo seleccionado.

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil - Servidor
Equipo	Nombre del equipo.	Cadena de caracteres

Campo	Comentario	Valores
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Fecha	Fecha de la operación registrada.	Fecha
Programa	Nombre del programa o versión del sistema operativo.	Cadena de caracteres
Versión	Versión del programa o sistema operativo.	Cadena de caracteres
Parche	Nombre del parche instalado.	Cadena de caracteres
Criticidad	Importancia del parche.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres

Campo	Comentario	Valores
Identificador de KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Instalación	Estado de la instalación del parche o actualización.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado
Error de instalación	El módulo de Cytomic Patch no se instaló correctamente.	• Imposible realizar la descarga: instalador no disponible • Imposible realizar la descarga: fichero corrupto • Espacio insuficiente en disco • Error en la instalación • Error en la descarga
URL de descarga	URL para descargar el parche de forma individual.	Cadena de caracteres
Código de resultado	Código resultado de la operación. Consulta la documentación del proveedor para interpretar el código de resultado.	Numérico
Nombre de la tarea	Nombre de la tarea asociada a la instalación del parche en el equipo. Visible solo al utilizar la opción de exportación detallada.	Cadena de caracteres

Campo	Comentario	Valores
Fecha de lanzamiento de la tarea	Fecha para la que se programa la ejecución de la tarea de Cytomic Patch asociada al equipo. Visible solo al utilizar la opción de exportación detallada.	Fecha
Fecha de inicio de la tarea	Fecha de comienzo de ejecución de la tarea de Cytomic Patch asociada al equipo. Visible solo al utilizar la opción de exportación detallada.	Fecha
Fecha de finalización de la tarea	Fecha en que finaliza la ejecución de la tarea de Cytomic Patch asociada al equipo. Visible solo al utilizar la opción de exportación detallada.	Fecha

Tabla 13.38: Campos del fichero exportado Historial de instalaciones

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Fechas	Período en el que se aplican las instalaciones de parches.	• Últimas 24 horas • Últimos 7 días • Último mes • Rango personalizado
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Criticidad	Importancia del parche instalado.	• Otros parches (no

Campo	Comentario	Valores
		de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Instalación	Estado de la operación registrada.	• Instalado • Requiere reinicio • El parche ya no es requerido • Desinstalado (requiere reinicio) • Error • Error en la descarga • Error en la instalación
Programa	Nombre del programa o versión del sistema operativo.	Cadena de caracteres
Parche	Nombre del parche instalado.	Cadena de caracteres
Intentos de instalación	Muestra todos los intentos fallidos de instalación de un parche en el equipo, o solo el último intento.	• Mostrar sólo el último intento • Mostrar todos los intentos

Campo	Comentario	Valores
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociada al parche.	Cadena de caracteres

Tabla 13.39: Campos de filtrado para el listado Historial de instalaciones

Ventana Parche instalado

Al hacer clic en una de las filas del listado se abrirá la ventana **Parche instalado** con información detallada de la operación registrada. Los datos pueden variar según el sistema operativo instalado en los equipos.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociada al parche.	Cadena de caracteres

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Fecha de instalación	Fecha en la que el parche se registró la operación.	Fecha
Resultado	Estado de la operación registrada.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado • Error en la instalación • Error en la descarga
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	N Numérico
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
Descripción	Notas que incluye el fabricante sobre los efectos que produce aplicar el parche, condiciones especiales y problemas solucionados.	Cadena de caracteres

Tabla 13.40: Campos de la ventana Parche instalado

Programas “End of Life”

Muestra los programas que ya no tienen soporte por parte de sus proveedores y que por tanto son un objetivo especialmente vulnerable para el malware y las amenazas.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software en EoL.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL.	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha (en rojo si el equipo entró en EOL)

Tabla 13.41: Campos del listado Programas EoL

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres

Campo	Comentario	Valores
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL.	Cadena de caracteres
EoL	Fecha en la que el programa entró en EoL.	Fecha
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha

Tabla 13.42: Campos del fichero exportado Programas EoL

Herramienta de filtrado

Campo	Comentario	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Fecha de "End Of Life"	Fecha en la que el programa entrará en EOL.	• Todos • Actualmente en "End of life"

Campo	Comentario	Valores
		Actualmente o en 1 año en "End Of Life"

Tabla 13.43: Campos de filtrado para el listado Programas EoL

Ventana Detalles del programa

Al hacer clic en uno de los programas del listado se accede a la ventana de **Detalles del programa**:

Campo	Comentario	Valores
Programa	Nombre del programa o versión del sistema operativo que recibió el parche.	Cadena de caracteres
Familia	Bundle, suit o grupo de programas al que pertenece el software.	Cadena de caracteres
Editor/Empresa	Empresa que diseñó o publicó el programa.	Cadena de caracteres
Versión	Versión del programa.	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha

Tabla 13.44: Campos de la ventana Detalles del programa

Parches excluidos

Este listado muestra los parches que el administrador ha marcado como excluidos para evitar su instalación en los equipos de la red. Se muestra una línea por cada par parche - equipo excluido, excepto en el caso de exclusiones para todos los equipos de la red, que se mostrarán en una única línea.

Campo	Comentario	Valores
Equipo	Dependiendo del destino de la exclusión el contenido de este campo varía:  Si el parche se ha excluido para un único equipo se incluye el nombre del equipo.  Si el parche se ha excluido para todos los equipos de la cuenta se incluye el literal "(Todos)".	Cadena de caracteres

Campo	Comentario	Valores
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Versión	Versión del programa al que pertenece el parche excluido.	Cadena de caracteres
Parche	Nombre del parche excluido.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Excluido por	Cuenta de usuario de la consola de administración que excluyó el parche.	Cadena de caracteres
Excluido desde	Fecha en la que se excluyó el parche.	Cadena de caracteres

Tabla 13.45: Campos del listado Parches excluidos

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Dependiendo del destino de la exclusión el contenido de este campo varía: Si el parche se ha excluido para un único equipo, indica el nombre del equipo. Si el parche se ha excluido para todos los equipos de la cuenta, indica el literal "(Todos)".	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción del equipo asignada por el administrador de la red.	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Versión	Versión del programa al que pertenece el parche excluido.	Cadena de caracteres

Campo	Comentario	Valores
Parche	Nombre del parche excluido.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga (KB)	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Excluido por	Cuenta de usuario de la consola de administración que excluyó el parche.	Cadena de caracteres

Campo	Comentario	Valores
Excluido desde	Fecha en la que se excluyó el parche.	Cadena de caracteres

Tabla 13.46: Campos del fichero exportado Parches excluidos

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo con un parche excluido.	Cadena de caracteres
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Parche	Nombre del parche excluido.	Cadena de caracteres
Mostrar parches no descargables	Indica los parches que no son descargables directamente por Cytomic Patch debido a requisitos adicionales del proveedor (aceptación de EULA, introducción de credenciales, captchas etc.).	Booleano
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad)

Campo	Comentario	Valores
		• Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack

Tabla 13.47: Campos de filtrado para el listado Parches excluidos

Ventana Parche excluido

Al hacer clic en una de las filas del listado se abrirá la ventana **Parche excluido** con información detallada del parche marcado para no instalarse en los equipos de la red. Los datos pueden variar según el sistema operativo instalado en los equipos.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad)

Campo	Comentario	Valores
		- Baja (de seguridad) - No clasificado (de seguridad) Service Pack
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Excluido por	Cuenta de usuario de la consola de administración que excluyó el parche.	Cadena de caracteres
Excluido desde	Fecha y hora en que excluido el parche.	Numérico
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
Descripción	Notas que incluye el fabricante sobre los efectos que produce aplicar el parche, condiciones especiales y problemas solucionados.	Cadena de caracteres

Tabla 13.48: Campos de la ventana Parche excluido

Resultados tarea de instalación / desinstalación de parches

Este listado muestra los resultados de tareas de instalación o desinstalación de parches en los equipos de la red.

Campo	Descripción	Valores
Equipo	Nombre del equipo en el que se realizó la	Cadena de caracteres

Campo	Descripción	Valores
	instalación / desinstalación del parche.	
Grupo	Grupo de Advanced EDR al que pertenece el equipo.	Cadena de caracteres
Estado	Estado de la tarea.	• Pendiente • En curso • Finalizada • Con error • Cancelada (no se pudo iniciar a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)
Parches instalados / desinstalados	Número de parches instalados / desinstalados.	Cadena de caracteres.
Fecha de comienzo	Fecha en la que se inicio la instalación.	Fecha
Fecha de fin	Fecha en la que se finalizo la instalación.	Fecha

Tabla 13.49: Campos de resultados de tarea de instalación / desinstalación

Herramientas de filtrado

Campo	Descripción	Valores
Estado	Estado de la tarea de instalación / desinstalación.	• Pendiente • En curso • Finalizada • Con error • Cancelada (no se pudo iniciar

Campo	Descripción	Valores
		a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)
Parches aplicados / desinstalados	Equipos en los que se han instalado / desinstalado parches.	• Todos • Sin parches instalados / desinstalados • Con parches instalados / desinstalados

Tabla 13.50: Filtros disponibles en listado Resultados tarea de instalación / desinstalación de parches

Ver parches instalados / desinstalados

Muestra los parches instalados en los equipos y otra información adicional.

Campo	Descripción	Valores
Equipo	Nombre del equipos en el que se realizó la instalación / desinstalación.	Cadena de caracteres
Grupo	Grupo de Advanced EDR al que pertenece el equipo.	Cadena de caracteres
Programa	Programa que recibe el parche.	Cadena de caracteres
Versión	Versión del programa.	Cadena de caracteres
Parche	Parche instalado / desinstalado.	Cadena de caracteres
Criticidad	Relevancia del parche instalado / desinstalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de

Campo	Descripción	Valores
		seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Resultado	Indica si el proceso se ha completado correctamente o ha sucedido algún error.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado
Fecha	Fecha de ejecución del proceso.	Fecha

Tabla 13.51: Campos de resultado de instalación / desinstalación de parches

Configuración de Control de Acceso a Endpoints

Control de Acceso a Endpoints monitoriza las conexiones entrantes que reciben los equipos de la red corporativa, y las autoriza o bloquea según el estado de la seguridad del equipo origen de la conexión.

Cuando el administrador configura una política de control de acceso a endpoints, debe detallar qué características del equipo origen de la conexión colocan en una situación de riesgo al equipo destino. Estas características están relacionadas con el modelo de gestión del equipo origen de la conexión, el estado de la protección instalada en él y su propio nivel de riesgo asociado.

Además, el administrador también deberá configurar los protocolos que se monitorizarán en las conexiones entrantes recibidas y asignar la acción que se ejecutará sobre ellas (autorizar o bloquear).



Para obtener información adicional sobre los distintos apartados del módulo Control de Acceso a Endpoints, consulta las referencias siguientes:

Crear y gestionar configuraciones en la página 258: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.

Acceso, control y supervisión de la consola de administración en la página 59: gestión de cuentas de usuario y asignación de permisos.

Gestión de listados en la página 47: información sobre cómo gestionar listados.

Contenido del capítulo

Configuración de Control de Acceso a Endpoints	459
Opciones de configuración de Control de Acceso a Endpoints	459
Mapa de conexiones	462
Estructura del mapa de conexiones	463
Navegación por el mapa de conexiones	464
Configuración del mapa de conexiones	464
Paneles/widgets de Control de Acceso a Endpoints	466
Listados del módulo Control de Acceso a Endpoints	472

Configuración de Control de Acceso a Endpoints

Requisitos mínimos necesarios

- **Software de protección Advanced EDR:** el equipo debe tener instalada la versión 4.40 de Advanced EDR o una superior.
- **Sistema operativo instalado en el equipo:** Control de Acceso a Endpoints está disponible para equipos con sistema operativo Windows.



Los equipos con sistema operativo macOS o Linux y Advanced EDR 4.40 o superior reportarán el estado del software de protección a los equipo Windows que quieran evaluar su estado de riesgo. Consulta [Modo de funcionamiento de Control de Acceso a Endpoints](#).

- **Puertos abiertos en los equipos:** el agente Advanced EDR requiere el puerto 33000 para la comunicación entre los equipos.

Acceso a la configuración

- Selecciona el menú superior **Configuración**, y haz clic en el menú lateral **Control de Acceso a Endpoints**.
- Haz clic en el botón **Añadir**. Se abrirá la ventana de configuración de **Control de Acceso a Endpoints**.

Permisos requeridos

Permiso	Tipo de acceso
Configurar Control de Acceso a Endpoints	Crear, modificar, borrar, copiar o asignar las configuraciones de Control de Acceso a Endpoints.
Ver configuraciones de Control de Acceso a Endpoints	Visualizar las configuraciones de Control de Acceso a Endpoints.

Tabla 13.52: Permisos requeridos para acceder a la configuración Control de Acceso a Endpoints

Opciones de configuración de Control de Acceso a Endpoints

Para configurar una política de Control de Acceso a Endpoints, sigue estos pasos:

- Escribe el nombre y la descripción para la configuración.
- Haz clic en el botón **Guardar**.
- En la lista de configuraciones, haz clic en la configuración que has creado. Se mostrará la ventana **Editar configuración**.
- Para seleccionar los equipos a los que se asignará la configuración, haz clic en el enlace **Destinatarios (No se ha asignado a ningún equipo)**. Para agregar equipos individuales, utiliza . Para eliminarlos, haz clic en .
- En la ventana **Editar configuración**, desplaza el cursor deslizante **Control de Acceso a Endpoints** a la posición **ON**.
- Para determinar las características que definen el estado de la seguridad en el equipo receptor de la conexión, consulta [Características que definen el estado de la seguridad del equipo origen de la conexión](#)
- Para establecer cuál será la acción que Control de Acceso a Endpoints aplicará cuando detecte una conexión de otro equipo clasificado como en riesgo, consulta [Modo de funcionamiento de Control de Acceso a Endpoints](#)
- Para configurar los protocolos de las conexiones entrantes a monitorizar, consulta [Monitorizar los protocolos en las conexiones entrantes](#)

Características que definen el estado de la seguridad del equipo origen de la conexión

Selecciona qué condiciones del equipo origen de la conexión suponen una situación de riesgo para el equipo destinatario de la conexión:

- **No está administrado/No está disponible:** el equipo origen de la conexión:
 - No tiene instalado un software de protección compatible. Consulta [Requisitos mínimos necesarios](#).
 - No tiene instalada la versión mínima del software de protección Advanced EDR. Consulta [Requisitos mínimos necesarios](#). Para actualizar el agente, la protección y el fichero de firmas del software de seguridad consulta [Actualización del producto](#) en la página 171.
 - No está disponible o un cortafuegos impide la conexión.
- **Está administrado por otra cuenta:** el equipo origen de la conexión se gestiona desde una cuenta diferente de la que gestiona al equipo destinatario de la conexión.
- **Protección no activada:** el equipo origen de la conexión tiene la protección debidamente actualizada pero no activada, y constituye un riesgo para el equipo destinatario de la conexión. Consulta [Requisitos mínimos necesarios](#).
- **Nivel de riesgo mayor que o igual a Medio, Alto o Crítico:** el equipo origen de la conexión tiene

asignado un nivel de riesgo igual o superior a Medio, Alto o Crítico. Consulta [Evaluación de riesgos](#) en la página [645](#)

Modo de funcionamiento de Control de Acceso a Endpoints

En el desplegable **Acción a realizar con las conexiones entrantes desde equipos en riesgo**, selecciona la acción que Control de Acceso a Endpoints aplicará a las conexiones entrantes detectadas en los equipos destinatarios:

- **Auditar:** Control de Acceso a Endpoints informa de las conexiones entrantes procedentes de equipos en riesgo. Consulta [Listados del módulo Control de Acceso a Endpoints](#).

Al tratarse de conexiones que no son bloqueadas por la protección, se muestran en rojo en el diagrama del [Mapa de conexiones](#)

- **Bloquear:** Control de Acceso a Endpoints detecta las conexiones entrantes procedentes de equipos en riesgo y las bloquea.

Al ser conexiones que han sido detectadas y bloqueadas por la protección, se muestran en gris en el diagrama del [Mapa de conexiones](#).

Para que el usuario del equipo reciba un aviso emergente cuando se bloquee una conexión, activa el control deslizante **Mostrar una alerta cuando el Control de Acceso a Endpoints bloquee una conexión**. Puedes añadir un mensaje que acompañará al aviso. Haz clic en **Guardar**.

Monitorizar los protocolos en las conexiones entrantes

De forma predeterminada, Control de Acceso a Endpoints monitoriza las conexiones entrantes para el tráfico SMB (protocolo que permiten a los usuarios comunicarse con equipos y servidores remotos para compartir, abrir y editar archivos) y RDP (protocolo que permite compartir remotamente el escritorio de los equipos).

Para configurar la monitorización de protocolos SMB y RDP, sigue estos pasos:

- Selecciona la casilla del protocolo que quieres configurar, y haz clic en . Se mostrará la ventana **Configurar protocolo**.
- Para añadir puertos a la configuración, escríbelos en la caja de texto y presiona la tecla **Enter**.



*Por defecto, Control de Acceso a Endpoints aplica la monitorización de protocolos a estaciones de trabajo. Si quieres que la aplique también a servidores, desplaza el cursor a la posición **OFF**.*

- Para añadir direcciones IP a las que permitir la conexión con los equipos, escríbelas en la caja de texto y presiona la tecla **Enter**.
- Haz clic en **Guardar**.

Para añadir protocolos diferentes a SMB y RDP:

- En la ventana **Añadir configuración** haz clic en . Se mostrará la ventana **Configurar protocolo**.
- En el desplegable **Protocolo** selecciona el protocolo que quieres monitorizar. Si el protocolo no está en la lista, haz clic en **Personalizado**.
- Sigue los pasos descritos en el punto anterior.
- Haz clic en **Guardar**.

La configuración creada se mostrará en primer lugar en la lista de configuraciones de Control de Acceso a Endpoints.

Mapa de conexiones

El mapa de conexiones representa visualmente las conexiones de los equipos de la red que cumplen las condiciones indicadas en la configuración del control de acceso a endpoints.



Consulta [Configuración de Control de Acceso a Endpoints](#)

Estructura del mapa de conexiones

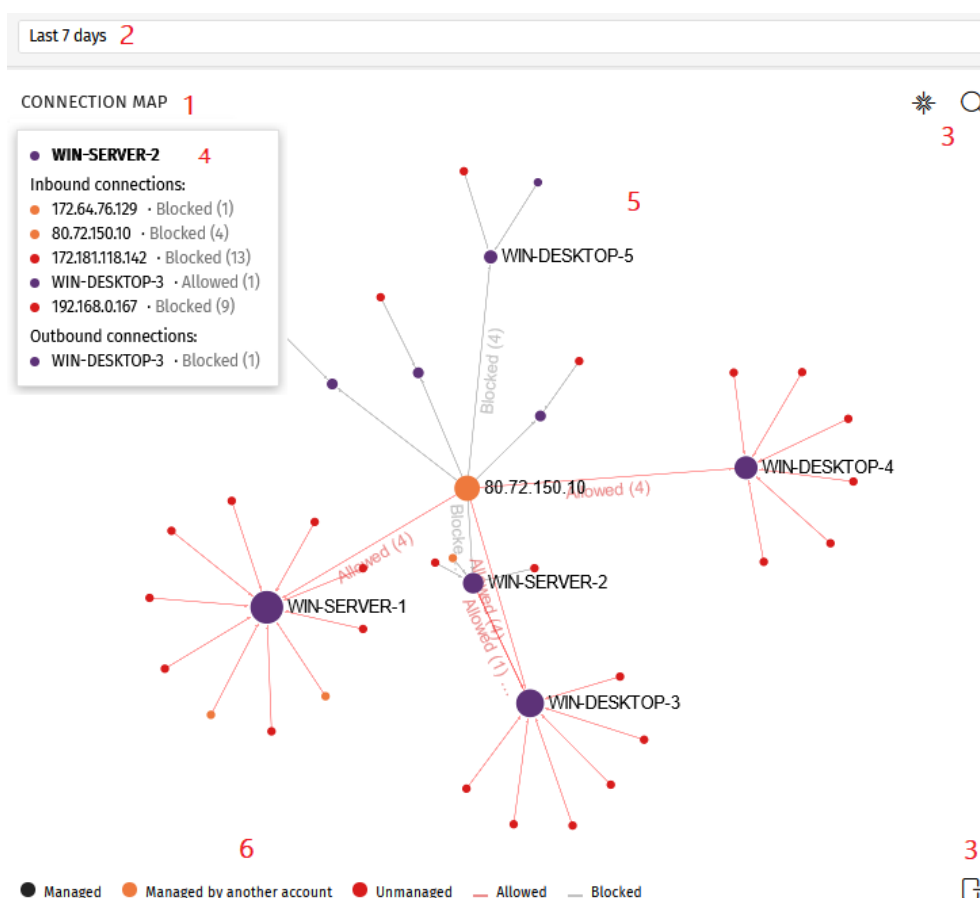


Figura 13.20: Diagrama del, mapa de conexiones

- **Nombre del widget (1)**
- **Selector de tiempo (2):** desplegable para seleccionar el periodo de tiempo sobre el que se mostrarán los datos. Consulta [Configuración del mapa de conexiones](#).
- **Herramientas (3):**
 - Para localizar un equipo o una dirección IP, haz clic en . Consulta [Configuración del mapa de conexiones](#)
 - Para guardar el mapa de conexiones, haz clic en . Consulta [Configuración del mapa de conexiones](#)
- **Panel informativo (4):** al situar el cursor sobre un nodo, se muestra un panel con información sobre las conexiones correspondientes al nodo seleccionado.
- **Diagrama (5):** representación gráfica que utiliza nodos y flechas para mostrar las conexiones entre los equipos y su dirección. También indica la acción que el control de acceso a endpoints llevó a cabo sobre las conexiones, y a cuántas conexiones afectó dicha acción. Consulta [Características](#)

de los nodos y las conexiones.

- **Leyenda (6):** sistema de colores para mostrar equipos administrados y no administrados, y líneas de las conexiones autorizadas y bloqueadas.

Navegación por el mapa de conexiones

- **Zoom:** por defecto, el diagrama se muestra con un nivel de zoom suficiente como para que todos los nodos sean visibles sin necesidad de desplazar la pantalla. Para alejar o acercar el diagrama, sitúa el cursor sobre él y utiliza la rueda del ratón. Haz clic en  para restablecer el tamaño del diagrama.
- **Filtro por grupos:** En función de los equipos o grupos de equipos involucrados en las conexiones, la cantidad de datos que se muestra en el diagrama puede ser elevada. Para limitar la información generada, puedes utilizar el icono  **Filtro por grupo** situado junto al icono  de notificaciones web. Para más información, consulta [Filtrar resultados por grupos](#) en la página 193.
- **Mover el diagrama:** para desplazar el diagrama, haz clic en cualquier lugar del mismo y muévelo en la dirección deseada. Utiliza  para devolverlo a su posición original.
- **Acceso al listado Conexiones identificadas por el Control de Acceso a Endpoints:** al hacer clic en el nodo asociado a un equipo, se muestra el listado **Conexiones identificadas por el Control de Acceso a Endpoints** filtrado por la dirección IP o nombre del equipo.



Consulta [Listados del módulo Control de Acceso a Endpoints](#) y [Características de los nodos y las conexiones](#).

Configuración del mapa de conexiones

- **Rango temporal.** Selecciona el periodo de tiempo sobre el que quieres obtener datos:
 - Últimas 24 horas
 - Últimos 7 días
 - Último mes
 - Último año
- **Herramienta de búsqueda.** Haz clic en  y selecciona en el desplegable el nombre del equipo o dirección IP que quieres localizar en el diagrama.
- **Guardar diagrama.** Puedes ocultar y mostrar capas en el diagrama y guardarlo. Para ello, haz clic en . Se mostrará un menú con las siguientes opciones:

- **Equipos:** oculta o muestra los nodos del diagrama.
- **Conexiones:** oculta o muestra las líneas de las conexiones.
- **Etiquetas de equipos:** oculta o muestra las etiquetas de los nodos.
- **Etiquetas de conexiones:** oculta o muestra las etiquetas de las líneas de conexiones, con el número de conexiones correspondientes a cada línea.
- Haz clic en **Exportar**.

Características de los nodos y las conexiones

En el diagrama del mapa de conexiones, los equipos y las conexiones se representan mediante nodos, líneas y etiquetas asociadas.

Color de los nodos

Los nodos muestran la información mediante su icono asociado:

- **Morado:** equipo administrado.
- **Naranja:** equipo administrado desde una cuenta diferente.
- **Rojo:** equipo no administrado.

Etiquetas de los nodos

Según el tipo de equipo, el nodo muestra en su etiqueta asociada la dirección IP o el nombre del equipo:

- **Equipo administrado desde la misma cuenta que el otro extremo de la conexión:** la etiqueta muestra el nombre del equipo seleccionado.
- **Equipo administrado desde una cuenta diferente a la del otro extremo de la conexión:** la etiqueta muestra la dirección IP del equipo seleccionado.
- **Equipo no administrado:** la etiqueta muestra la dirección IP del equipo seleccionado.



Consulta *Opciones de configuración de Control de Acceso a Endpoints*

Tamaño de los nodos

- **Nodo de equipo administrado (morado):** aumenta o disminuye según el número de conexiones entrantes y salientes.
- **Nodo de equipo administrado desde otra cuenta (naranja):** aumenta o disminuye según el número de conexiones entrantes y salientes.
- **Nodo de equipo no administrado (rojo):** aumenta o disminuye según el número de conexiones salientes.

Líneas de conexiones

Las conexiones entre los nodos se representan mediante la dirección de las líneas y su número:

Dirección de las líneas

- **Línea unidireccional:** el número asociado a la línea indica todas las conexiones permitidas o bloqueadas entre dos nodos durante el periodo de tiempo seleccionado.

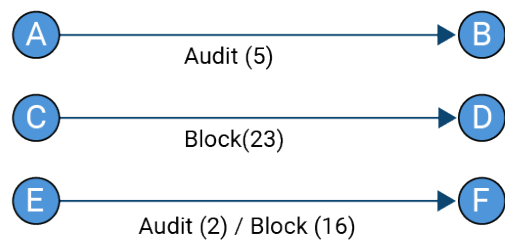


Figura 13.21: Línea unidireccional de la conexión

- **Línea bidireccional:** el número asociado a la línea indica la suma total de las conexiones permitidas y bloqueadas entre dos nodos, en ambas direcciones, durante el periodo de tiempo seleccionado.

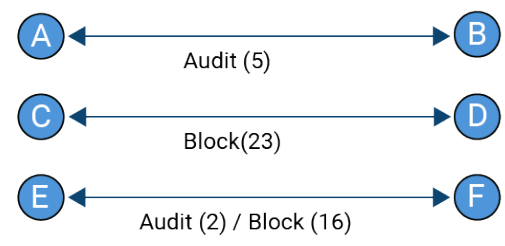


Figura 13.22: Línea bidireccional de la conexión

Color de las líneas

El color de la línea indica la acción que el control de acceso a endpoints ha aplicado a la conexión. Las líneas rojas representan aquellas conexiones que han sido autorizadas en modo Auditoría y, por tanto, no han sido bloqueadas. Las líneas grises representan las conexiones bloqueadas. Consulta [Modo de funcionamiento de Control de Acceso a Endpoints](#).

Paneles/widgets de Control de Acceso a Endpoints

Acceso al panel de control

Para acceder al panel de control, selecciona el menú superior **Estado**, y haz clic en el panel lateral **Control de Acceso a Endpoints**.

Permisos requeridos

Permiso	Acceso al widget
Visualizar detecciones y amenazas	Mapa de conexiones

Permiso	Acceso al widget
	Equipos con conexiones salientes de alto riesgo (top 5)
	Equipos con conexiones entrantes de alto riesgo (top 5)
	Conexiones por condición
	Conexiones por protocolo monitorizado

Tabla 13.53: Permisos requeridos para acceder a los widgets asociados a Control de Acceso a Endpoints

Mapa de conexiones

Representa visualmente las conexiones de los equipos de la red que cumplen las condiciones detalladas en la configuración Control de Acceso a Endpoints. Para ver los detalles de este widget consulta [Mapa de conexiones](#)

Equipos con conexiones salientes de alto riesgo (top 5)

Muestra las cinco direcciones IP o nombres de los equipos que envían más conexiones de alto riesgo a los equipos de la red.

Se muestra el nombre del equipo si:

- El equipo esta administrado por la misma cuenta que gestiona al equipo destino y tiene instalada la versión del software de seguridad 4.40 y superiores.
- El usuario que inició la sesión en la consola tiene visibilidad sobre el equipo.

En el resto de casos se muestra la IP.

TOP 5 COMPUTERS REPORTING HIGH-RISK OUTBOUND CONNECTIONS

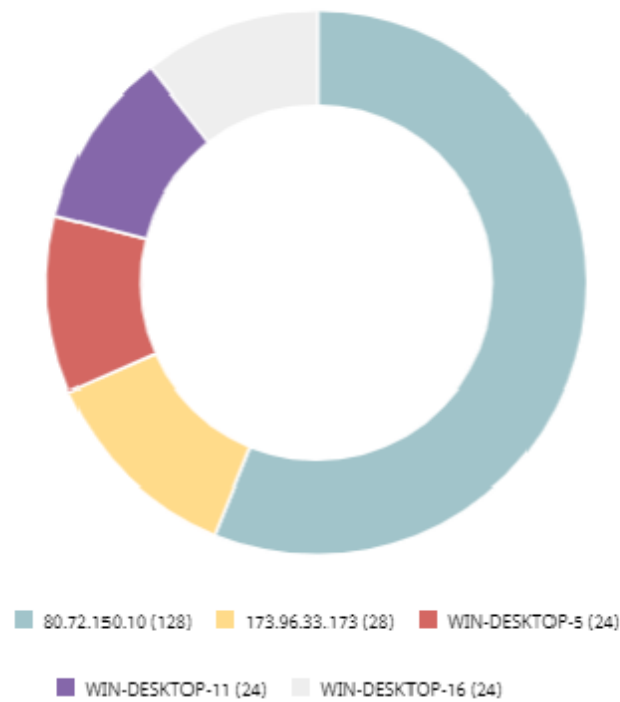


Figura 13.23: Panel de Equipos con conexiones salientes de alto riesgo (top 5)

Significado de las series

Cada color representa una de las cinco direcciones IP o equipos que más conexiones de alto riesgo envían a los equipos de la red, y el porcentaje que suponen sus conexiones enviadas con respecto al total.

Filtros preestablecidos desde el panel

Al hacer clic en una de las series, se abre el listado [Conexiones identificadas por el Control de Acceso a Endpoints](#) filtrado por las conexiones enviadas por el equipo.

Equipos con conexiones entrantes de alto riesgo (top 5)

Muestra los nombres de los cinco equipos de la red que reciben más conexiones entrantes de alto riesgo procedentes de equipos administrados

TOP 5 COMPUTERS REPORTING HIGH-RISK INBOUND CONNECTIONS

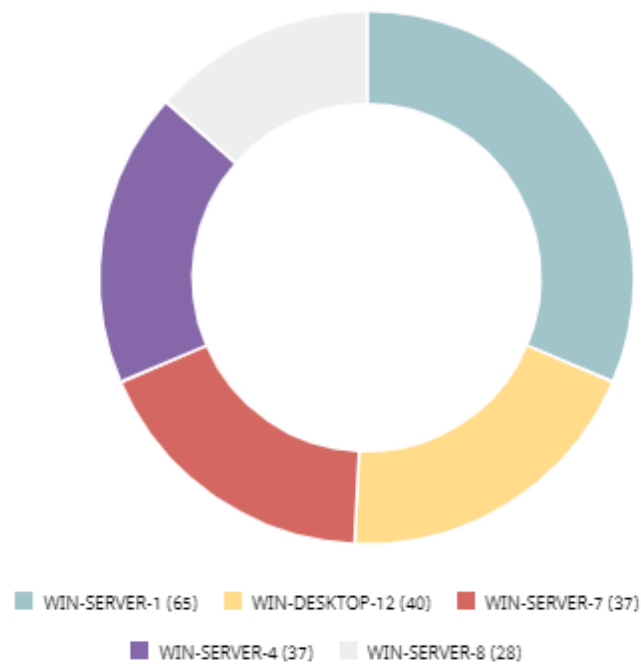


Figura 13.24: Panel de Equipos con conexiones entrantes de alto riesgo (top 5)

Significado de las series

Cada color representa uno de los cinco equipos destinatarios de las conexiones de alto riesgo, y el porcentaje que suponen sus conexiones recibidas con respecto al total.

Filtros preestablecidos desde el panel

Al hacer clic en una de las series, se abre el listado [Conexiones identificadas por el Control de Acceso a Endpoints](#) filtrado por las conexiones recibidas por el equipo.

Conexiones por condición

Muestra la evolución de las conexiones en función de la razón por la cual se las categorizó como peligrosas. Para más información, consulta [Características que definen el estado de la seguridad del equipo origen de la conexión](#)

CONNECTIONS BY CONDITION

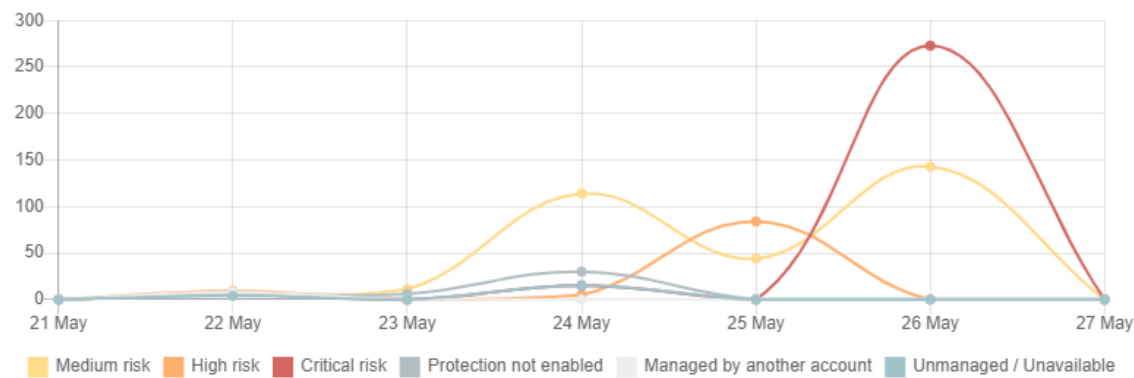


Figura 13.25: Panel Conexiones por condición

Significado de las series

Serie	Descripción
No está administrado/No está disponible	Número de conexiones de los equipos que no cumplen con los requisitos indicados en Requisitos mínimos necesarios .
Protección no activada	Número de conexiones de los equipos que no tienen la protección activada.
Está administrado por otra cuenta	Número de conexiones de los equipos con el software de protección instalado pero administrados por otra cuenta.
Riesgo crítico	Número de conexiones de los equipos en riesgo crítico.
Riesgo alto	Número de conexiones de los equipos en riesgo alto.
Riesgo medio	Número de conexiones de los equipos en riesgo medio.

Descripción de la serie Conexiones por condición

Filtros establecidos desde el panel

CONNECTIONS BY CONDITION

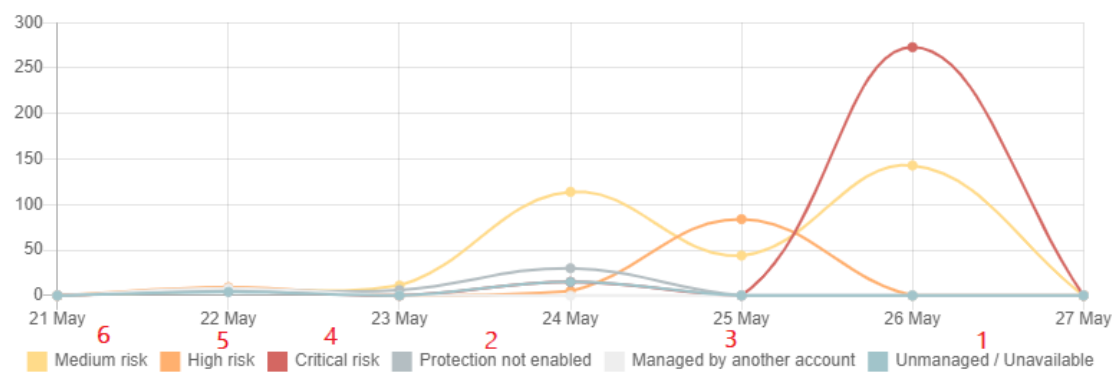


Figura 13.26: Zonas activas del panel Conexiones por condición

Al hacer clic en las zonas indicadas, se abre el listado **Conexiones identificadas por el Control de Acceso a Endpoints** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Listado de las conexiones con riesgo detectado = No está administrado/No está disponible.
(2)	Listado de las conexiones con riesgo detectado = Protección no activada.
(3)	Listado de las conexiones con riesgo detectado = Está administrado por otra cuenta.
(4)	Listado de las conexiones con riesgo detectado = Riesgo crítico.
(5)	Listado de las conexiones con riesgo detectado = Riesgo alto.
(6)	Listado de las conexiones con riesgo detectado = Riesgo medio.

Tabla 13.54: Definición de filtros del widget Conexiones por condición

Conexiones por protocolo monitorizado

Muestra las conexiones detectadas que transportan los protocolos monitorizados a lo largo del tiempo. Consulta **Monitorizar los protocolos en las conexiones entrantes**.

CONNECTIONS BY MONITORED PROTOCOL

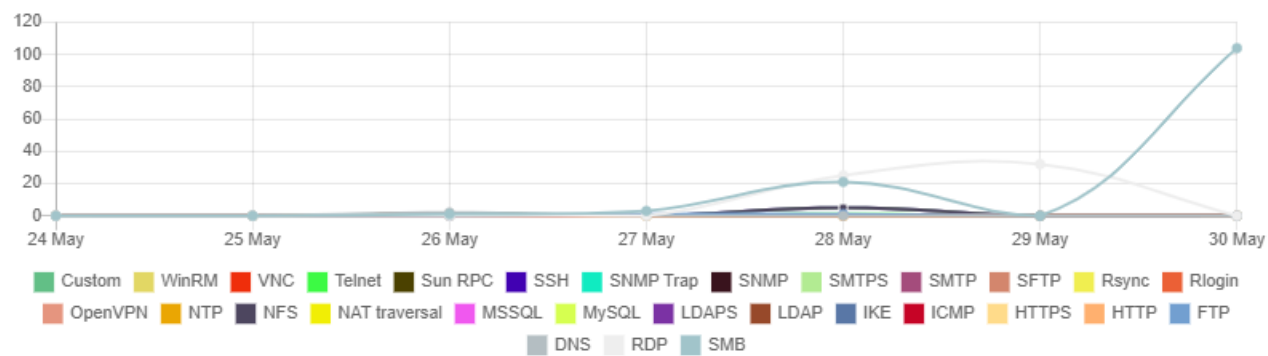


Figura 13.27: Panel de Conexiones por protocolo monitorizado

Significado de las series

Muestra el número de conexiones que se detectaron por cada protocolo.

Filtros establecidos desde el panel

Al hacer clic en un tipo de protocolo, se abre el listado **Conexiones identificadas por el Control de Acceso a Endpoints** con las conexiones en las que se utilizó el protocolo seleccionado.

Listados del módulo Control de Acceso a Endpoints

Acceso a los listados

Puedes acceder a los listados de Control de Acceso a Endpoints mediante las siguientes rutas:

- Desde el menú superior **Estado**, en el panel lateral haz clic en **Control de Acceso a Endpoints**. A continuación,haz clic en alguno de los widgets.
- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles. Haz clic en el listado **Conexiones identificadas por el Control de Acceso a Endpoints**

Permisos requeridos

Permiso	Acceso a listados
Visualizar detecciones y amenazas	Conexiones identificadas por el Control de Acceso a Endpoints

Tabla 13.55: Permisos requeridos para acceder a los listados de Control de Acceso a Endpoints

Conexiones identificadas por el Control de Acceso a Endpoints

Muestra las conexiones entrantes recibidas en los equipos de la red, que cumplen las condiciones detalladas en la configuración Control de Acceso a Endpoints. Consulta **Opciones de configuración de**

Control de Acceso a Endpoints

Campo	Descripción	Valores
Equipo	Nombre del equipo que recibe la conexión.	Cadena de caracteres
Grupo	Grupo al que pertenece el equipo que recibe la conexión.	Cadena de caracteres
Equipo remoto	Dirección IP o nombre del equipo origen de la conexión.	Cadena de caracteres
Riesgo detectado	Estado del equipo origen causante del registro de la conexión.	• No está administrado/No está disponible • Está administrado por otra cuenta • Protección no activada • Riesgo Medio • Riesgo Alto • Riesgo Crítico
Acción	Acción que Advanced EDR aplica a la conexión.	• Permitido • Bloqueado
Protocolo/Puerto	Protocolo/puerto de la conexión registrada.	Numérico
Numero de repeticiones	Número de veces que se detectó la conexión en una hora.	Numérico
Fecha	Fecha en la que Control de Acceso a Endpoints registró la conexión.	Fecha
Menú de contexto	Despliega un menú de acciones: • Ver conexiones del equipo: muestra las conexiones realizadas por el equipo elegido durante el tiempo seleccionado. • Ver conexiones del equipo remoto: muestra las conexiones	Enumeración

Campo	Descripción	Valores
	recibidas por el equipo seleccionado.	

Tabla 13.56: Campos del listado Conexiones identificadas por el Control de Acceso a Endpoints



Para visualizar los datos del listado gráficamente accede al widget **Programas bloqueados** por el administrador

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Identificador o nombre del cliente.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	• Estación • Portátil • Servidor
Equipo	Nombre del equipo que recibe la conexión.	Cadena de caracteres
Grupo	Grupo al que pertenece el equipo que recibe la conexión.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo que recibe la conexión.	Númérico
Riesgo detectado	Estado del equipo origen causante del registro de la conexión	• No está administrado/No está disponible • Está administrado por otra cuenta • Protección no activada • Riesgo Medio • Riesgo Alto • Riesgo Crítico
Protocolo	Protocolo/puerto de la conexión registrada.	Númérico

Campo	Descripción	Valores
Acción	Acción que Control de Acceso a Endpoints aplicó a la conexión.	• Permitido • Bloqueado
Dirección IP local	Dirección IP del equipo que recibe la conexión.	Numérico
Nombre del host remoto	Nombre del equipo origen de la conexión.	Cadena de caracteres
Dirección IP remota	Dirección IP del equipo origen de la conexión.	Numérico
Puerto local	Puerto del equipo destinatario por el que se registró la conexión.	Numérico
Puerto remoto	Puerto utilizado por el equipo origen para establecer la conexión.	Numérico
Fecha	Fecha en la que Control de Acceso a Endpoints registró la conexión.	Fecha
Numero de repeticiones	Número de veces que se detectó la conexión en una hora.	Numérico

Tabla 13.57: Campos del fichero exportado Conexiones identificadas por el Control de Acceso a Endpoints

Herramienta de filtrado

Campo	Descripción	Valores
Buscar equipo	Busca por el nombre del equipo.	Cadena de caracteres
Tipo de equipo	Filtra por clase del dispositivo.	• Estación • Portátil • Servidor
Fechas	Establece un intervalo de fechas desde el día presente hacia el pasado.	• Últimas 24 horas • Últimos 7 días • Último mes

Campo	Descripción	Valores
		Último año
Acción	Filtra por la acción que Control de Acceso a Endpoints aplicó a la conexión.	- Permitido - Bloqueado
Riesgo detectado	Filtra por el estado del equipo origen causante del registro de la conexión	- No está administrado/No está disponible - Está administrado por otra cuenta - Protección no activada - Riesgo Medio - Riesgo Alto - Riesgo Crítico
Protocolo	Filtra por el protocolo de la conexión registrada.	Cadena de caracteres

Tabla 13.58: Campos de filtrado para el listado Conexiones identificadas por el Control de Acceso a Endpoints

Ventana Detalle de la conexión

En el listado Conexiones identificadas por el Control de Acceso a Endpoints, haz clic en una de las líneas para abrir la ventana de detalle de la conexión, dividida en tres secciones:

- **Alertas de equipo (1):** muestra los datos de la alerta generada por el equipo que recibe la conexión.
- **Equipo afectado (2):** nombre, dirección IP y tipo del equipo destinatario de la conexión.
- **Detalles de la conexión (3):** resumen de los puertos y direcciones IP locales y remotas involucradas en la conexión, y número de veces que se detectó la conexión.

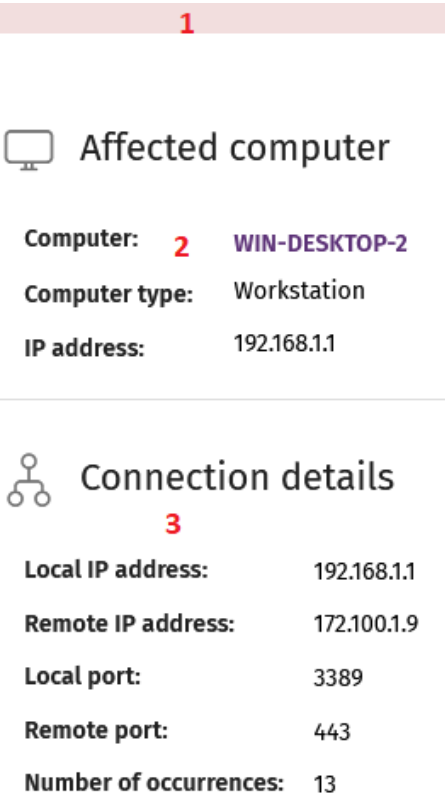


Figura 13.28: Distribución de la información de los detalles de la conexión

Alertas de equipo (1)

Campo	Descripción	Valores
Fecha de detección	Fecha de detección de la conexión.	Fecha
Riesgo detectado	Estado del equipo origen causante del registro de la conexión	• No está administrado/No está disponible • Está administrado por otra cuenta • Protección no activada • Nivel de riesgo mayor o igual a: ◦ Medio ◦ Alto ◦ Crítico

Campo	Descripción	Valores
Protocolo	Protocolo/puerto de la conexión registrada.	Numérico
Acción	Acción que Control de Acceso a Endpoints aplicó a la conexión.	• Permitido • Bloqueado
Recomendaciones	Recomendaciones para el administrador de la seguridad del equipo destinatario.	Cadena de caracteres

Tabla 13.59: Detalles de la alerta de equipo

Equipo afectado (2)

Campo	Descripción	Valores
Equipo	Nombre del equipo destinatario de la conexión. Si el usuario de la consola tiene visibilidad sobre el equipo, al hacer clic en él se accede a la ventana de detalles del equipo. Consulta Información de equipo en la página 218	Cadena de caracteres
Tipo de equipo	Clase de dispositivo.	• Estación • Portátil • Servidor
Dirección IP	Dirección IP principal del equipo destinatario de la conexión.	Numérico

Tabla 13.60: Detalles del equipo destinatario

Detalles de la conexión (3)

Campo	Descripción	Valores
Dirección IP local	Dirección IP del equipo destinatario en la que se registró la conexión.	Numérico
Dirección IP remota	Dirección IP del equipo origen de la conexión.	Numérico

Campo	Descripción	Valores
Puerto local	Puerto del equipo destinatario en el que se registró la conexión.	Numérico
Puerto remoto	Puerto utilizado por el equipo origen para establecer la conexión.	Numérico
Número de repeticiones	Número de veces que se detectó la conexión en una hora.	Numérico

Tabla 13.61: Detalles de la conexión

Capítulo 14

Cytomic Encryption (Cifrado de dispositivos)

Cytomic Encryption es un módulo integrado en la plataforma Cytomic que cifra el contenido de los medios de almacenamiento conectados a los equipos administrados por Advanced EDR. Su objetivo es minimizar la exposición de la información de las empresas, tanto en casos de pérdida o robo de los equipos como al descartar sistemas de almacenamiento en uso sin borrar previamente su contenido.

Cytomic Encryption es compatible con ciertas versiones de sistemas operativos Windows 7 en adelante y con determinadas versiones de macOS (consulta [Versiones compatibles del sistema operativo Windows](#)) y permite controlar el estado del cifrado de los equipos de la red, gestionando de forma centralizada sus claves de recuperación. Además, aprovecha recursos hardware como los chips TPM, ofreciendo una gran flexibilidad a la hora de elegir el sistema de autenticación más adecuado en cada caso.

Para obtener información adicional sobre los distintos apartados del módulo Cytomic Encryption consulta las referencias siguientes:



Crear y gestionar configuraciones en la página **258**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.

Acceso, control y supervisión de la consola de administración en la página **59**: gestión de cuentas de usuario y asignación de permisos.

Gestión de listados en la página **47**: información sobre como gestionar listados.

Contenido del capítulo

Introducción a los conceptos de cifrado **482**

Visión general del servicio de Cytomic Encryption	485
Características generales de Cytomic Encryption	486
Requisitos mínimos de Cytomic Encryption	487
Gestión de equipos según su estado de cifrado previo	488
Proceso de cifrado y descifrado en Windows	488
Comportamiento de Cytomic Encryption ante errores	494
Proceso para obtener la clave de recuperación	494
Paneles / widgets del módulo Cytomic Encryption	499
Listados en Cytomic Encryption	506
Configuración del cifrado	513
Filtros disponibles	515

Introducción a los conceptos de cifrado

Cytomic Encryption utiliza las herramientas integradas en los sistemas operativos Windows y macOS para gestionar el cifrado en los equipos de la red gestionados con Advanced EDR.

Para una correcta comprensión de los procesos involucrados en el cifrado y descifrado de la información, es necesario presentar algunos conceptos relativos a la tecnología de cifrado utilizada.

TPM

TPM (Trusted Platform Module, módulo de plataforma segura) es un chip que se incluye en algunas placas base de equipos de sobremesa, portátiles y servidores. Su principal objetivo es proteger la información sensible de los usuarios, almacenando claves y otra información utilizada en el proceso de autenticación.

Además, el TPM es el responsable de detectar los cambios en la cadena de inicio del equipo, impidiendo por ejemplo el acceso a un disco duro desde un equipo distinto al que se utilizó para su cifrado.

La versión mínima de TPM soportada por Cytomic Encryption es la 1.2. y Cytomic recomienda su uso en combinación con otros sistemas de autenticación soportados. En algunos escenarios es posible que el TPM esté deshabilitado en la BIOS del equipo y sea necesario su activación manual.

Tipos de autenticación soportados

Contraseña de inicio de sesión

En el sistema operativo macOS no se dispone de métodos de autenticación independientes, por lo que se utiliza siempre la contraseña de inicio de sesión, compatible con todas las versiones de macOS soportadas por Cytomic Encryption.

PIN

El PIN (Personal Identification Number, número de identificación personal) es una secuencia de números que actúa como contraseña simple y es requerida en el inicio de un equipo que tenga un volumen cifrado. Sin el PIN la secuencia de arranque no se completa y el acceso al equipo no es posible. Compatible con todas las versiones de Windows soportadas.

PIN extendido

Si el hardware es compatible, Cytomic Encryption utilizará un PIN extendido o PIN mejorado compuesto por letras y números para incrementar la complejidad de la contraseña.

Debido a que el PIN Extendido se pide en el proceso de inicio del equipo previo a la carga del sistema operativo, las limitaciones de la BIOS pueden restringir la entrada de teclado a la tabla ASCII de 7 bits.

Adicionalmente, los teclados que utilizan una distribución distinta a la dispuesta en el mapa de caracteres EN-US, tales como teclados QWERTZ o AZERTY, pueden provocar el fallo en la introducción del PIN Extendido. Por esta razón, Cytomic Encryption controla que los caracteres introducidos por el usuario pertenecen al mapa EN-US antes de establecer el PIN Extendido en el proceso de cifrado del equipo.

Compatible con todas las versiones de Windows soportadas.

Passphrase

Una passphrase es una contraseña de mayor longitud formada por caracteres alfanuméricos equivalente al PIN Extendido.

Cytomic Encryption establece las siguientes prioridades al solicitar un tipo u otro de contraseña al usuario:

- Passphrase: siempre que el equipo tenga un TPM instalado.
- PIN extendido: si el sistema operativo y el hardware del equipo lo soportan.
- PIN: si todas las demás opciones no son válidas.

Compatible con equipos Windows 8 y posteriores sin TPM.

Llave USB

Permite almacenar la clave de acceso en un dispositivo USB formateado con NTFS, FAT o FAT32. De esta forma, no se requiere introducir ninguna contraseña en el proceso de inicio del equipo, aunque es necesario que el dispositivo USB que almacena la contraseña esté conectado en el equipo.

Compatible con equipos Windows 7 sin TPM.



Algunos PCs antiguos no son capaces de acceder a las unidades USB en el proceso de arranque, comprueba que los equipos de tu organización tienen acceso a las unidades USB desde la BIOS.

Clave de recuperación

Cuando se detecta una situación anómala en un equipo protegido con Cytomic Encryption o en el caso de que hayamos olvidado la contraseña de desbloqueo, el sistema pedirá una clave de recuperación. Esta clave se gestiona desde la consola de administración y debe ser introducida para completar el inicio del equipo.



Cytomic Encryption únicamente almacena las claves de recuperación de los equipos que gestiona. La consola de administración no mostrará las claves de recuperación de los equipos cifrados por el usuario y no gestionados por Cytomic.

La clave de recuperación se solicita en los escenarios mostrados a continuación:

- Cuando se introduce errónea y repetidamente el PIN o la passphrase en el proceso de inicio del equipo.
- Cuando un equipo protegido con TPM detecta un cambio en la secuencia de arranque (disco duro protegido por TPM y conectado en otro equipo).
- Cuando se ha cambiado la placa base del equipo y por lo tanto el TPM.
- Al desactivar, deshabilitar o borrar el contenido del TPM.
- Al cambiar los valores de configuración de arranque del equipo.
- Al cambiar el proceso de arranque del equipo:
 - Actualización de la BIOS.
 - Actualización del firmware.
 - Actualización de la UEFI.
 - Modificación del sector de arranque.
 - Modificación del registro maestro de arranque (master boot record).
 - Modificación del gestor de arranque (boot manager).
 - Cambio del firmware implementado en ciertos componentes que forman parte del proceso de arranque del equipo (tarjetas de vídeo, controladores de discos, etc.) conocido como Option ROM.
 - Cambio de otros componentes que intervienen en las fases iniciales del arranque del sistema.

BitLocker

Es el software instalado en algunas versiones de los equipos Windows 7 y superiores encargado de gestionar el cifrado y descifrado de los datos almacenados en los volúmenes del equipo. Cytomic Encryption instala BitLocker automáticamente en aquellas versiones de servidor que no lo incluyan pero sean compatibles.

FileVault

Es el software integrado en el sistema operativo macOS, que permite cifrar de forma automática todos los archivos que se almacenan en el disco duro o memoria SSD del ordenador.

Partición de sistema

En el sistema operativo Windows, es una zona pequeña del disco duro que permanece sin cifrar y que es necesaria para que el equipo complete correctamente el proceso de inicio. Cytomic Encryption crea automáticamente esta partición de sistema si no existiera previamente.

Algoritmo de cifrado

El algoritmo de cifrado para Windows elegido en Cytomic Encryption es el AES-256 aunque los equipos con volúmenes cifrados por el usuario que utilicen otro algoritmo de cifrado también son compatibles.

En macOS, el único algoritmo disponible es el AES-XTS.

Visión general del servicio de Cytomic Encryption

El proceso general de cifrado abarca varios apartados que el administrador deberá conocer para gestionar correctamente los recursos de la red susceptibles de contener información delicada o comprometedora en caso de robo, pérdida o descarte del volumen sin borrar:

- **Cumplimiento de los requisitos mínimos de hardware y software:** consulta [Requisitos mínimos de Cytomic Encryption](#) para ver las limitaciones y particularidades del cifrado en cada plataforma compatible.
- **Estado previo del cifrado en el equipo del usuario:** dependiendo de si BitLocker o FileVault estaba siendo usado previamente en el equipo del usuario, el proceso de integración en Cytomic Encryption puede variar ligeramente.
- **Asignación de configuraciones de cifrado:** establece el estado (cifrado o no cifrado) de los equipos de la red y el o los métodos de autenticación.
- **Interacción del proceso de cifrado con el usuario del equipo:** el proceso de cifrado inicial requiere de la colaboración del usuario para completarse de forma correcta. Consulta [Cifrado de volúmenes sin cifrado previo](#) para más información.
- **Visualización del estado de cifrado del parque informático:** mediante los widgets / paneles incluidos en el menú superior **Estado**, panel lateral **Cytomic Encryption**. Consulta [Paneles / widgets del módulo Cytomic Encryption](#) para una descripción completa de los widgets incluidos en Cytomic Encryption. También se soportan filtros para localizar equipos en los listados según su estado. Consulta [Filtros disponibles](#) para más información.
- **Restricción de los permisos de cifrado a los administradores de la seguridad:** el sistema de roles mostrado en [Descripción de los permisos implementados](#) en la página **70** abarca la funcionalidad de cifrado y visualización del estado de los equipos de la red.
- **Obtención de la clave de recuperación:** en los casos en que el usuario haya olvidado la contraseña, el PIN / passphrase o el TPM haya detectado una situación anómala el administrador de la red podrá obtener de forma centralizada la clave de recuperación y enviársela al usuario. Consulta [Proceso para obtener la clave de recuperación](#) para más información.

Características generales de Cytomic Encryption

Tipos de autenticación soportados

Dependiendo de la existencia o no de TPM y de la versión del sistema operativo, Cytomic Encryption admite distintas combinaciones de métodos de autenticación, mostrados a continuación de forma ordenada según la recomendación de Cytomic:

Windows

- **TPM + PIN:** compatible con todas las versiones de Windows soportadas, requiere el chip TPM habilitado en la BIOS y el establecimiento de un PIN.
- **Solo TPM:** compatible con todas las versiones de Windows soportadas, requiere el chip TPM habilitado en la BIOS excepto en Windows 10, donde se habilita de forma automática.
- **Dispositivo USB:** requiere una llave USB y un equipo que pueda acceder a dispositivos USBs en el arranque. Necesario en equipos Windows 7 sin TPM.
- **Passphrase:** solo disponible en equipos Windows 8 y posteriores sin TPM.

macOS

No se utiliza un método de autenticación independiente sino la contraseña de inicio de sesión, compatible con todas las versiones del sistema operativo soportadas por Cytomic Encryption. Consulta [Versiones compatibles del sistema operativo Windows](#)

Cytomic Encryption utiliza por defecto un método de autenticación que incluye el uso de TPM si se encuentra disponible. Si se elige una combinación de autenticación no incluida en el listado anterior, la consola de administración mostrará una ventana de advertencia indicando que el equipo permanecerá sin cifrar.

Tipo de dispositivos de almacenamiento compatibles

Cytomic Encryption cifra todos los dispositivos internos de almacenamiento masivo:

Windows y macOS

- Unidades de almacenamiento fijas del equipo (sistema y datos).

Windows

- Discos duros virtuales (VHD) pero únicamente el espacio utilizado independientemente de lo indicado en la consola de administración.
- Discos duros extraíbles.
- Llaves USB.

No se cifrarán:

- Discos duros internos dinámicos.
- Particiones de tamaño muy reducido.

- Otros dispositivos de almacenamiento externo.

Requisitos mínimos de Cytomic Encryption

Los requisitos mínimos se dividen en:

- Versiones y familias compatibles del sistema operativo Windows.
- Versiones compatibles del sistema operativo macOS.
- Requisitos de hardware para equipos Windows.



A partir de la fecha 30/09/2024 no será posible añadir a la consola de administración nuevos equipos que utilicen los siguientes sistemas operativos: Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008 (no afecta a Windows Server 2008 R2). Los equipos instalados en una fecha anterior seguirán protegidos. Consulta <https://www.watchguard.com/wgrd-trust-center/end-of-life-policy>.

Versiones compatibles del sistema operativo Windows

- Windows 7 (Ultimate, Enterprise)
- Windows 8/8.1 (Pro, Enterprise)
- Windows 10 (Pro, Enterprise, Education)
- Windows 11 (Pro, Enterprise, Education)
- Windows Server 2008 R2, Windows Server 2012 y superiores (incluyendo a las ediciones Server Core)

Versiones compatibles del sistema operativo macOS

- macOS 10.15 Catalina
- macOS 11 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma

Requisitos de hardware para equipos Windows

- TPM 1.2 y superiores si se utiliza este método de autenticación.
- Llave USB y equipo compatible con la lectura de dispositivos USB desde la BIOS en sistemas Windows 7 sin TPM.



En el caso del sistema operativo macOS, no hay requisitos de hardware específicos.

Gestión de equipos según su estado de cifrado previo

Administración de equipos por Cytomic Encryption

Para que un equipo de la red se considere gestionado por Cytomic Encryption es necesario que se cumplan las condiciones siguientes:

- El equipo cumple con los requisitos mínimos descritos en [Requisitos mínimos de Cytomic Encryption](#)
- El equipo ha recibido al menos una vez una configuración desde la consola de administración que establezca el cifrado de los volúmenes y éste se ha completado con éxito.

Los equipos que previamente tenían cifrado alguno de sus volúmenes y no han recibido una configuración que cifre sus unidades no serán gestionados por Cytomic Encryption y por lo tanto el administrador no tendrá acceso a la clave de recuperación ni al estado del equipo.

Por el contrario, los equipos que han recibido una configuración que cifre sus unidades, independientemente de su estado anterior (cifrado o no) serán administrados por Cytomic Encryption.

Desinstalación del agente Advanced EDR

Independientemente de si el equipo estaba siendo administrado por Cytomic Encryption o no, si los dispositivos de almacenamiento estaban cifrados, al desinstalar Advanced EDR se dejarán tal y como están. No obstante, se perderá el acceso centralizado a la clave de recuperación.

Si posteriormente el equipo se reintegra en Advanced EDR se mostrará la última clave de recuperación almacenada.

Proceso de cifrado y descifrado en Windows

Cifrado de volúmenes sin cifrado previo

El proceso de cifrado se inicia cuando el agente Advanced EDR instalado en el equipo de usuario se descarga una configuración de tipo Cifrado. En ese momento se le mostrará al usuario una ventana

informativa que le guiará en todo el proceso.

El número de pasos total varía dependiendo del tipo de autenticación elegida por el administrador y del estado previo del equipo. Si cualquiera de los pasos termina en un error, el agente lo reportará a la consola de administración y el proceso se detendrá.



No se permitirá el cifrado de equipos desde una sesión de escritorio remoto ya que es necesario el reinicio del equipo y la introducción de una clave antes de la carga del sistema operativo, operaciones que no son posibles con un sistema de escritorio remoto estándar. El proceso de cifrado se iniciará cuando la instalación o desinstalación en curso de parches gestionados por el módulo Cytomic Encryption haya finalizado.

A continuación se muestra el proceso completo de cifrado y se indica si se muestra feedback al usuario del equipo y si es necesario el reinicio de la máquina:

Paso	Proceso en el equipo	Interacción con el usuario
1	El agente recibe una configuración del módulo de cifrado que pide cifrar el contenido de los dispositivos de almacenamiento instalados.	Ninguno
2	Si el equipo es de tipo servidor y no tiene las herramientas de BitLocker instaladas éstas se descargan y se instalan.	Se muestra una ventana pidiendo permiso para reiniciar el equipo y completar la instalación de BitLocker o posponer. Si se elige posponer el proceso se detiene y se volverá a preguntar en el siguiente inicio de sesión. Requiere reinicio.
3	Si el equipo no estaba cifrado previamente se crea la partición de sistema.	Se muestra una ventana pidiendo permiso para reiniciar el equipo y completar la creación de la partición de sistema o posponer. Si se elige posponer el proceso se detiene y se volverá a preguntar en el siguiente inicio de sesión. Requiere reinicio.
4	Si existe una directiva de grupo definida previamente por el administrador de la red	Si el administrador no ha definido directivas de grupo globales que entren

Paso	Proceso en el equipo	Interacción con el usuario
	que colisione con las establecidas por Cytomic Encryption se mostrará un error y el proceso terminará. Las directivas de grupo configuradas por Cytomic Encryption son: En el Editor de Directivas de grupo local, navega la ruta siguiente: Directiva equipo local > Configuración del equipo > Plantillas administrativas > Componentes de Windows > Cifrado de unidad BitLocker > Unidades del sistema operativo. Marca a Sin definir las políticas de grupo indicadas para evitar este error.	en colisión con las directivas locales definidas por Cytomic Encryption no se mostrará ningún mensaje.
5	Preparación del TPM si existe y si el método de autenticación elegido involucra a éste componente y no estaba habilitado previamente desde la BIOS.	Requiere confirmar un reinicio para que el usuario pueda entrar en la BIOS del equipo y habilitar el TPM. En sistemas operativos Windows 10 no es necesario modificar la BIOS pero se requiere el reinicio igualmente. El reinicio del paso 3, en caso de haberlo, se juntará con el actual.
6	Preparación del dispositivo USB si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir un dispositivo USB para almacenar la contraseña de inicio de equipo.
7	Almacenamiento del PIN si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir el PIN. Si se utilizan caracteres alfanuméricos y el hardware no es compatible se mostrará el error “-2144272180”. En este caso introduce un PIN numérico.
8	Almacenamiento de la passphrase si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir la passphrase.

Paso	Proceso en el equipo	Interacción con el usuario
9	Se genera la clave de recuperación y se envía a la nube de Cytomic. Una vez que la clave se ha recibido, el proceso continúa en el equipo del usuario.	Ninguno.
10	Comprobación de que el hardware del equipo es compatible con la tecnología de cifrado, e inicio del cifrado.	Se requiere confirmar un reinicio para hacer el chequeo del hardware utilizado en los distintos métodos de autenticación elegidos. Requiere reinicio.
11	Cifrado de volúmenes.	Comienza el proceso de cifrado en segundo plano sin ocasionar molestias al usuario del equipo. La duración depende del volumen de datos a cifrar. Una duración media del tiempo de cifrado se sitúa en torno a las 2-3 horas. El usuario puede utilizar y apagar el equipo normalmente. El proceso de cifrado se reanudará en el siguiente encendido del equipo.
12	El proceso de cifrado se completa de forma silenciosa y a partir de ese momento el proceso de cifrado y descifrado es transparente para el usuario.	Dependiendo del método de autenticación elegido el usuario puede necesitar introducir una llave USB, un PIN, una passphrase o nada en el inicio del equipo.

Tabla 14.1: Pasos para el cifrado de volúmenes sin cifrar previamente

Cifrado de volúmenes ya cifrados previamente

En el caso de que algún volumen del equipo ya estuviera cifrado, Cytomic Encryption modifica algunos parámetros para habilitar su gestión centralizada. A continuación se indican las acciones realizadas:

- Si el método de autenticación elegido por el usuario no coincide con el especificado en la configuración, éste se cambiará, solicitándole al usuario las claves o recursos hardware necesarios. Si no es posible asignar un método de autenticación compatible con la plataforma y con la configuración especificada por el administrador, el equipo quedará cifrado por el usuario y no será

gestionado por Cytomic Encryption.

- Si el algoritmo de cifrado utilizado no está soportado (distinto de AES-256) se dejará sin cambios para evitar el descifrado y cifrado completo el volumen pero el equipo será administrado por Cytomic Encryption.
- Si existen tanto volúmenes cifrados como sin cifrar, se cifrarán todos los volúmenes aplicando el mismo método de autenticación.
- Si el método de autenticación elegido previamente involucra la introducción de una contraseña y es compatible con los métodos soportados por Cytomic Encryption, se volverá a pedir la contraseña al usuario para unificar el método de autenticación en todos los volúmenes.
- Si el usuario eligió una configuración de cifrado distinta a la establecida por el administrador (cifrado únicamente de los sectores ocupados frente al cifrado completo del volumen) el volumen se dejará sin cambios para minimizar el proceso de cifrado.
- Al final de todo el proceso el dispositivo pasa a ser gestionado por Cytomic Encryption y se genera la clave de recuperación para su posterior envío a la nube de Cytomic.

Cifrado de nuevos volúmenes

Si una vez completado el proceso de cifrado el usuario del equipo crea un nuevo volumen, Cytomic Encryption lo cifrará inmediatamente respetando la configuración asignada por el administrador de la red.

Descifrado de volúmenes

Se distinguen tres casos:

- Si Cytomic Encryption cifra un equipo, a partir de ese momento el administrador podrá asignar una configuración para descifrarlo.
- Si un equipo ya estaba cifrado por el usuario antes de la instalación de Cytomic Encryption y se le asigna una configuración de cifrado se considerará cifrado por Cytomic Encryption y se podrá descifrar asignando una configuración desde la consola de administración.
- Si un equipo ya estaba cifrado por el usuario antes de la instalación de Cytomic Encryption y nunca se le ha asignado una configuración de cifrado no se considerará cifrado por Cytomic Encryption y no se podrá descifrar asignando una configuración desde la consola de administración.

Modificación local de la configuración de BitLocker

El usuario del equipo tiene acceso a la configuración local de BitLocker desde las herramientas de Windows pero los cambios que efectúe serán revertidos de forma inmediata a la configuración establecida por el administrador de la red a través de la consola de administración. El comportamiento de Cytomic Encryption ante un cambio de esta naturaleza se muestra a continuación:

- **Desactivar el desbloqueo automático de una unidad:** se revierte a la configuración de bloqueo automático.
- **Quitar la contraseña de un volumen:** se pedirá la nueva contraseña.

- **Descifrar un volumen previamente cifrado por Cytomic Encryption:** se cifrará automáticamente el volumen.
- **Cifrar una unidad descifrada:** si la configuración de Cytomic Encryption implica descifrar las unidades la acción del usuario prevalece y no se descifrá la unidad.

Cifrado y descifrado de discos duros externos y llaves USB

Como el usuario del equipo puede conectar y desconectar medios de almacenamiento externos en cualquier momento, el comportamiento de Cytomic Encryption para este tipo de dispositivos difiere en los puntos siguientes:

- Si el equipo del usuario o servidor no dispone de BitLocker, el agente no descargará los paquetes necesarios, y por lo tanto el dispositivo no se cifrará ni mostrará ningún aviso al usuario.
- Si el equipo dispone de BitLocker, solo se mostrará un mensaje emergente al usuario ofreciendo la posibilidad de cifrarlo en las siguientes situaciones:
 - Cada vez que conecte un dispositivo de almacenamiento USB sin cifrar.
 - Si hay un dispositivo conectado en el equipo y sin cifrar cuando el administrador activa la configuración desde la consola web.
- El mensaje de cifrado se mostrará al usuario durante 5 minutos, transcurridos los cuales dejará de ser visible. Tanto si el usuario acepta el cifrado como si no, el dispositivo podrá ser utilizado de forma normal, a no ser que se haya establecido previamente una configuración que impida el uso de estos dispositivos sin cifrar. Consulta [Escritura en unidades de almacenamiento extraíbles](#) en la página 337 para más información.
- Cifrar en un dispositivo USB no requiere crear una partición de sistema.
- Si el dispositivo de almacenamiento externo ya está cifrado por otra solución distinta de Cytomic Encryption, al conectarlo al equipo no se mostrará el mensaje de cifrado y se podrá usar con normalidad. Cytomic Encryption no enviará las claves de recuperación a la consola web.
- No se permitirá la escritura en dispositivos USB si está establecida la configuración **Escritura en unidades de almacenamiento extraíbles** de Cytomic Data Watch y el dispositivo no ha sido cifrado con BitLocker o con Cytomic Encryption. Consulta [Escritura en unidades de almacenamiento extraíbles](#) en la página 337 para más información.
- Para descifrar un dispositivo cifrado por Cytomic Encryption el usuario puede utilizar BitLocker de forma manual.
- Solo se cifra el espacio utilizado.
- Todas las particiones del dispositivo se cifran con la misma clave.



Retirar un dispositivo USB cuando el proceso de cifrado no se ha completado puede corromper todo su contenido.

Comportamiento de Cytomic Encryption ante errores

- **Errores en el test de hardware:** el test de hardware se ejecuta cada vez que se inicia el equipo hasta que sea superado, momento en el que el equipo comenzará el cifrado automáticamente.
- **Error al crear la partición de sistema:** muchos errores al crear la partición de sistema son subsanables por el propio usuario del equipo (por ejemplo la falta de espacio). Periódicamente Cytomic Encryption intentará crear la partición de forma automática.
- **Negativa a activar el chip TPM por parte del usuario:** el equipo mostrará un mensaje en cada proceso de inicio pidiéndole al usuario la activación del chip TPM. Hasta que esta condición no sea resuelta el proceso de cifrado no comenzará.

Proceso para obtener la clave de recuperación

La introducción de la clave de recuperación es necesaria en los siguientes escenarios:

- **Windows:** cuando el usuario haya perdido el PIN / passphrase / dispositivo USB, o el chip TPM haya detectado un cambio en la cadena de inicio del equipo.
- **macOS:** cuando el usuario haya perdido la contraseña de inicio de sesión o se detecte un cambio en la cadena de inicio del equipo.

Cytomic Encryption almacena todas las claves de recuperación de los equipos de la red cuyo cifrado gestiona, por lo que el administrador puede obtener la clave desde la consola web. Para ello, el administrador necesita los siguientes datos según el sistema operativo instalado en el equipo:

- **Windows:** es necesario el identificador de volumen cifrado (*Recovery Key ID*), que es una cadena de 40 dígitos asociado a cada volumen de datos cifrado.
- **macOS:** es necesario el identificador de la clave de recuperación asociada al equipo. Este identificador es único para todo el equipo e independiente del número de unidades de almacenamiento de que disponga.

Permisos requeridos

Permiso	Tipo de acceso
Acceder a las claves de recuperación de unidades	Buscar y obtener la clave de recuperación

Permiso	Tipo de acceso
cifradas	de una unidad cifrada.

Tabla 14.2: Permisos requeridos para obtener la clave de recuperación

Obtener el identificador de volumen cifrado (Windows)

Cuando el usuario no recuerda la contraseña de inicio del equipo o del USB cifrado al que desea acceder, el sistema le mostrará una ventana de aviso:

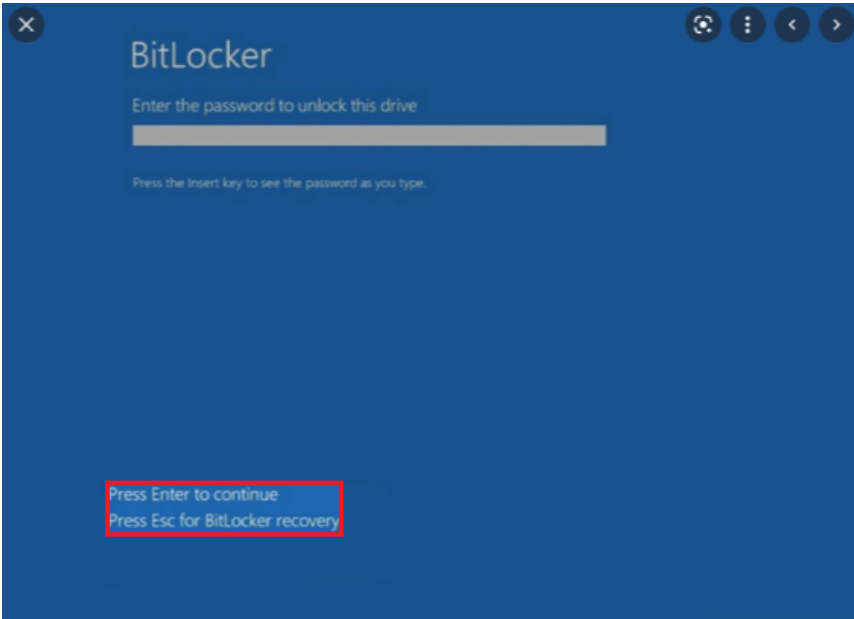


Figura 14.1: Acceso al identificador de volumen cifrado

Figura 14.2:

Al presionar la tecla **Esc**, el usuario accede a la ventana donde se muestra el identificador de volumen cifrado:



Figura 14.3: Identificador de volumen cifrado

Cuando se trata de particiones de disco cifradas, la ventana que se muestra al usuario cuando intenta acceder a la partición es diferente, y en ella solo están visibles los primeros 8 dígitos del identificador de volumen cifrado:

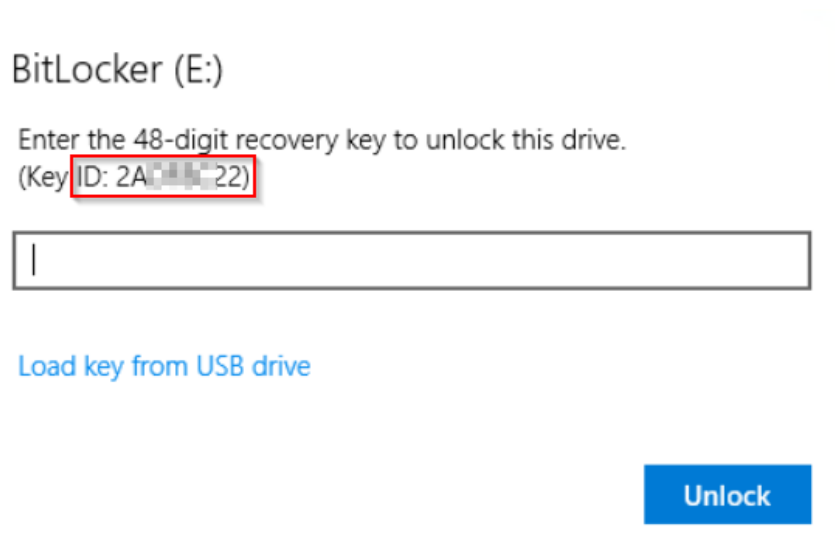


Figura 14.4: Identificador de partición de disco cifrada



*Para más información sobre cifrado de volúmenes en los equipos, consulta el apartado **Proceso de cifrado y descifrado en Windows**.*

Obtener el identificador de la clave de recuperación asociada al equipo (macOS)

Al intentar acceder al equipo cifrado, en la pantalla de login se muestra un mensaje que contiene el identificador de la clave de recuperación asociada al equipo, y recomienda contactar con el administrador de la configuración del cifrado.

Obtener la clave de recuperación

- En el menú superior **Equipos** haz clic en el equipo cuya clave quieres recuperar.
- En la pestaña **Detalles**, sección **Protección de datos**, haz clic en el enlace **Obtener la clave de recuperación** (en el caso de cifrado de unidades de almacenamiento extraíbles, utiliza el enlace **Ver dispositivos cifrados en este equipo**).

Se abrirá una ventana con los identificadores de volumen cifrados almacenados por Cytomic.

- Haz clic en un identificador. Se abrirá una ventana con la clave de recuperación.
- Copia la clave y envíasela al usuario.

Buscar la clave de recuperación

Si el usuario tiene visibilidad sobre todos los equipos de la cuenta, en los resultados de la búsqueda también se incluirán identificadores de volumen correspondientes a equipos que hayan sido eliminados.

Buscar la clave de recuperación desde el widget Equipos cifrados

- En el menú superior **Estado**, haz clic en panel lateral **Full Encryption**.
- En el widget **Equipos cifrados**, haz clic en el enlace **Búsqueda de clave de recuperación**.

ENCRYPTED COMPUTERS

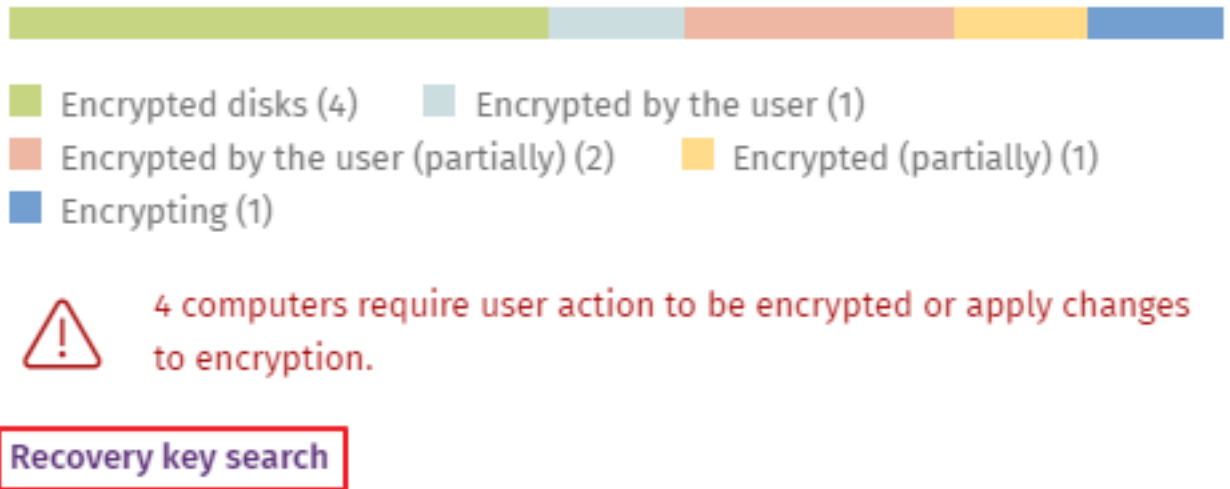


Figura 14.5: Buscar la clave de recuperación

- Escribe el identificador de volumen cifrado proporcionado por el usuario. Se mostrará la clave de recuperación que el usuario podrá utilizar para acceder al equipo.
- En el caso de los identificadores de volumen cifrado para particiones de disco, escribe los 8 primeros dígitos. Se mostrará la clave de recuperación que el usuario podrá utilizar para acceder a la partición de disco bloqueada.



Puede darse el caso de que los 8 dígitos iniciales sean los mismos para más de una clave de recuperación, en cuyo caso se mostrarán todas ellas en los resultados de la búsqueda.

Buscar la clave de recuperación desde el detalle del equipo

- En el menú superior **Equipos** haz clic en el equipo cuyas claves quieres recuperar.
- En la pestaña **Detalles**, sección **Protección de datos**, haz clic en el enlace **Obtener la clave de recuperación** (en el caso de cifrado de unidades de almacenamiento extraíbles, utiliza el enlace **Ver dispositivos cifrados en este equipo**).

Se abrirá una ventana con los identificadores de volumen cifrados almacenados por Cytomic.

- Haz clic en el enlace **Buscar otra clave** e introduce el identificador de volumen cifrado.

Paneles / widgets del módulo Cytomic Encryption

Acceso al panel de control

Para acceder haz clic en el menú superior **Estado**, panel lateral Cytomic Encryption.

Permisos requeridos

No se necesitan permisos adicionales para acceder a los widgets asociados a **Cytomic Encryption**.

Estado del cifrado

Muestra el total de equipos compatibles con Cytomic Encryption así como su estado con respecto a la tecnología de cifrado.

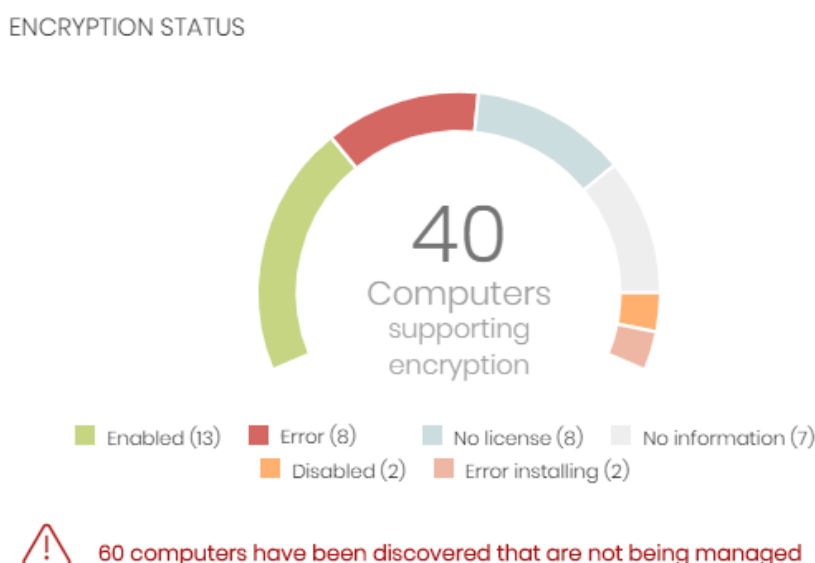


Figura 14.6: Panel de Estado del cifrado

Significado de las series

Serie	Descripción
Activado	Equipos con Cytomic Encryption instalado, con una configuración que indica cifrar el equipo y sin reporte de errores de cifrado ni de instalación.
Desactivado	Equipos con Cytomic Encryption instalado, con una configuración que indica no cifrar el equipo y sin reporte de errores de cifrado ni de instalación.
Error	No se ha podido realizar la acción que el administrador ha indicado en la configuración de cifrado o descifrado.
Error instalando	No se ha podido descargar e instalar BitLocker si fue necesario.

Serie	Descripción
Sin licencia	Equipo compatible con Cytomic Encryption pero sin licencia de Advanced EDR asignada.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con un agente sin actualizar.

Tabla 14.3: Descripción de la serie Estado del cifrado

Filtros preestablecidos desde el panel

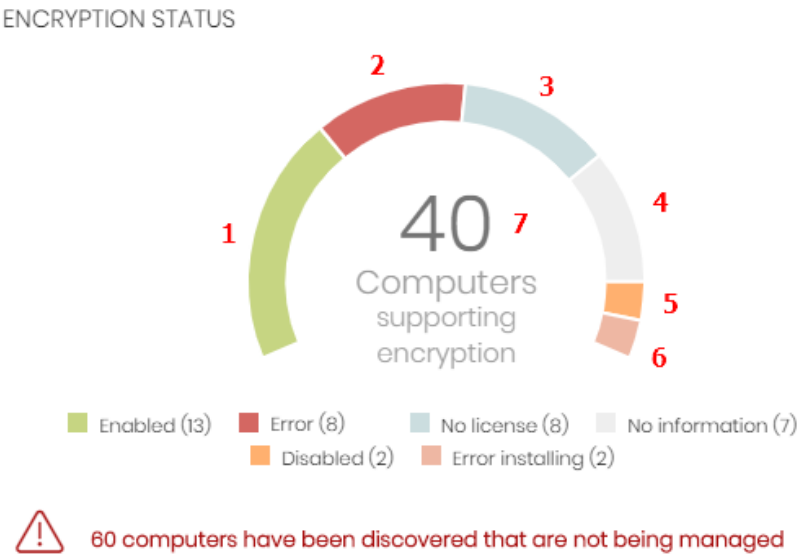


Figura 14.7: Zonas activas del panel Estado del cifrado

Al hacer clic en las zonas indicadas en **Zonas activas del panel Estado del cifrado** se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado del cifrado = Activado.
(2)	Estado del cifrado = Error.
(3)	Estado del cifrado = Sin licencia. El equipo no tiene asignada licencia de Advanced EDR.
(4)	Estado del cifrado = Sin información.
(5)	Estado del cifrado = Desactivado.

Zona activa	Filtro
(6)	Estado del cifrado = Error instalando.
(7)	Sin filtros.

Tabla 14.4: Definición de filtros del listado Estado del cifrado

Equipos compatibles con cifrado

Muestra los equipos compatibles y no compatibles con la tecnología de filtrado agrupados en series según su tipo.

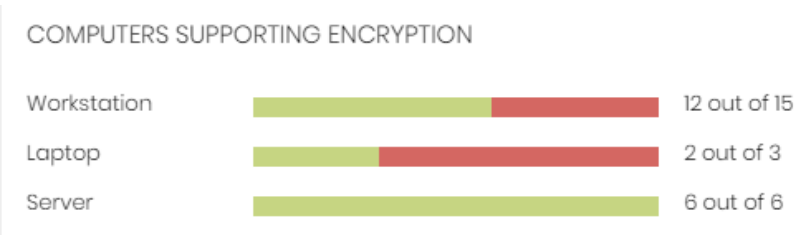


Figura 14.8: Panel de Equipos compatibles con cifrado

Significado de las series

Serie	Descripción
Estación - verde	Dispositivos de tipo estación compatibles con cifrado.
Estación - rojo	Dispositivos de tipo estación no compatibles con cifrado.
Portátil - verde	Dispositivos de tipo portátil compatibles con cifrado.
Portátil - rojo	Dispositivos de tipo portátil no compatibles con cifrado.
Servidor - verde	Dispositivos de tipo servidor compatibles con cifrado.
Servidor - rojo	Dispositivos de tipo servidor no compatibles con cifrado.

Tabla 14.5: Descripción de la serie Equipos compatibles con cifrado

Filtros preestablecidos desde el panel

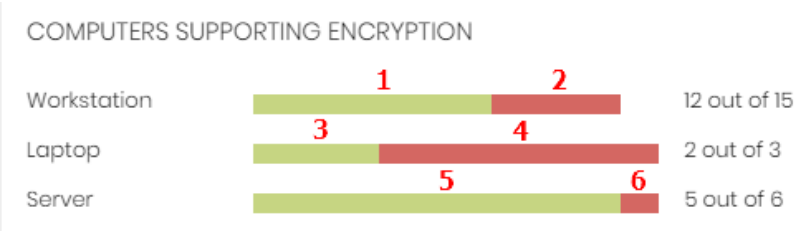


Figura 14.9: Zonas activas del panel Estado del cifrado

Al hacer clic en las zonas indicadas en **Zonas activas del panel Estado del cifrado** se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Tipo de equipo = Estación.
(2)	Listado de equipos con filtro No compatibles con cifrado.
(3)	Tipo de equipo = Portátil.
(4)	Listado de equipos con filtro No compatibles con cifrado.
(5)	Tipo de equipo = Servidor.
(6)	Listado de equipos con filtro No compatibles con cifrado.

Tabla 14.6: Definición de filtros del listado Estado del cifrado

Equipos cifrados

Muestra el estado del proceso de cifrado en los equipos de la red compatibles con Cytomic Encryption.



Para saber más sobre el proceso de búsqueda de claves de recuperación, consulta el apartado **Proceso para obtener la clave de recuperación.**

ENCRYPTED COMPUTERS



■ Encrypted disks (9) ■ Encrypted by the user (1)
■ Encrypted by the user (partially) (4) ■ Encrypted (partially) (4)
■ Encrypting (1) ■ Unencrypted disks (1)



9 computers require user action to be encrypted or apply changes to encryption.

[Recovery key search](#)

Figura 14.10: Panel Equipos cifrados

Significado de las series

Serie	Descripción
Desconocido	Medios de almacenamiento cifrados con un método de autenticación no soportado por Cytomic Encryption.
Discos no cifrados	Ninguno de los medios de almacenamiento del equipo están cifrados ni por el usuario ni por Cytomic Encryption.
Discos cifrados	Todos los medios de almacenamiento del equipo están cifrados por Cytomic Encryption.
Cifrando	Al menos un medio de almacenamiento del equipo está en proceso de cifrado.
Descifrando	Al menos un medio de almacenamiento del equipo está en proceso de descifrado.
Cifrado por el usuario	Todos los medios de almacenamiento se encuentran cifrados pero alguno de ellos o todos fueron cifrados por el usuario.
Cifrado por el usuario (parcialmente)	Alguno de los medios de almacenamiento se encuentran cifrados por el usuario y el resto permanece sin cifrar o está cifrado por Cytomic Encryption.
Cifrado (parcialmente)	Al menos uno de los medios de almacenamiento del equipo está cifrado por Cytomic Encryption pero el resto permanece sin cifrar.

Tabla 14.7: Descripción de la serie Equipos cifrados

Filtros preestablecidos desde el panel

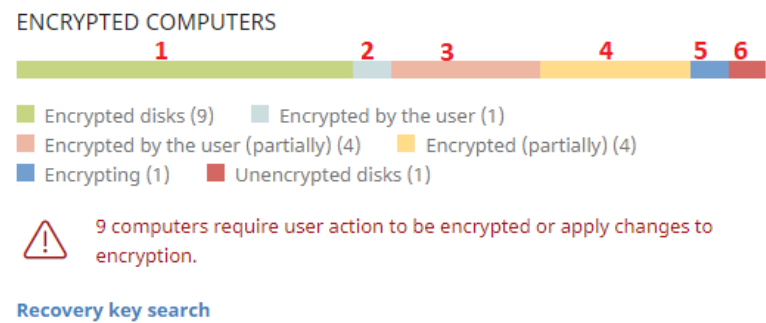


Figura 14.11: Zonas activas del panel Equipos Cifrados

Al hacer clic en las zonas indicadas en **Zonas activas del panel Equipos Cifrados** se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Cifrado de discos = Discos cifrados.
(2)	Cifrado de discos = Cifrado por el usuario.
(3)	Cifrado de discos = Cifrado por el usuario (parcialmente).
(4)	Cifrado de discos = Cifrado (parcialmente).
(5)	Cifrado de discos = Cifrando.
(6)	Cifrado de discos = Discos no cifrados.
(7)	Cifrado de discos = Descifrando.
(8)	Cifrado de discos = Desconocido.

Tabla 14.8: Definición de filtros del listado Estado del cifrado

Métodos de autenticación aplicados

Muestra los equipos con el cifrado configurado en la red, agrupados por el tipo de autenticación elegido. Consulta los tipos de autenticación compatibles en **Características generales de Cytomic Encryption**.

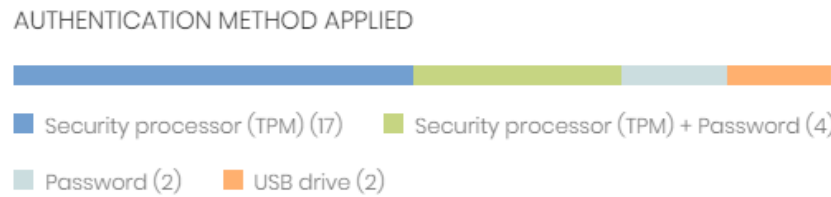


Figura 14.12: Panel Métodos de autenticación

Significado de las series

Serie	Descripción
Desconocido	El método de autenticación elegido por el usuario del equipo no está soportado por Cytomic Encryption.
Procesador de seguridad (TPM)	El método de autenticación utilizado es TPM.
Procesador de seguridad (TPM) + Contraseña	El método de autenticación utilizado es TPM y PIN o passphrase solicitado en el inicio del equipo.
Contraseña	- Equipos Windows: el método de autenticación elegido es PIN o passphrase solicitado en el inicio del equipo. - Equipos Mac: el método de autenticación aplicado es la contraseña solicitada en el inicio del equipo.
USB	El método de autenticación elegido es dispositivo USB conectado en el arranque del equipo.
Ninguno	Ninguno de los dispositivos de almacenamiento del equipo está cifrado.

Tabla 14.9: Descripción de la serie Métodos de autenticación aplicado

Filtros preestablecidos desde el panel

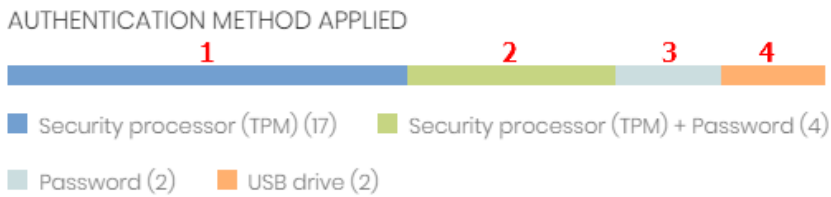


Figura 14.13: Zonas activas del panel Métodos de autenticación aplicado

Al hacer clic en las zonas indicadas en **Zonas activas del panel Métodos de autenticación aplicado** se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Método de autenticación = Procesador de seguridad (TPM)
(2)	Método de autenticación= Procesador de seguridad (TPM) + Contraseña
(3)	Método de autenticación = Contraseña
(4)	Método de autenticación = USB
(5)	Método de autenticación = Desconocido
(6)	Método de autenticación = Ninguno

Tabla 14.10: Definición de filtros del listado

Listados en Cytomic Encryption

Acceso a los listados

El acceso a los listados se puede hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Cytomic Encryption** y en el widget relacionado.
- ó
- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.
- Selecciona un listado de la sección **Protección de datos** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

El acceso al listado **Estado del cifrado** no requiere permisos adicionales para el administrador.

Estado del cifrado

Este listado muestra todos los equipos de la red gestionados por Advanced EDR y compatibles con Cytomic Encryption. Incorpora filtros relativos al módulo para controlar el estado del cifrado en el parque informático.

Campo	Comentario	Valores
Equipo	Nombre del equipo compatible con la tecnología de cifrado.	Cadena de caracteres
Estado del equipo	Reinstalación del agente:  Reinstalando agente.  Error en la reinstalación del agente. Reinstalación de la protección:  Reinstalando la protección.  Error en la reinstalación de la protección.  Pendiente de reinicio. Estado de aislamiento del equipo:  Equipo en proceso de entrar en aislamiento.  Equipo aislado.  Equipo en proceso de salir del aislamiento. Modo Contención de ataque RDP:  Equipo en modo contención de ataque RDP.  Finalizando modo de contención de ataque RDP.	Icono
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo y versión instalada en el equipo de usuario o servidor.	Cadena de caracteres
Cifrado de discos duros	Estado del módulo Cytomic Encryption.	- Sin información - Activado - Desactivado - Error

Campo	Comentario	Valores
		• Error instalando • Sin licencia
Estado de los discos	Estado de los medios de almacenamiento interno del equipo con respecto al cifrado.	• Desconocido • Discos no cifrados • Discos cifrados • Cifrando • Descifrando • Cifrado por el usuario • Cifrado por el usuario (parcialmente) • Cifrado (parcialmente)
Método de autenticación	Método de autenticación seleccionado para cifrar los discos.	• Todos • Desconocido • Procesador de seguridad (TPM) • Procesador de seguridad (TPM) + Contraseña • Contraseña • USB • Ninguno
Última conexión	Fecha de la última vez que el agente se conectó con la nube de Cytomic.	Fecha

Tabla 14.11: Campos del listado Estado de cifrado



Para visualizar los datos del listado gráficamente accede al widget **Equipos cifrados**

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo compatible con la tecnología de cifrado.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del módulo agente Cytomic.	Cadena de caracteres
Fecha de instalación	Fecha en la que el software Advanced EDR se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión		Fecha
Plataforma	Sistema operativo instalado en el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección	El módulo de la protección instalado en el equipo es la	Booleano

Campo	Comentario	Valores
actualizada	última versión publicada.	
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Conocimiento actualizado	El fichero de firmas descargado en el equipo es la última versión publicada.	Booleano
Fecha de la última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Cifrado de discos duros	Estado del módulo Cytomic Encryption.	• Sin información • Activado • Desactivado • Error • Error instalando • Sin licencia
Estados de los discos	Estado de los medios de almacenamiento interno del equipo con respecto al cifrado.	• Desconocido • Discos no cifrados • Discos cifrados • Cifrando • Descifrando • Cifrado por el usuario • Cifrado (parcialmente) • Cifrado por el usuario (parcialmente)
Acciones de cifrado pendientes del usuario	El usuario tiene pendiente introducir información o reiniciar el equipo para completar el proceso de cifrado de los volúmenes.	Booleano

Campo	Comentario	Valores
Métodos de autenticación	Método de autenticación seleccionado para cifrar los discos.	• Todos • Desconocido • Procesador de seguridad (TPM) • Procesador de seguridad (TPM) + Contraseña • Contraseña • USB • Ninguno
Fecha de cifrado	Fecha del volumen más antiguo cifrado dentro de la primera que vez se consideró al equipo como completamente cifrado (se cifraron todos sus volúmenes compatibles).	Fecha
Versión de especificación del TPM	Versión de las especificaciones TPM soportadas por el chip incluido en el equipo.	Cadena de caracteres
Fecha error instalación cifrado	Fecha del último error de instalación reportado.	Fecha
Error instalación cifrado	Se ha producido un error al instalar el módulo Cytomic Encryption en el equipo.	Cadena de caracteres
Fecha error cifrado	Última fecha en la que se reportó un error de cifrado en el equipo.	
Error cifrado	El proceso de cifrado devolvió un error.	Cadena de caracteres

Tabla 14.12: Campos del fichero exportado

Herramienta de filtrado

Campo	Comentario	Valores
Fecha de cifrado desde	Límite inferior del rango de fechas en la que se consideró al equipo como completamente cifrado.	Fecha
Fecha de cifrado hasta	Límite superior del rango de fechas en la que se consideró al equipo como completamente cifrado.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • macOS
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Estado de los discos	Estado de los medios de almacenamiento interno del equipo con respecto al cifrado.	• Desconocido • Discos no cifrados • Discos cifrados • Cifrando • Descifrando • Cifrado por el usuario • Cifrado (parcialmente) • Cifrado por el usuario (parcialmente)
Cifrado de discos duros	Estado del módulo Cytomic Encryption.	• Sin información • Activado • Desactivado • Error • Error Instalando • Sin licencia

Campo	Comentario	Valores
Método de autenticación	Método de autenticación seleccionado para cifrar los discos.	• Todos • Desconocido • Procesador de seguridad (TPM) • Procesador de seguridad (TPM) + Contraseña • Contraseña • USB • Ninguno
Última conexión	Fecha del último envío del estado de Advanced EDR a la nube de Cytomic.	Fecha
Acciones de cifrado pendientes del usuario	Indica si el proceso de cifrado está a la espera de acciones por parte del usuario.	• Todos • Si • No

Tabla 14.13: Campos de filtrado para el listado

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta [Información de equipo](#) en la página 218 para obtener más información.

Configuración del cifrado

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Cifrado**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración.

Permisos requeridos

Permiso	Tipo de acceso
Configurar cifrado de equipos.	Crear, modificar, borrar, copiar o asignar las configuraciones de Cifrado.

Permiso	Tipo de acceso
Ver configuraciones de cifrado de equipos	Visualizar las configuraciones de Cifrado.

Tabla 14.14: Permisos requeridos para acceder a la configuración de Cifrado

Opciones de configuración de Cytomic Encryption

Cifrar todos los discos duros de los equipos

Indica si los dispositivos de almacenamiento interno del equipo serán cifrados o no. Dependiendo del estado anterior del equipo, el comportamiento de Cytomic Encryption será diferente:

- Si el equipo está cifrado por Cytomic Encryption y se deshabilita **Cifrar todos los discos duros de los equipos**, se descifrarán todos los volúmenes cifrados.
- Si el equipo está cifrado pero no por Cytomic Encryption y se deshabilita **Cifrar todos los discos duros de los equipos** los volúmenes no sufren ningún cambio.
- Si el equipo está cifrado pero no por Cytomic Encryption y se habilita **Cifrar todos los discos duros de los equipos** se adecuará la configuración interna de cifrado para que coincida con los métodos soportados en Cytomic Encryption evitando volver a cifrar el volumen. Consulta [Cifrado de volúmenes ya cifrados previamente](#) para más información.

Si se trata de un equipo con sistema operativo macOS, se generará una clave de recuperación nueva. Consulta [Proceso de cifrado y descifrado para macOS](#)

- Si el equipo no está cifrado y se habilita **Cifrar todos los discos duros de los equipos** se cifrarán todos los volúmenes. Consulta [Proceso de cifrado y descifrado en Windows](#) y [Proceso de cifrado y descifrado para macOS](#).

Solicitar una contraseña para acceder al equipo (Windows)

Habilita la autenticación por contraseña en el arranque del equipo. Dependiendo de la plataforma y de la existencia de hardware TPM se permitirá el uso de dos tipos de contraseña:

- **Equipos con TPM:** se pedirá una contraseña de tipo PIN.
- **Equipos sin TPM:** se pedirá una contraseña de tipo passphrase.



Si estableces esta configuración a No y el equipo no tiene acceso a un procesador de seguridad TPM compatible, sus medios de almacenamiento no se cifrarán.

No cifrar los equipos que requieren un USB para autenticarse (Windows)

Para evitar la utilización de dispositivos USB soportados por Cytomic Encryption en la autenticación, el administrador puede deshabilitar su uso.



Solo los equipos Windows 7 sin TPM están en posición de utilizar el método de autenticación por USB. Si el administrador deshabilita el uso de USBs, estos equipos no serán cifrados.

Cifrar sólo el espacio utilizado (Windows)

El administrador puede minimizar el tiempo de cifrado empleado restringiendo la protección a los sectores del disco duro que están siendo utilizados. Los sectores liberados tras borrar un fichero continuarán cifrados pero el espacio libre previo al cifrado del disco duro permanecerá sin cifrar, siendo accesible por terceros mediante herramientas de recuperación de ficheros borrados.

Ofrecer cifrado de unidades de almacenamiento extraíbles (Windows)

Muestra al usuario una ventana con la posibilidad de cifrar los medios de almacenamiento masivo externos y llaves USB cuando los conecta al equipo. Consulta [Cifrado y descifrado de discos duros externos y llaves USB](#) para obtener más información acerca del comportamiento y los requisitos de esta configuración.

Filtros disponibles

Para localizar los equipos de la red que coincidan con alguno de los estados de cifrado definidos en Cytomic Encryption utiliza los recursos del árbol de filtros mostrados en [Árbol de filtros](#) en la página **180** con los campos mostrados a continuación:

- Cifrado:
 - Acciones de cifrado pendientes del usuario.
 - Cifrado de discos.
 - Fecha de cifrado.
 - Método de autenticación.
 - Tiene acciones pendientes de cifrado del usuario.
- Configuración:
 - Cifrado.
- Equipo:
 - Tiene TPM.
- Hardware:

- TPM - Activado.
- TPM - Fabricante.
- TPM - Propietario.
- TPM - Versión.
- TPM - Versión de especificación.
- Módulos:
 - Cifrado.

Capítulo 15

Configuración del bloqueo de programas

Para incrementar la seguridad de base en los equipos Windows de la red, el administrador puede bloquear la ejecución de los ficheros ejecutables (.exe) que considere peligrosos o no compatibles con la actividad desarrollada en la empresa. Las causas que pueden llevar a un administrador a prohibir la ejecución de un determinado programa pueden ser:

- Programas que por sus altos requisitos consumen mucho ancho de banda o establecen un número de conexiones desproporcionadamente grande, poniendo en peligro el rendimiento de la conectividad de la empresa si son ejecutados por muchos usuarios simultáneos.
- Programas que permiten acceder a contenidos susceptibles de contener amenazas de seguridad o que están protegidos por licencias que la empresa no ha adquirido previamente.
- Programas que permiten acceder a contenidos no relacionados con la actividad de la empresa y que pueden afectar al ritmo de trabajo de los usuarios.

Para obtener información adicional sobre los distintos apartados del módulo Bloqueo de programas consulta las referencias siguientes:



Crear y gestionar configuraciones en la página **258**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.

Acceso, control y supervisión de la consola de administración en la página **59**: gestión de cuentas de usuario y asignación de permisos.

Gestión de listados en la página **47**: información sobre como gestionar listados.

Contenido del capítulo

Configuración de Bloqueo de programas	518
Opciones de configuración de Bloqueo de programas	518
Listados del módulo Bloqueo de programas	519
Paneles / widgets del módulo Bloqueo de programas	522

Configuración de Bloqueo de programas

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Bloqueo de programas**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración de **Bloqueo de programas**.



Las configuraciones de bloqueo de programas solo se pueden asignar a puestos de trabajo o servidores Windows.

Permisos requeridos

Permiso	Tipo de acceso
Configurar bloqueo de programas	Crear, modificar, borrar, copiar o asignar las configuraciones de Bloqueo de programas.
Ver configuraciones de bloqueo de programas	Visualizar las configuraciones de Bloqueo de programas.

Tabla 15.1: Permisos requeridos para acceder a la configuración Bloqueo de programas

Opciones de configuración de Bloqueo de programas

Para crear una nueva configuración o modificar una existente introduce la información mostrada a continuación:

Campo	Descripción
Nombres de los programas a bloquear	Nombres de los ficheros ejecutables (.exe) que Advanced EDR impedirá su ejecución. En esta caja de texto acepta listas de nombres de ficheros copiadas / pegadas y separados por retorno de carro. No se admiten comodines para evitar configuraciones demasiado amplias que comprometan el buen funcionamiento del equipo.

Campo	Descripción
Código MD5 o SHA-256 de los programas a bloquear	MD5 o SHA-256 de los ficheros ejecutables (.exe) que Advanced EDR impedirá su ejecución. En esta caja de texto se aceptan listas de códigos MD5 o SHA-256 copiadas / pegadas y separados por retorno de carro.
Informar a los usuarios de los equipos de los bloqueados	Introduce un mensaje descriptivo para informar al usuario de que un fichero se ha bloqueado. El agente Advanced EDR mostrará una ventana desplegable con el contenido del mensaje.

Tabla 15.2: Configuración de una política de seguridad Bloqueo de programas



No bloquee programas del sistema operativo o componentes que sean necesarios para poder ejecutar correctamente los programas de usuario.

Advanced EDR no bloqueará ninguno de sus programas o módulos para garantizar el correcto funcionamiento de la solución de seguridad instalada.

Listados del módulo Bloqueo de programas

Acceso a los listados

El acceso a los listados se puede hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Seguridad** y en el widget relacionado.
ó
- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.
- Selecciona el listado **Programas bloqueados por el administrador** de la sección **Control de actividad** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

Permiso	Acceso a listados
Visualizar detecciones y amenazas	Programas bloqueados por el administrador

Tabla 15.3: Permisos requeridos para acceder a los listados de Programas bloqueados

Programas bloqueados por el administrador

Muestra el detalle de los programas bloqueados por Advanced EDR en los equipos de usuario y servidores.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Ruta	Ruta y nombre del programa bloqueado por el administrador en el equipo del usuario.	Cadena de caracteres
Fecha	Fecha en la que Advanced EDR bloqueó el programa.	Fecha

Tabla 15.4: Campos del listado Programas bloqueados por el administrador



Para visualizar los datos del listado gráficamente accede al widget **Programas bloqueados por el administrador**

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Software	Nombre del programa bloqueado por el administrador en el equipo del usuario.	Cadena de caracteres
Ruta	Ruta y nombre del programa bloqueado por el administrador en el equipo del usuario.	Cadena de caracteres
Acción	Acción ejecutada por Advanced EDR.	Cadena de caracteres "Bloquear"

Campo	Descripción	Valores
Fecha	Fecha en la que Advanced EDR bloqueó el programa.	Fecha
Usuario	Cuenta de usuario del sistema operativo que lanza el programa bloqueado.	Cadena de caracteres
MD5	Código MD5 del programa bloqueado por el administrador.	Cadena de caracteres
SHA-256	Código SHA-256 del programa bloqueado por el administrador.	Cadena de caracteres

Tabla 15.5: Campos del fichero exportado Programas bloqueados por el administrador

Herramienta de filtrado

Campo	Descripción	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Buscar hash	Código MD5 o SHA-256 del fichero a buscar.	Cadena de caracteres
Buscar programa comprometido	Nombre del programa bloqueado por el administrador.	Cadena de caracteres
Fechas	Intervalo de fechas en el que se ha producido el bloqueo del programa.	- Últimas 24 horas - Últimos 7 días - Último mes

Tabla 15.6: Campos de filtrado para el listado Programas bloqueados por el administrador

Ventana detalle del programa bloqueado

Al hacer clic en un elemento del listado se muestra la información del programa bloqueado.

Campo	Descripción	Valores
Programa bloqueado	Nombre del fichero bloqueado.	Cadena de caracteres

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se bloqueó el programa, dirección IP y grupo al que pertenece.	Cadena de caracteres
Usuario logueado	Cuenta de usuario bajo la cual se intentó ejecutar el programa bloqueado.	Cadena de caracteres
Nombre	Nombre del fichero bloqueado.	Cadena de caracteres
Ruta	Dispositivo de almacenamiento y carpeta del equipo donde se encuentra el programa bloqueado.	Cadena de caracteres
MD5	Código MD5 del programa bloqueado.	Cadena de caracteres
SHA-256	Si la detección lo incluye, se muestra el código SHA-256 del programa bloqueado.	Cadena de caracteres
Fecha detección	Fecha en la que se bloqueó el programa.	Fecha

Tabla 15.7: Campos de la ventana Detalle del programa bloqueado

Paneles / widgets del módulo Bloqueo de programas

Acceso al panel de control

Para acceder al panel de control haz clic en el menú superior **Estado**, panel lateral **Seguridad**.

Permisos requeridos

Permiso	Acceso a Widgets
Visualizar detecciones y amenazas	Programas bloqueados por el administrador

Tabla 15.8: Permisos requeridos para el acceso a los widgets de Programas bloqueados

Programas bloqueados por el administrador

Muestra el número de intentos de ejecución registrados en el parque informático y bloqueados por Advanced EDR según la configuración establecida por el administrador de la red.

Advanced EDR muestra una incidencia cada 24 horas por cada hash distinto detectado en cada equipo.



Figura 15.1: Panel Programas bloqueados por el administrador

Significado de las series

Serie	Descripción
Bloqueados	Número de intentos de ejecución registrados en el parque informático y bloqueados por Advanced EDR en el intervalo configurado.

Tabla 15.9: Descripción de la serie Programas bloqueados por el administrador

Filtros preestablecidos desde el panel



Figura 15.2: Zonas activas del panel Programas bloqueados por el administrador

Al hacer clic en las zonas indicadas en **Zonas activas del panel Programas bloqueados por el administrador** se abre el listado **Programas bloqueados por el administrador** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.

Tabla 15.10: Definición de filtros del listado Programas bloqueados por el administrador

Capítulo 16

Configuración de software autorizado

En los modos hardening y lock de la protección avanzada, Advanced EDR impide la ejecución de los programas desconocidos para la inteligencia de Cytomic hasta que se completa su clasificación. En casos muy concretos esta funcionalidad puede generar inconvenientes y retrasos menores para el usuario, sobre todo cuando el administrador de la red conoce el origen del programa y la naturaleza de su bloqueo:

- Programas de nicho muy específico y con un número de usuarios muy bajo.
- Programas que se actualizan automáticamente desde la Web del fabricante y sin intervención.
- Programas que distribuyen su funcionalidad a lo largo de cientos de librerías que son cargadas en memoria y, por tanto, bloqueadas conforme el usuario las va utilizando desde los distintos menús del programa.
- Programas que siguen el modelo cliente-servidor, donde la parte del cliente se almacena en un recurso de red compartido.
- Software polimórfico que genera nuevos ficheros ejecutables dinámicamente.



Para obtener información adicional sobre los distintos apartados del módulo Software autorizado consulta las referencias siguientes:

Crear y gestionar configuraciones en la página **258**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.

Acceso, control y supervisión de la consola de administración en la página **59**: gestión de cuentas de usuario y asignación de permisos.

Protección avanzada en la página **296**: configuración de los modos lock y hardening.

Contenido del capítulo

Software autorizado y exclusiones de elementos	526
Configuración de Software autorizado	527

Software autorizado y exclusiones de elementos

Advanced EDR permite evitar el bloqueo de programas mediante tres funcionalidades:

- **Mediante Archivos y rutas excluidas del análisis:** evita el análisis de ciertos elementos del equipo. No provoca bloqueos en la ejecución del software desconocido, pero puede suponer un agujero de seguridad y no se recomienda su uso excepto en casos de problemas de rendimiento. Consulta [Archivos y rutas excluidas del análisis](#) en la página 294 para más información.



Agregar una ruta a una carpeta específica para excluir del análisis solo excluye esa carpeta en particular. Las subcarpetas que están dentro de la carpeta excluida no se excluyen y seguirán siendo analizadas.

- **Desbloqueo de programas en clasificación:** ejecuta temporalmente los programas bloqueados pero tiene un enfoque reactivo: hasta que el programa no ha sido bloqueado, el administrador no puede proceder a su desbloqueo. Dado que un mismo software puede estar formado por varios componentes, y cada uno de ellos requerir un desbloqueo individual, el ciclo de bloqueos y desbloqueos se puede extender a lo largo del tiempo.
- **Configuración de software autorizado:** el administrador autoriza al usuario de forma proactiva ejecutar programas desconocidos antes de que Cytomic emita una clasificación. Este módulo es útil cuando la protección avanzada está en modo Lock o Hardening y encuentra un programa desconocido que impide al usuario su uso.

Software autorizado permite aprobar ficheros binarios ejecutables, pero excluye los ficheros de tipo script, dlls independientes y otros. Cuando Software autorizado permite ejecutar un binario, también permitirá ejecutar todos los recursos que necesite, incluyendo dlls y otros programas que pueda crear o invocar. Advanced EDR permitirá ejecutar cualquier fichero cuyo origen sea un instalador .msi o fichero .exe autoextraíble aprobado por Software autorizado.

Software autorizado establecido por el partner

Por defecto los administradores no pueden modificar ni borrar las configuraciones de **Software autorizado** enviadas por el partner. En las configuraciones enviadas desde el partner marcadas con **Editable settings**, los administradores podrán añadir nuevas reglas de Software autorizado, aunque no podrán borrar ni modificar las reglas establecidas por el partner.

Si el partner cambia el estado de las configuraciones enviadas de editable a no editable, las reglas de software autorizado añadidas por el usuario se ocultarán y dejarán de aplicarse, de modo que solo se

aplicarían las enviadas por el partner. Si el partner vuelve a establecer la configuración como editable, las reglas añadidas por el administrador se restaurarán y volverán a aplicarse.

Configuración de Software autorizado

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Software autorizado**.
- Haz clic en el botón **Añadir**, se abrirá la ventana **Añadir configuración**.



Las configuraciones de Software autorizado solo se pueden asignar a puestos de trabajo o servidores Windows.

Permisos requeridos

Permiso	Tipo de acceso
Configurar software autorizado	Crear, modificar, borrar, copiar o asignar las configuraciones de Software autorizado.
Ver configuraciones de software autorizado	Visualizar las configuraciones de Software autorizado.

Tabla 16.1: Permisos requeridos para acceder a la configuración Software autorizado

Funcionamiento del módulo Software autorizado

Los usuarios de la red podrán ejecutar el software desconocido que se encuentre en proceso de clasificación siempre que el administrador de la red lo haya permitido mediante una regla de software autorizado.

Cuando el proceso de análisis termine, Advanced EDR emitirá una clasificación del programa (goodware o malware). Si el programa resulta ser una amenaza, quedará bloqueada su ejecución independientemente de que pertenezca a una configuración de software autorizado.

Opciones de configuración del módulo Software autorizado

Una configuración de software autorizado está formada por una o más reglas, cada una de ellas describe un único software o una familia de programas a los que Advanced EDR permitirá su ejecución cuando ésta ha sido bloqueada por no conocerse su clasificación.

Crear una regla de software autorizado

Haz clic en el enlace  **Autorizar programas** para crear una regla con la información mostrada a continuación, y haz clic en el botón **Autorizar**:

Campo	Descripción
Nombre	Nombre de la regla.
MD5 o SHA-256	MD5 o SHA-256 de los ficheros cuya ejecución permitirá Advanced EDR. Consulta el apartado Calcular el MD5 o SHA-256 de uno o más ficheros .
Nombre del producto	Es el campo Nombre producto de la cabecera del archivo a desbloquear. Para obtener el valor, haz clic con el botón derecho del ratón en el programa y elige Propiedades, Detalles .
Ruta del archivo	Ruta donde se almacena el programa en el equipo de usuario o servidor. Acepta variables de entorno de sistema.
Nombre del archivo	Nombre del archivo. Acepta los comodines * y ?.
Versión del archivo	Es el campo Versión de la cabecera del archivo a desbloquear. Para obtener el valor, haz clic con el botón derecho del ratón en el programa y elige Propiedades, Detalles .
Firma	Es la huella digital correspondiente a la firma del archivo. Consulta el apartado Obtener la huella digital de un programa firmado .

Tabla 16.2: Configuración de una regla de software autorizado

Borrar una regla de software autorizado

- Haz clic en el icono  situado a la derecha de la regla de software autorizado a borrar.
- Haz clic en el botón **Guardar** situado en la parte superior derecha de la ventana para actualizar la configuración de software autorizado.

Modificar una regla de software autorizado

- Haz clic en el nombre de la regla de software autorizado. Se abrirá la ventana **Autorizar programas**.
- Modifica las propiedades de la regla y haz clic en el botón **Autorizar**.
- Haz clic en el botón **Guardar** situado en la parte superior derecha de la ventana. La configuración de software autorizado se actualizará.

Copiar una regla de software autorizado

- Haz clic en el icono  situado a la derecha de la regla de software autorizado a copiar. Se abrirá la ventana **Autorizar programas**. El campo **Nombre** contiene el nombre de la regla con el prefijo “copia de”.
- Modifica las propiedades de la regla y haz clic en el botón **Autorizar**.
- Haz clic en el botón **Guardar** situado en la parte superior derecha de la ventana. La configuración de software autorizado se actualizará.

Calcular el MD5 o SHA-256 de uno o más ficheros

Existen multitud de herramientas en el mercado que calculan el código MD5 o SHA-256 de un fichero. En este apartado se utilizará la herramienta PowerShell incluida en Windows 10.

- Abre la carpeta que contiene los ficheros, haz clic en el menú **Archivo** del explorador y elige **Abrir Windows PowerShell**. Se abrirá una ventana con la línea de comandos.



```
PS C:\Windows> Get-FileHash -Algorithm md5 -path *.*.exe
```

Algorithm	Hash	Path
MD5	B28629E512290B02B36588B39A42B8A4	C:\Windows\bfsvc.exe
MD5	800EF617DDC3C635CD25E20E0EC39CC6	C:\Windows\explorer.exe
MD5	67094590E3D57130C587CD6D8AFB6597	C:\Windows\HelpPane.exe
MD5	DF73D52FDCE65F90A2E49EFB5248C77C	C:\Windows\hh.exe
MD5	06E6C0482562459ADB462CA9008262F8	C:\Windows\notepad.exe
MD5	BD2DF000DAFEE5CF6A9E10B5333C7F3A	C:\Windows\py.exe
MD5	89666526F21B8CB3F65622D8AFD9356F	C:\Windows\pyw.exe
MD5	29409008DF22243BB320333F9FD5C060	C:\Windows\regedit.exe
MD5	5B6E47C03F517838B813AB87C27DEF6D	C:\Windows\splwow64.exe
MD5	CAA192BFD8B5F2A131EBD649B7062DE3	C:\Windows\winhlp32.exe
MD5	1D27F61CC5D659247D2E0C111C5386DE	C:\Windows\write.exe

Figura 16.1: Línea de comandos con el resultado del comando Get-FileHas

- Escribe el siguiente comando y sustituye \$files por la ruta de los ficheros. Se admiten los comodines * y ?.

MD5

```
PS c:\carpeta> Get-FileHash -Algorithm md5 -path $files
```

SHA-256

```
PS c:\carpeta> Get-FileHash -Algorithm sha256 -path $files
```

- Para copiar los códigos MD5 o SHA-256 al portapapeles, presiona la tecla **Alt** y sin soltarla, selecciónalos con el ratón. Una vez hecho, presiona la combinación de teclas **Ctrl+C**.

- Para pegar todos los códigos MD5 o SHA-256 desde el portapapeles a la consola de Advanced EDR, haz clic en el campo **MD5** o SHA-256 de la regla de software autorizado y presiona la combinación de teclas `Ctrl+V`.
- Haz clic en el botón **Autorizar** y en el botón **Guardar** situado en la parte superior derecha de la pantalla. La configuración de software autorizado se actualizará.

Obtener la huella digital de un programa firmado

- Abre Windows Powershell y navega hasta el directorio en el que se encuentra el programa.
- Ejecuta el comando y sustituye `$file` por la ruta de los ficheros:

```
PS c:\carpeta> Get-AuthenticodeSignature -FilePath $file
```

- Selecciona la cadena de caracteres que devuelve el comando y presiona `Ctrl+C` para copiarla al portapapeles.
- Haz clic en el campo **Firma** de la regla de software autorizado y presiona la combinación de teclas `Ctrl+V` para pegar la huella digital .
- Haz clic en el botón **Autorizar** y en el botón **Guardar** situado en la parte superior derecha de la pantalla. La configuración de software autorizado se actualizará.

Capítulo 17

Gestión y detección de IOCs

IOC (Indicators Of Compromise) es un estándar de la industria que permite describir condiciones en los equipos informáticos que, de cumplirse, pueden comprometer la seguridad de las organizaciones. Siendo un concepto similar al del fichero de firmas, su principal diferencia con éste es su formato abierto, que favorece la colaboración e intercambio de inteligencia de seguridad, y permite al administrador extender de forma sencilla las capacidades de detección de Advanced EDR.

Este capítulo describe las herramientas implementadas en Advanced EDR para importar y exportar IOCs en el producto, buscar en los equipos protegidos indicadores de compromiso y visualizar de forma rápida los resultados.

Para obtener información adicional sobre los distintos apartados del módulo Software autorizado consulta las referencias siguientes:



Crear y gestionar configuraciones en la página **258**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.

Acceso, control y supervisión de la consola de administración en la página **59**: gestión de cuentas de usuario y asignación de permisos.

Protección avanzada en la página **296**: configuración de los modos lock y hardening.

Contenido del capítulo

Conceptos de IOCs	532
Flujo de trabajo general con IOCs	533
Gestión de IOCs	533
Búsqueda de IOCs en la red	540

Listados de IOCs encontrados	543
Paneles / widgets de IOCs	550

Conceptos de IOCs

Para una correcta comprensión de los procesos involucrados en el uso de IOCs es necesario presentar algunos conceptos relativos a las tecnologías que soportan este estándar de la industria.

IOC (Indicator Of Compromise, Indicador de compromiso)

Conjunto de reglas que describen patrones de comportamiento sospechosos de pertenecer a un ciberataque. A diferencia del fichero de firmas, con un objetivo similar, el IOC tiene un formato abierto que permite el intercambio de inteligencia de seguridad entre los diversos actores (proveedores, consumidores, usuarios etc.).

Existen varios estándares para describir patrones de comportamiento sospechosos, de entre todos ellos el más extendido en la actualidad es STIX.

STIX (Structured Threat Information Expression)

Es un lenguaje basado en JSON que describe las amenazas de seguridad de manera estructurada e interrelacionada para lograr una mejor legibilidad y comprensión. Esta basado en grafos que representa los objetos y sus relaciones de manera intuitiva.

Cada IOC contiene una serie de entidades y relaciones que describen al detalle cada “artefacto” o indicio que identifica al ataque, como por ejemplo direcciones IP o dominios susceptibles de albergar servidores C&C (Command & Control), MD5 o SHA de ficheros sospechosos de contener virus y otras amenazas etc.

STIX también permite aprovechar la información descrita en otros formatos, como por ejemplo reglas YARA.

Advanced EDR es compatible con el estándar STIX 2.x

YARA (Yet Another Recursive Acronym)

Es un lenguaje basado en reglas que permite crear descripciones de familias de malware basadas en patrones textuales o binarios. Estas reglas están formadas por conjuntos de cadenas de caracteres y expresiones booleanas que las relacionan, y se utilizan en búsquedas sobre los ficheros del equipo sospechoso de haber sido infectado.

Un IOC puede incorporar una única regla YARA en su definición, aunque ésta puede ser todo lo compleja que sea necesaria para detectar familias enteras de malware.

Otros formatos de IOCs

Actualmente, en el mercado existen varios formatos abiertos para el intercambio de inteligencia de seguridad que cumplen funciones equivalentes. Algunos de esos formatos son OpenIOC y TAXII, entre otros. Por otra parte, un mismo formato de IOC puede tener varias versiones incompatibles entre sí, como es el caso de STIX 1.x y 2.x.

Para poder reutilizar IOCs descritos en formatos no compatibles con Advanced EDR, existen herramientas gratuitas que realizan las conversiones necesarias para transformar cualquier IOC en uno con el formato STIX 2.x.

Resultados generados por una búsqueda de IOCs

Para no sobrecargar a los equipos de la red, Advanced EDR limita la profundidad de las búsquedas complejas de IOCs aplicando las reglas siguientes:

- **Para IOCs simples o con una regla YARA:** son aquellos que buscan un único atributo con un valor concreto. Estos IOCs devolverán hasta 10 resultados por equipo, momento en que la búsqueda se detendrá.
- **Para IOCs complejos:** son aquellos que buscan varios atributos, o un atributo con varios valores. Estos IOCs devolverán el primer resultado encontrado en cada equipo, momento en que la búsqueda se detendrá.

Debido a este modo de funcionamiento, el número de resultados mostrado en los listados y widgets puede no ser completo, sobre todo en infecciones masivas con muchos ficheros afectados en cada equipo de la red de la empresa. En estos casos se garantiza que por lo menos se muestre un resultado por cada equipo de la red sin afectar a su rendimiento.

Flujo de trabajo general con IOCs

Sigue el flujo de trabajo para buscar con éxito indicios de ataques informáticos en la red:

- Comprueba que la cuenta de usuario que accede a la consola tiene los permisos requeridos. Consulta el apartado [Gestión de IOCs](#) para más información.
- Importa IOCs de terceros o créalos mediante el asistente. Consulta el apartado [Gestión de IOCs](#) para más información.
- Crea una tarea de búsqueda de IOCs. Consulta el apartado [Búsqueda de IOCs en la red](#) para más información.
- Visualiza los IOCs encontrados mediante los resultados de la tarea de búsqueda, con el listado de IOCs o con los widgets disponibles. Consulta el apartado [Búsqueda de IOCs en la red](#) y [Paneles / widgets de IOCs](#) para más información.

Gestión de IOCs

Acceso a la galería de IOCs

Para acceder a la galería de IOCs, haz clic en el menú superior **Configuración** y en el panel lateral **Galería de IOCs**. Se desplegará un listado con los IOCs importados.

Permisos requeridos

Para poder ver y acceder a la funcionalidad de IOCs es necesario tener asignado el permiso **Buscar y administrar IOCs** en el rol de la cuenta de usuario. Para asignar el permiso consulta el apartado **Buscar y administrar IOCs** en la página 73.



Búsqueda de IOCs es compatible con equipos Windows.

Galería de IOCs

La galería de IOCs muestra un listado de todos los IOCs importados o creados con el asistente. Por cada IOC se incluye la información siguiente:

Campo	Descripción	Valores
Nombre	Nombre del IOC asignado en el momento de su creación o importación.	Cadena de caracteres
Descripción	Campo descripción del IOC.	Cadena de caracteres
Tipo	Estado de IOC: • STIX (Pendiente de aprobación): el IOC fue importado desde una fuente externa y requiere su aprobación para adaptarlo al formato aceptado por Advanced EDR. • STIX: el IOC fue importado desde una fuente externa y se aprobó, con lo que ya se encuentra adaptado al formato aceptado por Advanced EDR y puede usarse en las búsquedas. • Creado por el usuario: IOC creado a través del asistente de la consola web. No requiere aprobación para usarse en las búsquedas. Consulta el apartado Aprobar un IOC importado para obtener más información.	Enumeración
Fecha de modificación	Fecha en la que se modificó el IOC.	Fecha

Campo	Descripción	Valores
Fecha de creación	Fecha en la que se creó el IOC.	Fecha

Tabla 17.1: Listado de IOCs creados o importados

Crear un nuevo IOC

- Haz clic en el botón **Añadir** situado en la esquina superior derecha. Se abrirá la ventana **Añadir IOC**.
- Introduce los campos **Nombre**, **Autor**, **Descripción**.
- En el campo propiedad Introduce la característica del ataque a detectar:
 - **MD5 del archivo**: comprueba que existe un fichero con el hash indicado en formato MD5.
 - **SHA-256 del archivo**: comprueba que existe un fichero con el hash indicado en formato SHA-256.
 - **Nombre del archivo**: comprueba que existe un fichero con el nombre indicado.
 - **Ruta del archivo**: comprueba que existe un fichero con la ruta indicada.
 - **Dominio**: comprueba que existe una conexión de red establecida mediante TCP o UDP desde o hacia el dominio indicado.
 - **IPv4**: comprueba que existe una conexión TCP o UDP establecida desde o hacia la IP indicada.
 - **IPv6**: comprueba que existe una conexión TCP o UDP establecida desde o hacia la IP indicada en formato IPv6.
 - **Regla YARA**: comprueba que existe un fichero cuyo contenido coincide con el patrón descrito en la regla YARA indicada.
- **Selecciona el operador**: determina el modo de comparación de la propiedad encontrada en el equipo con el valor de referencia establecido por el administrador en el IOC.
 - **En**: cuando se indiquen una o varias propiedades en el campo valor, el equipo solo deberá cumplir una.
 - **Es igual a**: la propiedad encontrada en el equipo coincide exactamente con la indicada por el administrador en el campo valor.
- **Valor**: establece las propiedades con las que se realizará la búsqueda:
 - Uno o varios valores separados por retorno de carro.
 - No admite comodines.
- **Nueva condición**: añade más condiciones a la regla. Se aplicarán los operadores lógicos Y/O.

Operadores lógicos

Para combinar dos condiciones o más en una misma regla se utilizan los operadores lógicos Y y O. Al añadir una segunda condición y sucesivas a una regla se mostrará de forma automática un desplegable con los operadores lógicos disponibles, que se aplicarán a las condiciones adyacentes.

Agrupaciones de condiciones de regla

Los paréntesis en una expresión lógica se utilizan para variar el orden de evaluación de los operadores que relacionan las condiciones de las reglas introducidas.

Para encerrar dos o más condiciones en un paréntesis crea una agrupación marcando con las casillas de selección las condiciones consecutivas que formarán parte del grupo y haz clic en el botón **Agrupar condiciones**. Se mostrará una línea delgada que abarcará las reglas de reglas de monitorización que forman parte de la agrupación.

Mediante el uso de paréntesis se definen agrupaciones de varios niveles para poder anidar grupos de operandos en una expresión lógica.

Condiciones de uso de reglas YARA

Un IOC no puede incorporar más de una regla YARA. Si el administrador añade una regla YARA a un IOC vacío, no podrá utilizar otras propiedades. De igual modo, si el administrador ya ha añadido otras propiedades al IOC, las reglas YARA quedarán deshabilitadas.

En caso de que la regla no cumpla con la sintaxis YARA, la consola mostrará un mensaje de error y no permitirá guardar el IOC.

Copiar un IOC

Las copias de IOCs se ejecutan desde el listado de **Galería de IOCs** siguiendo los pasos mostrados a continuación:

- Haz clic en el icono . Se desplegará un menú de contexto.
- Selecciona la opción **Hacer una copia**. Se mostrará la ventana **Editar IOC** con los datos del IOC original precargados, excepto por:
 - **Nombre**: nombre del IOC original precedido por "copia de".
 - **Identificador**: no se mostrará. Se generará un nuevo **Identificador** automáticamente al guardar el IOC.

Borrar IOCs

Durante la ejecución de una tarea no se podrá borrar un IOC que esté en uso, sin importar el estado en el que se encuentre la tarea. Al intentarlo se mostrará un mensaje de error.

Borrar un IOC

Haz clic en el menú de contexto del IOC a borrar y elige la opción **Eliminar**. El IOC se borrará del listado. Las estadísticas de los IOCs encontrados hasta la fecha del borrado se mantendrán en el listado de **IOCs detectados** y en los widgets del panel de control **IOCs**.

Borrar uno o varios IOCs

- Selecciona los elementos que quieres eliminar con las casillas de selección del listado de IOCs.
- Haz clic en el botón de menú desplegable y en **Borrar**. La opción de **Borrar** también se muestra en la barra de herramientas superior.

Las estadísticas de los IOCs encontrados hasta la fecha del borrado se mantendrán en el listado de **IOCs detectados** y en los widgets del panel de control **IOCs**.

Importar y exportar IOCs

Durante la ejecución de una tarea no se podrá importar un IOC con el mismo Identificador que otro en uso, sin importar el estado en el que se encuentre la tarea. Al intentarlo se mostrará un mensaje de error.

Importar un IOC

Para importar un IOC sigue los pasos mostrados a continuación:

- Haz clic en el icono  situado en la esquina superior derecha. Se mostrará la ventana de importación.
- Haz clic en **Seleccionar archivo** y elige un fichero compatible con STIX, YARA o valores separados por comas.
- Haz clic en el botón **Importar**. El nuevo IOC se mostrará en la galería de IOCs.
- En el caso de que el IOC ya exista se preguntará que hacer:
 - **Reemplazar**: actualiza el IOC existente con la nueva información.
 - **Ignorar**: descarta la nueva información conservando el IOC existente.

Aprobar un IOC importado

Los IOCs importados de fuentes externas requieren un paso previo antes de poder utilizarse en las búsquedas. Este paso es necesario para comprobar que realmente el IOC subido es interpretado por Advanced EDR de forma correcta, ya que no todas las entidades soportadas por la especificación STIX 2.x se tienen en cuenta a la hora de realizar una búsqueda.

Una vez importado el IOC, sigue los pasos mostrados a continuación:

- Si el IOC no ha sido aprobado mostrara el mensaje (**Pendiente de aprobación**) en la columna **Tipo** del listado.
- Haz clic en el IOC a aprobar. Se mostrará la ventana de **Editar IOC**.

- Si existe alguna regla del IOC que no pueda ser interpretada por Advanced EDR se mostrará un recuadro en rojo indicado la situación. Los datos mostrados en la ventana de edición se corresponderán a las secciones del IOC que son correctamente interpretadas por Advanced EDR.
- Si las reglas mostradas son correctas, haz clic en el botón **Aprobar sentencia de búsqueda y guardar** para poder utilizar el IOC en las búsquedas.

Advanced EDR solo elimina reglas en un IOC importado al ejecutar búsquedas. El IOC sin embargo se almacenará de forma íntegra en el servidor de Cytomic y se podrán ver sus entidades y relaciones así como el código fuente original.

Exportar un único IOC

- En el listado de IOCs haz clic en el icono  asociado al IOC a exportar. Se mostrará un menú desplegable.
- Selecciona la opción **Exportar**. Se descargará en el equipo del administrador un fichero JSON con la definición del IOC.

Exportar uno o varios IOCs

- Haz clic en las casillas de selección de los IOCs a exportar en el listado de IOCs.
- Haz clic en la opción **Exportar** de la barra de herramientas. Se descargará un único archivo json con la definición de todos los IOCs seleccionados.

Visualizar IOCs importados

Representar gráficamente un IOC

Haz clic sobre el menú contextual del IOC elegido y en la opción **Ver archivo STIX original**. Se mostrará la ventana **Archivo STIX** con la representación gráfica del IOC y el **Código** del IOC.

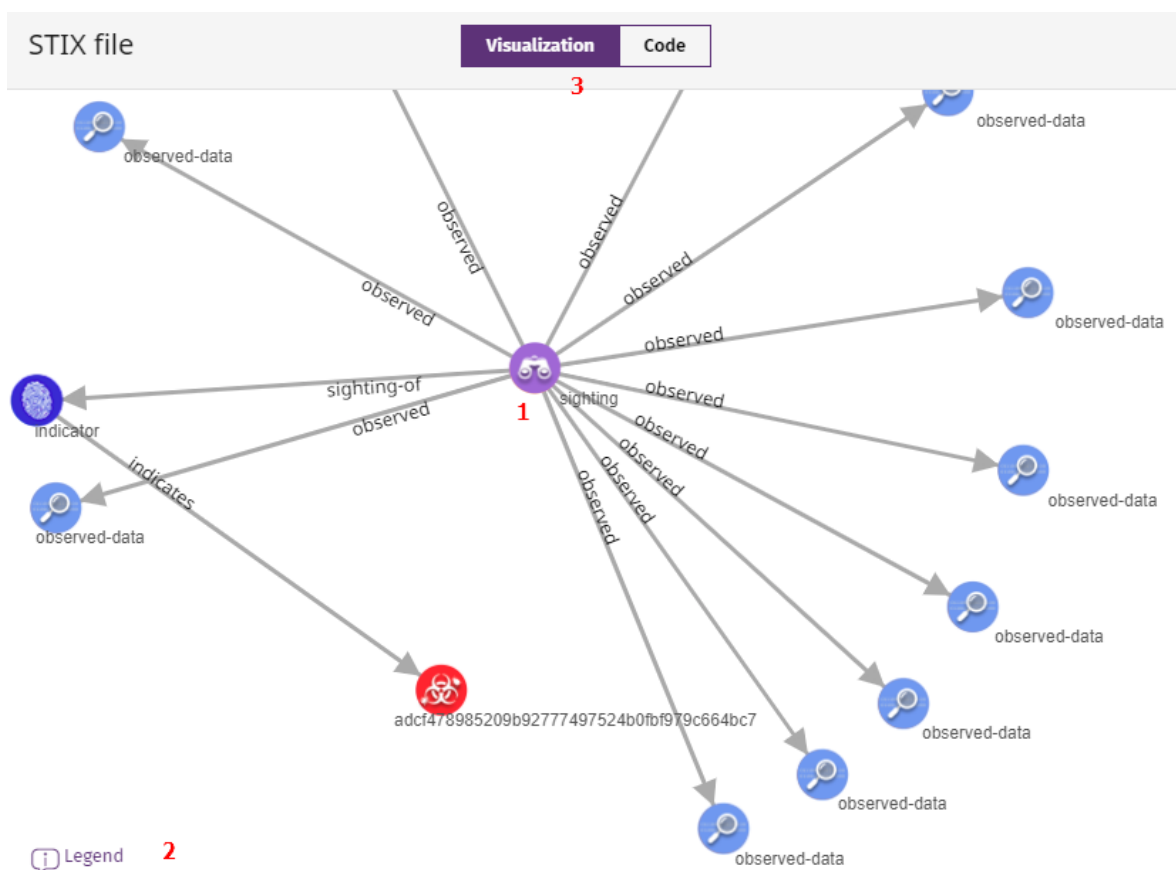


Figura 17.1: Representación gráfica de un IOC

La ventana Archivo STIX tiene las características siguientes:

- Ordena las distintas entidades **(1)** del diagrama pinchando en cada una de ellas y arrastrándola con el ratón.
- Haz clic en el enlace **Leyenda (3)** para obtener el significado de cada uno de los iconos representados en la gráfica.
- Haz clic en el selector **Visualización / Código (3)** para alternar entre la vista gráfica y la definición del IOC. El código del IOC se muestra tabulado y se puede copiar al portapapeles.



Aunque el código del IOC se muestra de forma íntegra tal y como se importó desde la fuente original, Advanced EDR puede omitir ciertas secciones no compatibles con la implementación. Por esta razón los resultados obtenidos de una búsqueda pueden no ser los esperados.

Filtrar IOCs importados

Para filtrar los elementos del listado de IOCs utiliza la barra de búsqueda del panel de la **Galería de IOCs**. Introduce el nombre o la descripción como términos de búsqueda para mostrar solo los elementos del

listado que coincidan.

Búsqueda de IOCs en la red



Búsqueda de IOCs es compatible con equipos Windows.

Advanced EDR utiliza su motor de tareas para configurar y ejecutar búsquedas de IOCs en los equipos de la red del cliente, accesible desde el menú de **Tareas** y desde la **Galería de IOCs**. Consulta el capítulo **Tareas** en la página **825** para obtener más información sobre cómo gestionar tareas en Advanced EDR.

Permisos requeridos para gestionar tareas de tipo Detectar IOCs

Para gestionar tareas de tipo **Detectar IOCs** es necesario que la cuenta de usuario utilizada para acceder a la consola web tenga asignado el permiso **Buscar y administrar IOCs** a su rol. Para obtener más información sobre el sistema de permisos consulta **Descripción de los permisos implementados** en la página **70**.

Acceso a búsqueda de IOCs



Las búsquedas solo se pueden ejecutar con IOCs previamente aprobados.

Desde el menú de Tareas

- En el menú superior haz clic en **Tareas**, **Añadir tarea** y selecciona **Detectar IOCs**.

Desde el listado de Galería de IOCs

- En el menú superior **Configuración**, accede en el panel lateral a la **Galería de IOCs**.
- Selecciona el IOC o grupo de IOCs a buscar marcando las casillas de selección.
- Para buscar IOCs, si has seleccionado un solo elemento haz clic en el menú de contexto asociado y selecciona **Buscar IOCs**. Si has seleccionado varios, haz clic en **Buscar IOCs** en la barra superior de herramientas. Se creará una nueva tarea de búsqueda de IOCs. Para configurarla consulta **Configurar una tarea de búsqueda de IOCs**.

Configurar una tarea de búsqueda de IOCs

- Escribe la información general de la tarea en los campos **Nombre** y **Descripción**.
- Haz clic en el enlace **Destinatarios (No se ha asignado a ningún equipo)** y haz clic en el botón **Cerrar** para salvar la tarea. Se abrirá una ventana nueva donde seleccionar los equipos que

recibirán la tarea configurada.

- Selecciona el tipo de equipos que recibirán la tarea: **Estación**, **Portátil** o **Servidor**.
- Haz clic en el botón  para agregar equipos individuales o grupos de equipos, y en el botón  para eliminarlos.
- Haz clic en el botón **Ver equipos** para verificar los equipos que recibirán la tarea.
- Indica la programación horaria de la tarea:
 - **Empieza:** marca el inicio de la tarea.

Valor	Descripción
Lo antes posible (activado)	La tarea se lanza en el momento si el equipo está disponible (encendido y accesible desde la nube), o cuando se encuentre disponible dentro del margen definido en el desplegable Equipo apagado .
Lo antes posible (desactivado)	La tarea se lanza en la fecha seleccionada en el calendario, indicando si se tiene en cuenta la hora del equipo o la hora del servidor Advanced EDR.
Equipo apagado	Si el equipo está apagado o inaccesible, la tarea no se podrá lanzar. El sistema de programación de tareas permite establecer la caducidad de la tarea en función del intervalo de tiempo definido por el administrador, desde 0 (la tarea caduca de forma inmediata si el equipo no está disponible) a infinito (la tarea siempre está activa y se espera a que el equipo esté disponible de forma indefinida): • No ejecutar: la tarea se cancela si en el momento del lanzamiento el equipo no está encendido o no es accesible. • Dar un margen de: define un intervalo de tiempo dentro del cual, si el equipo inicialmente no estaba disponible y vuelve a estarlo, la tarea será lanzada. • Ejecutar cuando se encienda: no establece ningún intervalo de tiempo sino que se espera de forma indefinida a que el equipo esté accesible para lanzar la tarea.

Tabla 17.2: Comportamiento del inicio de la tarea si el equipo no está disponible

- **Tiempo máximo de ejecución:** indica el tiempo máximo que la tarea puede tardar en completarse, transcurrido el cual se cancelará con error si no ha terminado.

Valor	Descripción
Sin límite	La duración de la ejecución de la tarea no está definida, pudiéndose extender hasta el infinito.
1, 2, 8 o 24 horas	La duración de la ejecución de la tarea está acotada. Transcurrido el tiempo indicado, la tarea se cancela con error si no ha terminado.

Tabla 17.3: Configuración de la duración de la tarea

- Haz clic en **Guardar**. La tarea aparecerá en el listado de tareas configuradas, pero mostrará la etiqueta **Sin publicar**, indicando que no está activa.
- Haz clic en el enlace **Publicar** para introducir la tarea en el programador de Advanced EDR, encargado de marcar el momento en que se lanzan las tareas según su configuración.

Prioridad de las tareas de búsqueda de IOCs

Tarea	Comportamiento
Detección de IOCs	Espera a que finalice la tarea de búsqueda en ejecución y comienza al acabar la primera.
Instalación de parches	La tarea de búsqueda de IOCs se ejecuta de forma concurrente con la tarea de instalación de parches. No se interrumpirá la tarea de instalación de parches por el riesgo que supone para la integridad del sistema.
Análisis o desinfección	Cancela la tarea de análisis o desinfección y comienza la ejecución de la tarea de detección de IOCs. Las tareas de análisis o desinfección creadas cuando hay una tarea de búsqueda de IOCs en funcionamiento no inician su ejecución hasta que la tarea de IOCs ha finalizado.
Búsqueda de Cytomic Data Watch	Comienza a ejecutar la tarea sin cancelar ni detener la tarea de Cytomic Data Watch.
Indexación de Cytomic Data Watch	Comienza a ejecutar la tarea y detiene temporalmente la tarea de Cytomic Data Watch.

Tabla 17.4: Orden de prioridad al ejecutar tareas de IOCs

Comportamiento de las tareas de búsqueda de IOCs frente a reinicios del equipo

La ejecución de las tareas de búsqueda se cancelan y se reinician automáticamente cuando sea posible en el equipo del usuario y desde su comienzo en los casos siguientes:

- Cuando el administrador solicita el reinicio del equipo desde consola web.
- Cuando el usuario local solicita el reinicio del equipo desde el propio equipo.
- Cuando se tiene que proceder al reinicio del equipo automáticamente por actualización de alguno de los componentes del software de seguridad instalado.

Comportamiento en caso de cancelación manual de tareas de búsqueda de IOCs

En caso de que el administrador interrumpa de manera manual la tarea desde la consola web el comportamiento será el siguiente:

- La búsqueda de IOCs se detendrá lo antes posible en el equipo.
- Se registrarán los resultados detectados hasta el momento de la cancelación.

Listados de IOCs encontrados

Acceso a los listados

Para acceder al listado completo de los IOCS detectados:

- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del menú lateral.
- Selecciona el listado **IOCs detectados** en la sección de **Seguridad**.

Para acceder al listado de un IOC concreto:

- En el menú superior **Configuración** selecciona **Galería de IOCs**.
- Haz clic en el icono  situado a la derecha de cada línea de IOC para desplegar su menú de contexto.
- Selecciona **Ver detecciones del IOC**. Se mostrará el listado **IOCs detectados** filtrado por el IOC seleccionado.

Para ver el listado de IOCs detectados asociado a una tarea de búsqueda:

- Haz clic en el menú superior **Tareas**. Se mostrará el listado de tareas creadas.
- En una tarea de tipo **Búsqueda de IOCs** haz clic sobre el enlace **Ver Resultados**.

Permisos requeridos

Para poder ver y acceder a los listados relacionados con los IOC's es necesario tener asignado el permiso **Buscar y administrar IOC's** en el rol de la cuenta de usuario.

IOC's encontrados por cada tarea

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se encontró el IOC.	Cadena caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Estado	Estado de la tarea.	• Pendiente • En curso • Finalizado • Con error • Cancelada (no se pudo iniciar a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)
IOC's detectados	Número de IOC's detectados en el equipo.	Cadena de caracteres
Fecha de comienzo	Fecha y hora en la que se inició la tarea.	Fecha
Fecha de fin	Fecha en la que se finalizó la tarea.	Fecha

Tabla 17.5: Listado de resultados de IOC's encontrados

Campos mostrados en el enlace Ver IOC's detectados

Al visualizar los resultados de una tarea de IOC's, en la parte superior derecha se muestra la opción de **Ver IOC's detectados**. Haz clic sobre ella y se mostrará el listado completo de los IOC's encontrados en la tarea.

Campo	Descripción	Valores
Equipo	Nombre del equipo en el que se ha detectado el IOC.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Nombre del IOC detectado	Nombre del IOC encontrado en el equipo.	Cadena de caracteres
Descripción de IOC detectado	Descripción asignada por el administrador al dar de alta el IOC.	Cadena de caracteres
Fecha	Fecha en la que se ha detectado el IOC en el equipo.	Fecha

Tabla 17.6: Campos mostrados en el enlace Ver IOCs detectados

Herramienta de filtrado

Campo	Descripción	Valores
Estado	Estado de la tarea.	• Todos los estados • Pendiente • En curso • Finalizada • Con error • Cancelada (no se pudo iniciar a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)
Detecciones	Resultado de la búsqueda de IOCs.	• Todos • Sin detecciones • Con detecciones

Tabla 17.7: Herramientas de filtrado

IOCs detectados

Muestra todos los IOCs encontrados en los equipos de la red por todas las tareas de búsqueda de IOCs ejecutadas. Si una tarea identifica un mismo IOC más de una vez en un equipo el listado de IOCs detectados eliminará los resultados duplicados:

Campo	Descripción	Valor
Equipo	Nombre del equipo donde se detectó el IOC.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Tarea	Nombre de la tarea en la que se localizó el IOC.	Cadena de caracteres
Nombre del IOC	Nombre del IOC detectado.	Cadena de caracteres
Fecha de la detección	Fecha en la que se detectó el IOC.	Fecha

Tabla 17.8: Campos del listado IOCs detectados



Para visualizar de forma gráfica los datos del listado accede al widget **IOCs más detectados**.

Campos mostrados en fichero exportado:

Campo	Descripción	Valor
Cliente	Nombre de la cuenta del cliente.	Cadena de caracteres
Tipo de equipo	Clase de dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo en el que se localizó el IOC.	Cadena de caracteres

Campo	Descripción	Valor
Nombre del IOC	Nombre del IOC encontrado.	Cadena de caracteres
Descripción del IOC	Descripción del IOC encontrado en el equipo.	Cadena de caracteres
ID del IOC	Identificador interno del IOC. Coincide con el contenido del campo <code>id</code> del JSON.	Cadena de caracteres
Tarea	Nombre de la tarea que encontró el IOC.	Cadena de caracteres
Fecha	Fecha en la que se ejecutó la tarea de búsqueda de IOCs.	Fecha
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP del equipo en el que se encontró el IOC.	Dirección IP
Dominio	Dominio al que pertenece el equipo en el que se encontró el IOC.	Cadena de caracteres
Descripción	Descripción del IOC encontrado en el equipo.	Cadena de caracteres

Tabla 17.9: Campos de las tablas exportadas

Campos mostrados en el excel de detalle

Campo	Descripción	Valor
Cliente	Nombre de la cuenta del cliente.	Cadena de caracteres
Tipo de equipo	Clase de dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo en el que se localizó el IOC.	Cadena de caracteres

Campo	Descripción	Valor
Nombre del IOC	Nombre del IOC encontrado.	Cadena de caracteres
Descripción del IOC	Descripción del IOC encontrado en el equipo.	Cadena de caracteres
ID del IOC	Identificador interno del IOC. Coincide con el contenido del campo <code>id</code> del JSON.	Cadena de caracteres
Tarea	Nombre de la tarea que encontró el IOC.	Cadena de caracteres
Fecha	Fecha en la que se ejecutó la tarea de búsqueda de IOCs.	Fecha
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Dirección de IP	Dirección IP del equipo en el que se encontró el IOC.	Dirección IP
Dominio	Dominio al que pertenece el equipo en el que se encontró el IOC.	Cadena de caracteres
Descripción	Descripción del IOC encontrado en el equipo.	Cadena de caracteres
Elemento detectado	Identifica los elementos definidos en el IOC que se han encontrado en el equipo.	- Nombre, ruta y hash del fichero - Dirección IP y puerto - Dominio y puerto

Tabla 17.10: Campos mostrados en el excel de detalle

Herramientas de filtrado

Campo	Descripción	Valor
Fechas	Fecha en la que se encontraron los IOCs.	Últimas 24 horas

Campo	Descripción	Valor
		- Últimos 7 días - Último mes - Rango personalizado
Tipo de equipo	Clase de dispositivo donde se encontraron los IOCs.	- Estación - Portátil - Servidor

Tabla 17.11: Filtro de los resultados del listado de detección de IOCs

Ventana IOC detectado

Al hacer clic en una de las filas del listado se mostrará la ventana de **IOC detectado** con información de detalle.

Campo	Descripción	Valores
Nombre	Nombre del IOC encontrado.	Cadena de caracteres
Fecha de detección	Fecha en la que se encontró el IOC.	Fecha
Equipo	Nombre del equipo en el que se encontró el IOC.	Cadena de caracteres
Identificador	Identificador interno del IOC. Coincide con el contenido del campo <code>id</code> del JSON.	Cadena de caracteres
Descripción	Descripción asignada al IOC.	Cadena de caracteres
Pattern (STIX)	Atributo y valor de la definición STIX utilizado para localizar la posible amenaza.	Cadena de caracteres
Fecha de modificación	Fecha en la que se modificó el IOC.	Fecha
Fecha de	Fecha en la que se creó el IOC.	Fecha

Campo	Descripción	Valores
creación		
Elementos detectados	Identifica los elementos definidos en el IOC que se han encontrado en el equipo.	- Nombre, ruta y hash del fichero - Dirección IP y puerto - Dominio y puerto

Tabla 17.12: Campos de la ventana de IOC detectado

Paneles / widgets de IOCs

Acceso al panel de control

Para acceder al panel de control haz clic en el menú superior **Estado**, panel lateral **IOCs**.

Permisos requeridos

Para poder acceder al panel de control de IOCs es necesario tener asignado el permiso **Buscar y administrar IOCs** en el rol de la cuenta de usuario.

Últimas tareas de búsqueda de IOCs

Muestra un listado de las últimas tareas de búsqueda de IOCs creadas. Este widget está formado por varios enlaces que permiten gestionar las tareas de búsqueda de IOCs en la red del cliente:

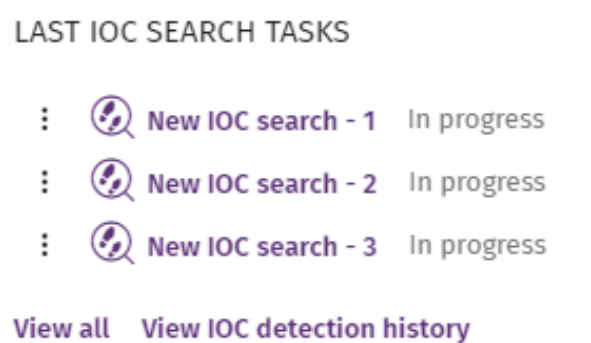


Figura 17.2: Widget de últimas tareas de detección de IOCs

- Haz clic en una tarea para editar su configuración.
- Haz clic en el enlace **Ver todas** para acceder directamente al listado de tareas filtrado por el tipo 'IOC'.

- Haz clic en el enlace **Ver historial de detecciones de IOCs** para acceder al listado **Historial de detecciones** con todas las tareas de detección terminadas con éxito o con error.
- Haz clic en el icono de menú de contexto asociado a cada tarea para ver sus resultados

IOCs más detectados

Muestra una gráfica con los IOCs encontrados en los equipos de la red en el periodo de tiempo establecido. Los resultados se visualizan en una gráfica de estilo Treemap.

DETECTED IOCS TREND

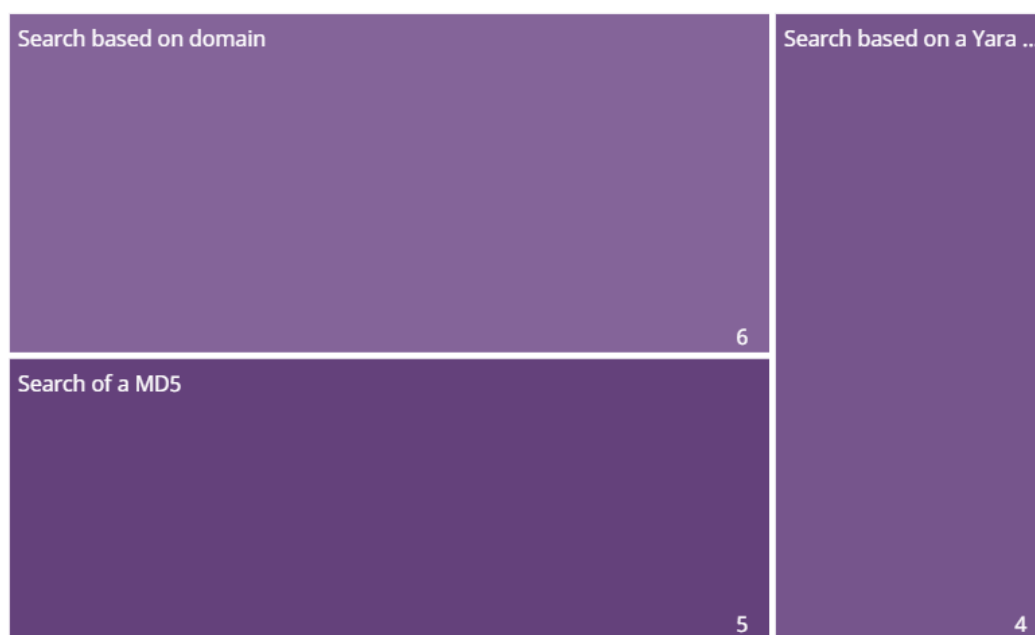


Figura 17.3: Widget IOCs más detectados

Significado de las series:

Serie	Descripción
Nombre del IOC	Nombre del IOC encontrado. El rectángulo cubre una superficie proporcional al número de veces que se ha encontrado el IOC en particular sobre el total de IOCs encontrados en el parque informático del cliente.
Número de detecciones	Suma del número de equipos en los que se ha encontrado cada IOC. Las tareas de búsqueda sólo identifican cada IOC una vez en cada equipo.

Tabla 17.13: Descripción de la serie IOCs más detectados

Filtros preestablecidos del panel:

Al hacer clic en los rectángulos en la figura **Widget de últimas tareas de detección de IOCs** se abre el listado **IOCS detectados** filtrado por el nombre del IOC seleccionado.

Evolución de los IOCs detectados

Muestra una gráfica de líneas con la progresión del número de IOCs detectados en los equipos de la red.

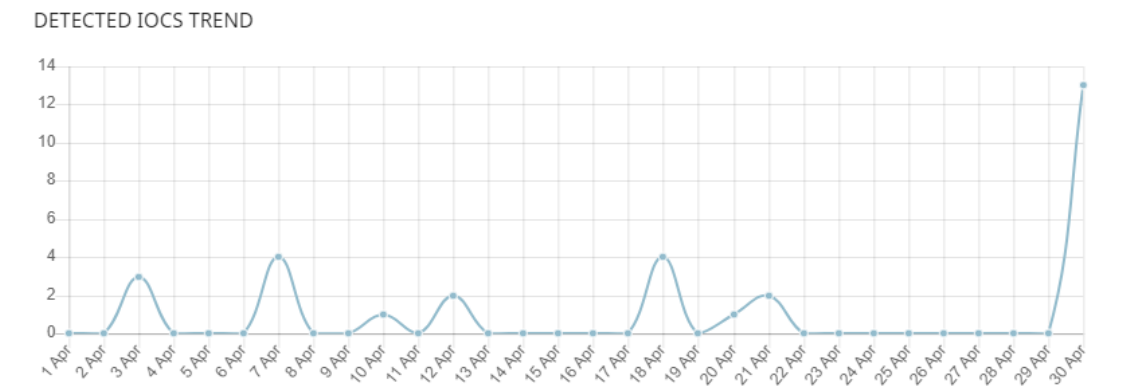


Figura 17.4: Panel Evolución de los IOCs detectados

Significado de las series:

Serie	Descripción
Serie	Representación visual del número de detecciones de IOCs.
Eje Y	Número de IOCs detectados.
Eje X	Fecha de las detecciones de IOCs.

Tabla 17.14: Descripción de la serie de evolución de los IOCs detectados

Filtros preestablecidos del panel

Al hacer clic en los distintos puntos de gráfica mostrada en [Listado de resultados de IOCs encontrados](#) se abre el listado **IOCS detectados** filtrado la fecha seleccionada.

Configuración de indicadores de ataque

En los ataques informáticos dirigidos a las empresas, los hackers tratan de romper las defensas de seguridad mediante el despliegue de múltiples acciones coordinadas entre sí. Estas acciones se distribuyen a lo largo de períodos de tiempo extensos, y utilizan múltiples estrategias y vectores de infección. Muchas de estas acciones aparentan ser inocuas si se observan de forma individual, pero consideradas en su conjunto, pueden ser interpretadas como parte de un ciberataque en curso.

Advanced EDR incluye en su licencia de uso básica un servicio de threat hunting transversal. Este servicio inspecciona el flujo de telemetría enviado por el software de seguridad instalado en los equipos de la red del cliente mediante tecnologías avanzadas de análisis automático, con el objetivo de localizar indicios de ataques en curso. Finalmente, un equipo de especialistas (hunters) criban estos indicios que se representan en la consola del administrador como detecciones de IOAs (Indicator Of Attack).

Un detección de IOA es un indicio que Advanced EDR muestra en la consola del administrador cuando detecta un patrón de eventos susceptible de pertenecer a un ciberataque. Por lo tanto, puede tratarse de un indicador adelantado de infección, que alerta al administrador de la existencia de un ataque en curso, pero también puede representar a una alerta, que muestra un ataque informático que consiguió penetrar en las defensas de la compañía.

Puesto que la existencia de una detección de IOA puede revelar la existencia de un peligro inminente, Advanced EDR facilita la ejecución de una respuesta automática que minimice la superficie de ataque.

Para obtener información adicional sobre los distintos recursos del módulo Identificadores de ataque, consulta las referencias siguientes:



Crear y gestionar configuraciones en la página **258** : información sobre cómo crear, modificar, borrar o asignar configuraciones a los equipos de la red.

La consola de administración en la página **35** : información sobre cómo gestionar las cuentas de usuario y la asignación de permisos.

Gestión de listados en la página **47**: información sobre cómo gestionar listados

Contenido del capítulo

Introducción a los conceptos de IOAs	554
Gestión de detecciones de indicadores de ataque	559
Detección y protección frente ataques RDP	562
Configuración de Indicadores de ataque (IOA)	566
Listados del módulo Indicadores de ataque (IOA)	569
Diagramas de grafos	580
Paneles / widgets del módulo Indicadores de ataque	592

Introducción a los conceptos de IOAs

Esta sección incluye los conceptos que el administrador necesita conocer para comprender los procesos involucrados en la detección de IOAs, y en la ejecución de acciones (automáticas y manuales) de resolución.

Evento

Acción relevante ejecutada por un proceso en el equipo del usuario y monitorizada por Advanced EDR. Los eventos se envían a la nube de Cytomic en tiempo real como parte del flujo de telemetría. Las tecnologías avanzadas de análisis automático, los analistas y threat hunters los analizan en su contexto para determinar si son susceptibles de pertenecer a la cadena CKC de un ataque informático.

Indicio

Secuencia de acciones poco frecuentes encontradas en los eventos generados por los equipos del cliente y que pueden pertenecer a un ataque informático en fase temprana.

Indicador de ataque (IOA)

Es un indicio con alta probabilidad de pertenecer a un ataque informático. Por lo general, se trata de ataques en fase temprana o en fase de explotación. Generalmente, estos ataques no utilizan malware, ya que los atacantes suelen utilizar las propias herramientas del sistema operativo para ejecutarlos y así ocultar su actividad. Se recomienda su contención o resolución con la mayor urgencia posible.

Para facilitar la gestión de detecciones de IOAs, Advanced EDR asocia a cada uno de ellos un estado, modificables de forma manual por el administrador:

- **Pendiente:** la detección está pendiente de investigación y/o resolución. El administrador debe comprobar que el ataque es real y tomar las medidas necesarias para mitigarlo. Todas las detecciones nuevas se crean con el estado pendiente asignado.
- **Archivado:** la detección ya fue investigada por el administrador y las acciones de resolución se completaron, o no fueron necesarias por tratarse de un falso positivo. Por cualquiera de estas razones, el administrador cierra la detección.

Advanced EDR muestra información relevante de la detección, como la táctica y técnica MITRE empleadas, los campos del evento registrado en el equipo que generó la detección y, en caso de estar disponible, los informes siguientes:

- **Investigación avanzada del ataque:** incluye información del equipo involucrado, una descripción detallada de la táctica y técnica utilizadas, recomendaciones para mitigar el ataque y la secuencia de eventos que desencadenó la generación de la detección. Consulta [Campos de la ventana Detalle del IOA](#).
- **Gráfica del ataque:** incluye un diagrama de grafos interactivo con la secuencia de eventos que desencadenó la generación de la detección. Consulta [Diagramas de grafos](#).
- **Investigación:** abre la consola de investigación donde muestra toda la telemetría registrada en el equipo en el momento en que se produce la detección. Para facilitar la búsqueda al administrador, la consola de investigación se posiciona en el último evento que generó la detección del IOA. El administrador puede revisar los eventos generados hasta 5 días antes, los del día de la detección y los ocurridos hasta 1 día después.

Indicadores de ataque avanzados

Los indicadores de ataque avanzados son aquéllos que realizan un seguimiento detallado de las aplicaciones que se ejecutan en los equipos, para detectar comportamientos sospechosos, analizar los eventos generados por las aplicaciones y determinar si constituyen un ataque.

La existencia de una detección de este tipo no implica por sí sola que se esté produciendo un ataque, y por ello es necesario que el administrador del parque informático los analice para determinar su naturaleza.

Advanced EDR muestra información relevante de la detección del IOA avanzado, como la táctica y técnica MITRE empleadas, los campos del evento registrado en el equipo que generó la detección y los informes siguientes:

- **Investigación:** abre la consola de investigación donde muestra toda la telemetría registrada en el equipo en el momento en que se produce la detección. Para facilitar la búsqueda al administrador, la consola de investigación se posiciona en el último evento que generó la detección del IOA avanzado. El administrador puede revisar los eventos generados hasta 5 días antes, los del día de la detección y los ocurridos hasta 1 día después.
- **Actividad:** muestra un listado de los eventos que desencadenaron la detección del IOA avanzado.



Los indicadores de ataque avanzados solo son compatibles con equipos con sistema operativo Windows.

Indicador de ataque avanzado de agrupación

Los indicadores avanzados de agrupación reúnen bajo un mismo nombre varios IOAs que comparten una misma táctica (consulta [Táctica \("Qué"\)](#)). Su comportamiento es idéntico al de un IOA avanzado a todos los efectos, excepto:

- Cuando el administrador consulta los detalles de un IOA de agrupación, la información mostrada hace referencia únicamente a su táctica. Consulta [Información asociada al IOA](#)
- Todos los IOAs que forman un IOA de agrupación comparten la misma táctica. Por esta razón, existen exactamente 14 IOAs avanzados de agrupación, uno por cada táctica disponible en el estándar MITRE.

A continuación, se muestra un listado de todos los IOAS avanzados de agrupación soportados en la consola de administración:

Táctica	Nombre	Descripción	Severidad
TA0001	Initial Access (Acceso inicial)	The adversary is trying to get into your network. (El atacante está intentando entrar en la red).	Medium (Medio)
TA0002	Execution (Ejecución)	The adversary is trying to run malicious code. (El atacante está intentando ejecutar código malicioso).	Medium (Medio)
TA0003	Persistence (Persistencia)	The adversary is trying to maintain their foothold. (El atacante está intentando asegurar que el malware se ejecute cada vez que los equipos se reinician).	Medium (Medio)
TA0004	Privilege Escalation (Escalado de Privilegios)	The adversary is trying to gain higher-level permissions. (El atacante está intentando escalar permisos).	Medium (Medio)
TA0005	Defense Evasion (Defensa y evasión)	The adversary is trying to avoid being detected. (El atacante está intentando ocultar sus acciones).	Medium (Medio)
TA0006	Credential Access	The adversary is trying to steal account	Medium

Táctica	Nombre	Descripción	Severidad
	(Acceso a credenciales)	names and passwords. (El atacante está intentando robar credenciales).	(Medio)
TA0007	Discovery (Descubrimiento)	The adversary is trying to figure out your environment. (El atacante esta intentando descubrir las características de la infraestructura IT).	Medium (Medio)
TA0008	Lateral Movement (Movimiento lateral)	The adversary is trying to move through your environment. (El atacante está intentando moverse a través de la red).	Medium (Medio)
TA0009	Collection (Recolección)	The adversary is trying to gather data of interest to their goal. (El atacante está intentando recopilar datos para conseguir sus fines)	Medium (Medio)
TA0010	Exfiltration (Exfiltración)	The adversary is trying to steal data. (El atacante está intentando robar datos).	Medium (Medio)
TA0011	Command and Control (Comando y control)	The adversary is trying to communicate with compromised systems to control them. (El atacante está intentando comunicarse con los equipos comprometidos para controlarlos).	Medium (Medio)
TA0012	Impact (Impacto)	The adversary is trying to manipulate, interrupt, or destroy your systems and data. (El atacante está intentando manipular, parar o destruir equipos y datos).	Medium (Medio)
TA0013	Resource Development (Desarrollo de recursos)	The adversary is trying to establish resources they can use to support operations. (El atacante está intentando preparar recursos que le faciliten sus operaciones futuras).	Medium (Medio)
TA0014	Reconnaissance	The adversary is trying to gather	Medium

Táctica	Nombre	Descripción	Severidad
	(Exploración)	information they can use to plan future operations. (El atacante está intentando recopilar información para utilizar en acciones futuras).	(Medio)

Tabla 18.1: Listado de Indicadores de ataque avanzados de agrupación disponibles

Compatibilidad de los IOAs avanzados con soluciones de seguridad de terceros

Cyatomic sigue todas las recomendaciones de los fabricantes de sistemas operativos para asegurarse de que sus productos de seguridad coexisten en el equipo del cliente sin problemas con otras soluciones antivirus y EDR. No obstante, la implementación de los IOAs avanzados se realiza mediante hooks. Si existen varias soluciones de seguridad instaladas en el equipo que utilizan esta tecnología de interceptación, es posible que sean incompatibles. Para evitar posibles problemas, desactiva todas las tecnologías basadas en hooks del producto de seguridad en el equipo del usuario.

Las tecnologías que utilizan hooks en Advanced EDR son:

- Anti - exploit. Consulta [Anti-exploit](#) en la página **302**
- Inyección avanzada de código. Consulta [Anti-exploit](#) en la página **302**
- IOAs avanzados

CKC (Cyber Kill Chain)

La empresa Lockheed-Martin describió en 2011 un marco o modelo para defender las redes informáticas, en el que se afirmaba que los ciberataques ocurren en fases y cada una de ellas puede ser interrumpida a través de controles establecidos. Desde entonces, la Cyber Kill Chain ha sido adoptada por organizaciones de seguridad de datos para definir las fases de los ciberataques. Estas fases abarcan desde el reconocimiento remoto de los activos del objetivo hasta la exfiltración de datos.

Mitre corp.

Empresa sin ánimo de lucro que opera en múltiples centros de investigación y desarrollo financiados con fondos federales dedicados a abordar problemas relativos a la seguridad. Ofrecen soluciones prácticas en los ámbitos de defensa e inteligencia, aviación, sistemas civiles, seguridad nacional, judicatura, salud y ciberseguridad. Son los creadores del framework ATT&CK.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

Conjunto de recursos desarrollados por la empresa Mitre Corp. para describir y categorizar los comportamientos peligrosos de los ciberdelincuentes, basados en observaciones a lo largo de todo el mundo. ATT&CK es una lista ordenada de comportamientos conocidos de los atacantes, separados en tácticas y técnicas, y que se expresan a través de una matriz. Ya que esta lista es una representación completa de los comportamientos que los hackers reproducen cuando se infiltran en las redes de las

empresas, es un recurso útil para desarrollar mecanismos tanto defensivos como preventivos y resolutivos por parte de las organizaciones. Para más información sobre el framework ATT&CK consulta <https://attack.mitre.org/>.

Técnica (“Cómo”)

En terminología ATT&CK, las técnicas representan la forma o la estrategia con la que un adversario logra un objetivo táctico. Es decir, el “cómo”. Por ejemplo, un adversario, para lograr el objetivo de acceder a algunas credenciales (táctica) realiza un volcado de las mismas (técnica).

Subtécnica (“Cómo”)

En terminología ATT&CK, una subtécnica describe un "cómo" para una técnica particular. Es un proceso o mecanismo para lograr el objetivo de una táctica. Por ejemplo, el Password Spraying es un tipo de ataque de fuerza bruta para lograr el Credential Access.

Táctica (“Qué”)

En terminología ATT&CK, las tácticas representan el motivo u objetivo final de una técnica. Es el objetivo táctico del adversario: la razón para realizar una acción.

Gestión de detecciones de indicadores de ataque



Para crear, modificar o borrar configuraciones o recursos asociados a los indicadores de ataque, la cuenta de usuario que accede a la consola de Advanced EDR requiere el permiso Configurar indicadores de ataque (IOA). Para listar configuraciones o recursos asociados a los indicadores de ataque se requiere el permiso Ver configuración de indicadores de ataque (IOA). Consulta [Gestión de roles y permisos](#) en la página 67.

Advanced EDR te permite gestionar las detecciones de indicadores de ataque y mostrar los equipos de la red donde se detectaron:

- [Mostrar las detecciones de IOAs en el parque](#)
- [Buscar los equipos con detecciones de un tipo de IOA](#)
- [Buscar las detecciones de IOAs en un equipo](#)
- [Buscar equipos y detecciones de IOAs relacionados](#)
- [Archivar una o varias detecciones de IOAs](#)
- [Marcar detecciones de IOAs como pendientes](#)
- [Mostrar el detalle de una detección de IOA y las recomendaciones](#)

Mostrar las detecciones de IOAs en el parque

- Selecciona el menú superior **Estado**, panel lateral **Indicadores de ataque (IOA)**.
- En la parte superior de la ventana indica el intervalo de datos a mostrar.
- El widget **Servicio Threat Hunting** contiene los eventos, indicios e indicadores de ataque detectados en el intervalo elegido.
- Haz clic en el área **Indicadores de ataque**. Se abrirá el listado **Indicadores de ataque (IOA)** que muestra todas las detecciones en el intervalo de tiempo seleccionado.

Para más información sobre este widget, consulta [Servicio Threat Hunting](#).

Buscar los equipos con detecciones de un tipo de IOA

- Selecciona el menú superior **Estado**, panel lateral **Indicadores de ataque (IOA)**.
- Haz clic en el tipo de indicador de ataque en el panel **Indicadores de ataque (IOA) detectados** o en **Indicadores de ataque situados en la matriz de MITRE ATT&CK**.
- Haz clic en el tipo de indicado de ataque. Se abrirá el listado **Indicadores de ataque (IOA)** filtrado por tipo de ataque configurado.

Para más información sobre estos widgets, consulta [Indicadores de ataque situados en la matriz de MITRE ATT&CK](#) y [Indicadores de ataque \(IOA\)](#).

Buscar las detecciones de IOAs en un equipo

- Haz clic en el menú superior **Estado**, panel lateral **Indicadores de ataque (IOA)**.
- Haz clic en el equipo apropiado del panel **Indicadores de ataque (IOA) por equipo**. Se abrirá el listado **Indicadores de ataque (IOA)** con el filtro por equipo configurado.

Para más información sobre este widget, consulta [Indicadores de ataque \(IOA\) por equipo](#).

Buscar equipos y detecciones de IOAs relacionados

- En el menú superior selecciona **Estado**.
- En el panel izquierdo haz clic en **Añadir**. Se mostrará una ventana con los listados disponibles.
- En la sección **Seguridad**, selecciona **Indicadores de seguridad (IOA)**. Se abrirá la ventana **Nuevo listado de Indicadores de ataque (IOA)**.
- Cada detección mostrada en el listado **Indicadores de ataque (IOA)** tiene asociado un menú de contexto con las opciones:
 - **Visualizar los IOAs detectados en el equipo** : muestra el listado **Indicadores de ataque (IOA)** filtrado por el campo **Equipo**.

- **Visualizar equipos con el IOA detectado** : muestra el listado **Indicadores de ataque (IOA)** filtrado por el campo **Indicador de ataque**.

Para más información acerca de los listados, consulta [Listados del módulo Indicadores de ataque \(IOA\)](#).

Archivar una o varias detecciones de IOAs

Cuando la causa que motivó la detección ha sido resuelta, o cuando se ha comprobado que se trataba de un falso positivo, el administrador puede archivarla:

- Selecciona el menú superior **Estado** y haz clic en el enlace **Añadir** del panel lateral **Mis listados**. Se mostrará la ventana **Abrir listado** con las plantillas disponibles.
- En la sección **Seguridad** haz clic en la plantilla **Indicadores de ataque (IOA)**. Se mostrará el listado de IOAs detectados sin filtros configurados.
- Configura los filtros necesarios y haz clic en el botón **Filtrar**.
- Haz clic en el menú de contexto asociado al indicador a archivar y selecciona la opción **Archivar IOA** . El indicador de ataque pasará a estado **Archivado**.

O bien:

- Selecciona las casillas asociadas a las detecciones a archivar.
- En la barra de herramientas, haz clic en el icono **Archivar IOA** . Las detecciones pasarán a estado **Archivado**.

Marcar detecciones de IOAs como pendientes

Advanced EDR añade las detecciones como pendientes para indicar al administrador que es necesaria su revisión. El propio administrador también puede marcar como pendiente una detección previamente archivada, cuando la causa que la motivó no fue resuelta completamente.

- Selecciona el menú superior **Estado** y haz clic en el enlace **Añadir** del panel lateral **Mis listados**. Se abrirá la ventana **Abrir listado** con las plantillas disponibles.
- En la sección **Seguridad**, haz clic en la plantilla **Indicadores de ataque (IOA)**. Se mostrará el listado sin filtros configurados.
- Configura los filtros necesarios y haz clic en el botón **Filtrar**.
- Haz clic en el menú de contexto asociado a la detección que quieres investigar y selecciona la opción **Marcar IOA como pendiente** . El Indicador de ataque pasará a estado **Pendiente**.

O bien:

- Haz clic en las casillas de selección asociadas a las detecciones que quieres investigar.
- En la barra de herramientas haz clic en la opción **Marcar IOA como pendiente** . Las detecciones pasarán a estado **Pendiente**.

Mostrar el detalle de una detección de IOA y las recomendaciones

- Selecciona el menú superior **Estado** y en el enlace **Añadir** del panel lateral **Mis listados**. Se abrirá la ventana **Abrir listado** con las plantillas disponibles.
- En la sección **Seguridad** haz clic en la plantilla **Indicadores de ataque (IOA)**. Se mostrará el listado sin filtros configurados.
- Configura los filtros necesarios y haz clic en el botón **Filtrar**.
- Haz clic en un indicador de ataque del listado. Se abrirá la ventana de detalle. Consulta [Ventana de detalle](#).

Detección y protección frente ataques RDP

Dentro de los ataques informáticos recibidos en la compañías, los servicios de escritorio remoto son los más frecuentemente utilizados mediante fuerza bruta, si éstos se encuentran expuestos directamente a la red Internet. Advanced EDR detecta y protege los equipos de la red frente a ataques que utilizan el protocolo RDP (Remote Desktop Protocol) como vector de infección.

Mediante el protocolo RDP, los usuarios conectan con equipos remotos y ejecutan procesos que les permiten utilizar los recursos del equipo destino. En el caso de usuarios no legítimos, este protocolo también puede ser utilizado para facilitar los desplazamientos laterales dentro de la red de la corporativa y acceder a otros recursos dentro de la infraestructura IT.

Al activar la configuración Ataque por fuerza bruta al RDP / Credenciales comprometidas tras ataque por fuerza bruta (consulta [Activar y modificar la detección de IOAs](#) en la página 567), Advanced EDR ejecuta las acciones siguientes:

- Registra en cada equipo protegido los intentos de acceso remoto por RDP recibidos en las últimas 24 horas, cuyo origen se encuentra fuera de la red del cliente.
- Evalúa si el equipo está siendo sometido a un ataque por fuerza bruta a través de RDP.
- Detecta si alguna de las cuentas del equipo ya ha sido vulnerada para acceder a los recursos del equipo.
- Bloquea las conexiones RDP para mitigar el ataque.

Detección de IOA asociado a un ataque RDP

Advanced EDR muestra la detección **Ataque por fuerza bruta al RDP** cuando detecta un patrón de ataque mediante el protocolo RDP. En esta situación, el equipo ha recibido un gran volumen de conexiones RDP

que intentan iniciar una sesión remota, pero que han terminado en fracaso por no contar con credenciales válidas.

Modos de contención RDP

Modo de Contención de ataque RDP inicial

Cuando un equipo protegido por Advanced EDR recibe una gran cantidad de intentos de conexión por RDP erróneos por carecer de credenciales válidas, el software de protección genera el IOA **Ataque por fuerza bruta al RDP** y configura el equipo en modo **Contención de ataque RDP inicial**. En este modo se bloquea el acceso por RDP al equipo desde aquellas IPs externas a la red del cliente que han tenido un mayor volumen de intentos de conexión durante las 24 últimas horas. Para permitir el acceso de una o varias de estas IPs, utiliza la lista **IPs de confianza** de la configuración **Indicadores de ataque IOA**. Consulta [IPs de confianza](#).

Modo de Contención de ataque RDP restrictivo

Se activa cuando un equipo protegido por Advanced EDR que ya se encuentra en el modo **Contención de ataque RDP inicial** registra un inicio de sesión correcto con una cuenta que anteriormente registró errores por falta de credenciales válidas. En este momento, el software de protección genera el IOA **Credenciales comprometidas tras ataque por fuerza bruta al RDP** y se considera que la cuenta ha sido vulnerada. Como mecanismo de mitigación, se bloquean todas las conexiones RDP desde el exterior que hayan intentado conectar por lo menos una vez con el equipo atacado en las 24 horas anteriores.

Configurar la respuesta a un ataque RDP

Cuando Advanced EDR detecta un ataque o una intrusión RDP, tiene dos opciones de respuesta: informar únicamente, o informar y proteger al equipo del ataque.

Para configurar la respuesta a un ataque RDP:

- En la configuración **Indicadores de ataque** asignada al equipo, haz clic en el enlace **Configuración avanzada** de la sección **Ataque por fuerza bruta al RDP / Credenciales comprometidas tras ataque por fuerza bruta**. Se mostrarán las opciones de configuración asociadas a este tipo de IOA.
- Establece la opción adecuada en **Respuesta en estación** y / o **Respuesta en servidores**:
 - **Informar y bloquear ataques RDP**: Advanced EDR muestra en la consola la detección **Ataque por fuerza bruta al RDP** y además establece el modo de contención apropiado para el equipo atacado.
 - **Solo informar**: Advanced EDR solo muestra en la consola la detección **Ataque por fuerza bruta al RDP**.

Para obtener más información consulta [Opciones de configuración de Indicadores de ataque \(IOA\)](#).

Localizar los equipos de la red en modo Contención de ataque RDP

La consola localiza los equipos en modo contención mediante los recursos siguientes:

- Con la serie **XX Equipos en modo contención de ataque RDP** en el widget **Servicio Threat Hunting**. Consulta [Servicio Threat Hunting](#).
- Con los filtros del listado **Estado de protección de los equipos**. Consulta [Estado de protección de los equipos](#) en la página 621.
- En el listado exportado de **Estado de protección de los equipos**. Consulta [Estado de protección de los equipos](#) en la página 621.
- Con un filtro en el árbol de equipos. Consulta [Equipos en modo Contención de ataque RDP](#) en la página 187.

Visualizar el estado de contención de los equipos

La consola muestra el estado de contención de los equipos en los recursos siguientes:

- En el listado **Estado de protección de los equipos**: mediante el icono . Consulta [Estado de protección de los equipos](#) en la página 621.
- En el listado exportado de **Estado de protección de los equipos**: en la columna **Modo “Contención de ataque RDP”**. Consulta [Estado de protección de los equipos](#) en la página 621.
- En el listado **Estado de cifrado**: mediante el icono . Consulta [Estado del cifrado](#) en la página 506.
- En el listado exportado de **Estado de cifrado**: en la columna **Modo “Contención de ataque RDP”**. Consulta [Estado del cifrado](#) en la página 506.
- En el listado **Estado de gestión de parches**: mediante el icono . Consulta [Estado de gestión de parches](#) en la página 418.
- En el listado exportado de **Estado de gestión de parches**: en la columna **Modo “Contención de ataque RDP”**. Consulta [Estado de gestión de parches](#) en la página 418.
- En el listado **Estado de Data Control**: mediante el icono . Consulta [Estado de Cytomic Data Watch](#) en la página 350.
- En el listado exportado de **Estado de Data Control**: en la columna **Modo “Contención de ataque RDP”**. Consulta [Estado de Cytomic Data Watch](#) en la página 350.
- En el **Listado de equipos**: mediante el icono . Consulta [Listado de equipos](#) en la página 194.
- En el **Listado exportado de equipos**: en la columna **Modo “Contención de ataque RDP”**. Consulta [Listado de equipos](#) en la página 194.
- En el **Listado de Indicadores de ataque (IOA)**: en la columna **Acción**. Consulta [Indicadores de ataque \(IOA\)](#).

- En el listado exportado de **Listado de Indicadores de ataque (IOA)**: en la columna **Acción**. Consulta [Indicadores de ataque \(IOA\)](#).
- En la alertas de la ventana **Información del equipo**. Consulta [Equipo en estado de contención](#) en la página [221](#).
- En la ventana **Detalle del IOA**: en el campo **Equipo**. Consulta [Ventana de detalle](#).

Finalización automática del estado de Contención de ataque RDP

A las 24 horas del inicio del estado de contención, Advanced EDR evalúa el volumen de intentos de conexión por RDP. Si se mantiene por debajo de ciertos umbrales, se retira el estado de contención, si no es así, se extiende durante 24 horas más.

Las IPs bloqueadas en el modo de contención continuarán bloqueadas aunque haya finalizado el ataque RDP. De esta manera, con el paso del tiempo, el software de seguridad aprende las IPs que los cibercriminales utilizan para atacar la red del cliente y, cuando todas ellas hayan sido bloqueadas, el ataque quedará sin efecto y ya no será necesario mantener el modo de contención.

Finalizar manualmente el estado de Contención de ataque RDP

Si el administrador considera que su red ha sido asegurada y ya no existe peligro de ataques por RDP, puede revertir el bloqueo de forma manual:

- Desde los listados indicados en [Visualizar el estado de contención de los equipos](#):
 - Abre uno de los listados y selecciona las casillas asociadas a los equipos. Se muestra la barra de herramientas.
 - Haz clic en el icono **Finalizar el modo Contención de ataque RDP** .

O bien:

- Haz clic en el menú de contexto situado a la derecha del equipo. Se muestra un desplegable con las opciones disponibles.
- Selecciona la opción **Finalizar el modo Contención de ataque RDP** .
- Desde la ventana de información del equipo:
 - Abre uno de los listados indicados en [Visualizar el estado de contención de los equipos](#) y haz clic en el equipo. Se mostrará la ventana de **Información de equipo**.
 - Haz clic en el botón **Finalizar modo "Contención de ataque RDP"**.

Una vez iniciado el proceso de finalización manual del modo de contención, la consola de administración envía el comando de forma inmediata a los equipos involucrados. En función de si el equipo es accesible y de si está disponible la funcionalidad de tiempo real, la acción se ejecutará en el momento, o el equipo pasará al estado **Finalizando el modo de contención RDP**, en cuyo caso mostrará:

- Un icono parpadeante en  los listados indicados en **Visualizar el estado de contención de los equipos**.
- Un mensaje de advertencia en la ventana de **Información del equipo**.
- Un mensaje de advertencia en la ventana de **Detalle del IOA**.



Consulta *Configuración de la comunicación en tiempo real* en la página 281.

Se considera que el equipo continua en estado de contención hasta que el comando no es aplicado de forma correcta. Si se produce un problema, se vuelve a intentar cada 4 horas durante los siguientes 7 días. Si la acción no se completa, la consola vuelve a mostrar el estado **Contención de ataque RDP**.

Una vez finalizado de forma manual el estado de contención, Advanced EDR ejecuta las acciones siguientes:

- Libera todas las IPs registradas y bloqueados en el equipo, y deja la tecnología como si no hubiera sido utilizada previamente.
- El equipo deja de bloquear conexiones RDP.



Si el software de seguridad determina de forma automática que el equipo ya no esta bajo un ataque de tipo RDP, finalizará el estado de contención pero no liberará las IPs registradas ni, por lo tanto, dejará de bloquearlas.

Configuración de Indicadores de ataque (IOA)

Acceso a la configuración

- Selecciona el menú superior **Configuración**, menú lateral **Indicadores de ataque (IOA)**.
- Haz clic en el botón **Añadir**. Se muestra la ventana **Añadir configuración**.



Las configuraciones de Indicadores de ataque (IOA) se pueden asignar a puestos de trabajo o servidores Windows, Linux y macOS.

Permisos requeridos

Permiso	Tipo de accesos
Configurar indicadores de ataque (IOA)	Crear, modificar, borrar, copiar o asignar las configuraciones de Indicadores de ataque (IOA).
Ver configuración de indicadores de ataque (IOA)	Visualizar las configuraciones de Indicadores de ataque (IOA).

Tabla 18.2: Permisos requeridos para acceder a la configuración Indicadores de ataque (IOA)

Activar y modificar la detección de IOAs

Por defecto, Advanced EDR asigna una configuración de tipo Indicadores de ataque (IOA) a todos los equipos gestionados de la red, con todos los tipos de IOA activados por defecto. Para desactivar la detección de un tipo de IOA específico:

- Selecciona el menú superior **Configuración**, menú lateral **Indicadores de ataque (IOA)**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración de **Añadir configuración**
- Selecciona los IOAs que Advanced EDR buscará en el flujo de telemetría generado por los equipos.

Para poder seleccionar indicadores de ataque avanzados concretos, es necesario activarlos todos. Para ello, desplaza el control deslizante.

- Selecciona los equipos que recibirán la nueva configuración y haz clic en el botón **Guardar**

Para más información sobre cómo gestionar configuraciones, consulta [Gestión de configuraciones](#) en la página 251.

Opciones de configuración de Indicadores de ataque (IOA)

Para activar o desactivar los IOAs que quieres monitorizar, usa el control deslizante correspondiente:

Campo	Descripción
Ataque por fuerza bruta al RDP Credenciales comprometidas tras ataque por fuerza bruta al RDP	Detecta volúmenes grandes de intentos de inicio de sesión remota a través del protocolo RDP.
Resto de IOAs	Cyatomic actualiza de forma periódica la lista de indicadores de ataque para reflejar las estrategias de nueva aparición empleadas por los ciberdelincuentes.

Campo	Descripción
Indicadores de ataque avanzados	Lista de los indicadores de ataque avanzados seleccionados para su búsqueda en los equipos de usuario y servidores. Disponible solo para equipos Windows.

Tabla 18.3: Tipos de indicios disponibles en una configuración de Indicadores de ataque (IOA)

Activar y desactivar la tecnología de IOAs avanzados

La generación de IOAs avanzados emplea tecnologías nuevas y recopila una mayor cantidad de telemetría de los dispositivos. En servidores con múltiples usuarios y en situaciones específicas, puede afectar el rendimiento del dispositivo. Para desactivar esta tecnología por completo, utiliza el control deslizante **IOAs avanzados**.



Desactivar IOAs avanzados de forma individual no desactiva la tecnología y no mejora sustancialmente el rendimiento.

Información asociada al IOA

En la lista de **Indicadores de ataque y comportamiento**, haz clic en el icono ⓘ situado junto al nombre de cada elemento. Se mostrará información sobre el IOA (nombre, riesgo, descripción, recomendaciones, MITRE...). Para más información, consulta [Campos de la ventana Detalle del IOA](#).

Respuesta automática para ataques RDP

Campo	Descripción
Respuesta en estaciones	• Informar y bloquear ataques RDP: genera un IOA y bloquea los ataques RDP. Consulta Detección y protección frente ataques RDP. • Solo informar: genera un IOAs.
Respuesta en servidores	• Informar y bloquear ataques RDP: genera un IOAs y bloquea los ataques RDP. Consulta Detección y protección frente ataques RDP. • Solo informar: genera un IOAs.

Tabla 18.4: Acciones de respuesta automática para IOAs de tipo RDP

IPs de confianza

Escribe la lista de IPs de los equipos que consideras seguros. Las conexiones RDP cuyo origen figura en la lista, no son bloqueadas, pero generan indicios en los paneles de control de Indicadores de ataque (IOA).

Utiliza comas para separar IPs individuales y guiones para separar rangos de IPs.

Listados del módulo Indicadores de ataque (IOA)

Acceso a los listados

Accede a los listados siguiendo dos rutas:

- En el menú superior **Estado**, haz clic en el panel de la izquierda **Indicadores de ataque** y en el widget relacionado.

O bien:

- En el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.
- En la sección **Seguridad**, selecciona el listado **Indicadores de ataque (IOA)** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

Permiso	Acceso a listados
Visualizar detecciones y amenazas	Indicadores de ataque (IOA)

Tabla 18.5: Permisos requeridos para acceder a los listados de Indicadores de ataque (IOA)

Indicadores de ataque (IOA)

Muestra el detalle de los IOAs detectados por Advanced EDR en los equipos de usuario y servidores. La generación de detecciones cumple las reglas siguientes:

- Cada detección hace referencia a un único equipo y a un tipo de IOA. Si se produce la misma cadena de eventos sospechosos en varios equipos, se genera una detección independiente para cada equipo.
- Si la tripla patrón - equipo - tipo se detecta varias veces, las detecciones se agruparán, indicando el número de repeticiones en el campo **Ocurrencias**. Para obtener más información sobre el algoritmo de agrupación consulta [Agrupación de detecciones generadas por IOAs](#).

Campo	Comentario	Valores
Equipo	Nombre del equipo con el IOA detectado.	Cadena de caracteres

Campo	Comentario	Valores
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Indicador de ataque	Nombre de la regla interna que detecta el patrón de eventos que genera la detección.	Cadena de caracteres
Ocurrencias	Número de veces que se repite la detección. Para conocer el algoritmo de agrupación que aplica en cada caso consulta Agrupación de detecciones generadas por IOAs .	Número
Riesgo	Importancia del impacto del IOA detectado: • Crítico • Alto • Medio • Bajo • Desconocido	Enumeración
Acción	Tipo de acción ejecutada por Advanced EDR en los IOAs Ataque por fuerza bruta al RDP: • Informado • Ataque bloqueado Consulta Respuesta automática para ataques RDP .	Enumeración
Estado	• Archivado: la detección ya no requiere atención por parte del administrador al tratarse de un falso positivo o por haberse completado las tareas de resolución. • Pendiente: la detección no ha sido investigada por el administrador. Consulta Indicadores de ataque (IOA) .	Enumeración
Fecha	Fecha y hora en la que se detectó por última vez el IOA.	Fecha

Tabla 18.6: Campos del listado Indicadores de ataque (IOA)

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Indicador de ataque	Nombre de la regla que detecta el patrón de eventos que genera la detección.	Cadena de caracteres
Ocurrencias	Número de veces que se repite la detección. Para conocer el algoritmo de agrupación que aplica en cada caso consulta Agrupación de detecciones generadas por IOAs .	Número
Riesgo	Importancia del impacto del IOA detectado: • Crítico • Alto • Medio • Bajo • Desconocido	Enumeración
Acción	Tipo de acción ejecutada por Advanced EDR: • Informado • Ataque bloqueado Consulta Respuesta automática para ataques RDP .	Enumeración
Estado	• Archivado: la detección ya no requiere atención por parte del administrador al tratarse de un falso positivo o por haberse completado las tareas de resolución. • Pendiente: la detección no ha sido investigado por el administrador. Consulta Indicadores de ataque (IOA) .	Enumeración
Fecha	Fecha y hora en la que se detectó por última vez el IOA.	Fecha
Fecha de archivado	Fecha de la última vez que se archivó la detección.	Fecha
Tiempo hasta el archivado	Tiempo que ha transcurrido desde que se detectó el IOA hasta que el administrador pudo verificar su validez y desarrollar las labores de resolución en caso de ser	Fecha

Campo	Comentario	Valores
	necesarias.	
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción breve de las estrategias empleadas por el atacante.	Cadena de caracteres

Tabla 18.7: Campos del fichero exportado Indicadores de ataque (IOA)

Herramienta de filtrado

Campo	Descripción	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Riesgo	Importancia del impacto del IOA detectado: • Crítico • Alto • Medio • Bajo • Desconocido	Enumeración
Acción	Tipo de acción ejecutada por Advanced EDR: • Informado • Ataque bloqueado Consulta Respuesta automática para ataques RDP .	Enumeración
Táctica	Categoría de la táctica de ataque que generó la detección,	Cadena de

Campo	Descripción	Valores
	mapeado según la especificación MITRE. Para localizar rápidamente una táctica concreta, escribe los términos a buscar en la caja de texto situada bajo el desplegable. Haz clic en el icono  y selecciona la táctica por la que quieres filtrar.	caracteres
Fechas	Intervalo de fechas en el que se ha producido la detección.	- Últimas 24 horas - Últimos 7 días - Último mes
Estado	Indica el estado en el que se encuentra la detección.	- Pendiente - Archivado
Indicador de ataque	Nombre del IOA que generó las detecciones a buscar. Para localizar rápidamente detecciones generadas por un IOA concreto, escribe los términos a buscar en la caja de texto situada bajo el desplegable. Haz clic en el icono  y selecciona el IOA por el que quieres filtrar.	Cadena de caracteres
Técnica	Categoría de la técnica o subtécnica de ataque que generó el IOA, mapeado según la especificación MITRE. - Al filtrar por una técnica, se muestran las detecciones generadas por los IOAs que tienen esa técnica asociada o alguna de sus sub técnicas. - Al filtrar por una subtécnica, se muestran las detecciones generadas por los IOAs que tienen asociada esa subtécnica en concreto . Las técnicas se identifican por una cadena de caracteres con el formato TXXXX. Las sub técnicas se identifican por una cadena de caracteres con el formato TXXXX.YYY. Para localizar rápidamente una técnica concreta, escribe los términos a buscar en la caja de texto situada bajo el	Cadena de caracteres

Campo	Descripción	Valores
	desplegable. Haz clic en el icono  y selecciona la técnica por la que quieres filtrar.	

Tabla 18.8: Campos de filtrado para el listado Indicadores de ataque (IOA)

Ventana de detalle

Haz clic en uno de los elementos del listado para mostrar la ventana de detalle. Incluye una descripción detallada del cuándo y dónde se produjo la detección, así como el detalle del patrón de eventos registrado que motivó su aparición.

En los IOAs Avanzados se añade la pestaña **Actividad** donde se muestran todos los eventos que forman parte del posible ataque.

Campo	Comentario	Valores
Estado	Estado de la detección y fecha de la asignación del estado.	• Pendiente • Archivado
Fecha de detección	Fecha y hora en la que se detectó por última vez el IOA.	Fecha
Indicador de ataque (IOA)	Nombre de la regla que detecta el patrón de eventos que genera la detección.	Cadena de caracteres
Riesgo	Importancia del impacto del IOA detectado: • Crítico • Alto • Medio • Bajo • Desconocido	Enumeración
Descripción	Detalle de la cadena de eventos detectada en el equipo del cliente, y de las consecuencias que puede tener en el caso de que el ataque cumpla sus objetivos.	Cadena de caracteres
Investigación avanzada	Informe con el detalle completo del IOA que generó	Botón

Campo	Comentario	Valores
del ataque (no disponible en IOAs avanzados)	la detección: - Identificador del equipo y fecha. - Nombre del tipo de IOA detectado. - Descripción detallada del funcionamiento interno del IOA que generó la detección, con el mapeo a la táctica y técnica MITRE utilizadas. - Herramientas del sistema operativo utilizadas en el ataque. - Detalle del equipo. - Criticidad del ataque. - Estado del equipo con respecto al ataque. - Estado de la evolución del ataque. - Usuarios logueados en el momento del ataque. - IPs / URLs accedidas. - Historial de repeticiones diarias del ataque. - Grafo de ejecución de la cadena de procesos involucrados en el ataque. - Consejos para mitigar o resolver el ataque. Los informes tienen una duración de un mes desde la generación de la detección, transcurrido el cual dejarán de estar accesibles. A su vez, un informe muestra los eventos que forman parte del ataque en el intervalo de los 30 días anteriores a la detección del IOA.	
Ver gráfica del ataque (no disponible en IOAs avanzados)	Grafo interactivo con la secuencia de procesos que generó la detección. Consulta Diagramas de grafos.	Botón
Acción	Tipo de acción ejecutada por Advanced EDR: - Informado - Ataque bloqueado Consulta Respuesta automática para ataques	Enumeración

Campo	Comentario	Valores
	RDP.	
Recomendaciones	Acciones de resolución recomendadas por Cytomic para el administrador de la red.	Cadena de caracteres

Tabla 18.9: Campos de la ventana Detalle del IOA

Pestaña detalles

Campo	Comentario	Valores
Equipo	Nombre y grupo del equipo afectado. Si el equipo se encuentra en modo contención, se añade el botón Finalizar modo "Contención de ataque RDP" . Consulta Finalizar manualmente el estado de Contención de ataque RDP .	Cadena de caracteres
Ocurrencias detectadas	Número de veces que se repite el IOA . Para conocer el algoritmo de agrupación que aplica en cada caso consulta Agrupación de detecciones generadas por IOAs .	Número
Último evento	Fecha en la que se ha producido el evento que desencadenó el IOA en el equipo.	Fecha
Ver detalle de actividad completo	Disponible en IOAs avanzados. Consulta Pestaña Actividad .	
Ver investigación del equipo	Consulta Pestaña Investigación .	
Otros detalles	JSON con los campos relevantes del evento que desencadenó la generación del IOA. Consulta Formato de los eventos recogidos en la telemetría en la página 867.	Cadena de caracteres
Táctica	Categoría de la táctica del ataque que generó el IOA, mapeado según la especificación MITRE.	Cadena de caracteres
Técnica	Categoría de la técnica del ataque que generó el IOA, mapeado según la especificación MITRE. Se identifican por una cadena de caracteres con el formato TXXXX.	Cadena de caracteres

Campo	Comentario	Valores
Subtécnica	Categoría de la subtécnica del ataque que generó el IOA, mapeado según la especificación MITRE. Se identifican por una cadena de caracteres con el formato TXXXX.YYY.	Cadena de caracteres
Plataforma	Sistemas operativos y entornos donde MITRE ha registrado el tipo de ataque.	Cadena de caracteres
Descripción	Detalle de la táctica y técnica empleadas por el IOA detectado, según la matriz de MITRE.	Cadena de caracteres

Tabla 18.10: Campos de la ventana Detalle del IOA

Pestaña Actividad

La ventana de detalle de un IOA Avanzado tiene una pestaña adicional **Actividad** donde se muestra un listado con todos los eventos que desencadenaron la detección. De esta forma, el administrador puede comprobar la secuencia de pasos ejecutada por el software malicioso y confirmar o desestimar el ataque.

Campo	Comentario	Valores
Buscar	Filtra el listado buscando por el contenido de los campos Fecha y Acción. Soporta búsquedas parciales de cadenas de caracteres.	
Fecha	Fecha en la que se registro el evento.	Fecha
Acción	Resumen de los detalles del evento. Para obtener toda la información haz clic en el evento.	Cadena de caracteres
Exportar 	Exporta en un fichero Excel el listado de eventos mostrado en la consola.	

Tabla 18.11: Campos de la pestaña Actividad

Al hacer clic en un evento se desplegará el panel lateral **Detalles del evento** con dos pestañas:

- **Detalles:** muestra los campos del evento y su contenido. Para conocer el significado de cada campo consulta [Formato de los eventos recogidos en la telemetría](#) en la página 867.
- **MITRE:** muestra la táctica, técnica y subtécnica asociada al evento, así como su descripción. Si el IOA Avanzado está asociado a más de una técnica, el panel MITRE agrupa la información en varios desplegables, uno por cada técnica. Toda la información de la pestaña MITRE se recoge de la fuente oficial accesible en la dirección web <https://attack.mitre.org/matrices/enterprise/>.

Campo	Descripción
Táctica	Nombre de la táctica de la matriz MITRE relacionada con el IOA avanzado. Las tácticas vienen identificadas por una cadena de caracteres con el formato TXXXXX.
Técnica	Nombre de la técnica de la matriz MITRE relacionada con IOA avanzado. Las técnicas se identifican por una cadena de caracteres con el formato TXXXXX.
Subtécnica	Nombre de la subtécnica de la matriz MITRE relacionada con IOA avanzado. Las subtécnicas se identifican por una cadena de caracteres con el formato TXXXXX.YYY.
Plataforma	Sistemas operativos afectados por la técnica & táctica.
Permisos necesarios	Permisos que requiere el atacante para desarrollar el ataque descrito en la técnica & táctica.
Descripción	Descripción de la técnica & táctica según los datos publicados por MITRE.

Tabla 18.12: Campos de la pestaña MITRE

Pestaña Investigación

Todos los tipos de IOAs incorporan la posibilidad de abrir una consola de investigación en Cytomic Orion que muestra la telemetría completa registrada en el equipo y permite realizar una investigación. La consola se posiciona en el último evento que generó la detección del IOA para facilitar el análisis al administrador, y le permite retroceder hasta 5 días en el tiempo para acceder al contexto del equipo en el que se produjo la detección, y un día posterior para poder calibrar los efectos del ataque en el equipo.

Para obtener más información sobre la consola de investigación consulta [Sección Investigación \(5\)](#) en la página [238](#).

Agrupación de detecciones generadas por IOAs

Para evitar mostrar un excesivo número de registros en la consola del cliente, Advanced EDR puede agrupar dos o más detecciones de un mismo IOA, e indica el número de repeticiones en el campo **Ocurrencias** del listado de IOAs u **Ocurrencias detectadas** en su detalle. Para agrupar dos o más detecciones es necesario que se cumplan las condiciones siguientes:

- Que las detecciones se hayan creado a partir del mismo IOA
- Que se detecten en el mismo equipo
- Que se detecten en un intervalo de tiempo próximo

El algoritmo de agrupación empleado varía dependiendo del tipo de IOA y de si el equipo está en modo auditoría o no (para activar o desactivar el modo auditoría consulta [Modo auditoría](#) en la página 306).

Algoritmo de agrupación de detecciones para IOAs

- La primera detección se registra de forma normal con el campo **Ocurrencias detectadas** a 1.
- Se agrupan todas las detecciones repetidas en intervalo de 6 horas. Se envía una detección al final de cada intervalo y se indica en el campo **Ocurrencias detectadas** el acumulado de detecciones registradas hasta el momento.
- Si no se registran detecciones iguales en un intervalo de 6 horas no se envía una detección para ese intervalo.
- Pasados 4 intervalos (24 horas) se vuelve a iniciar el proceso.

Algoritmo de agrupación de detecciones para IOAs avanzados

- La primera detección se registra de forma normal con el campo **Ocurrencias detectadas** a 1.
- Se agrupan todas las detecciones repetidas en intervalo de 1 hora. Se envía una detección al final de cada intervalo y se indica en el campo **Ocurrencias detectadas** el acumulado de detecciones registradas hasta el momento.
- Si no se registran detecciones iguales en un intervalo de 1 hora no se envía una detección para ese intervalo.
- Pasadas 24 horas se vuelve a iniciar el proceso.

Algoritmo de agrupación de detecciones para IOAs avanzados con el modo de auditoría activado

En este modo no se agrupan detecciones. Cada detección se envía con el campo **Ocurrencias detectadas** a 1.

Algoritmo de agrupación de detecciones para IOAs de tipo Ataques RDP



Para obtener más información sobre el algoritmo de detección de ataques de red consulta [Detección y protección frente ataques RDP](#).

Advanced EDR muestra como máximo 50 detecciones iguales cada 24 horas del IOA Ataques de red por cada equipo. Se considera que dos detecciones de tipo Ataques de red son iguales cuando:

- El equipo destino del ataque es el mismo.
- El proceso involucrado en el equipo del usuario atacado es el mismo. Dependiendo de la etapa del ataque de red, este proceso será el que atiende a las peticiones RDP del sistema operativo, o bien cualquier otro proceso que se ejecuta de forma remota en el equipo tras un inicio de sesión exitoso si está precedido de varios intentos de inicio de sesión erróneos.

Diagramas de grafos

Para ver el detalle de una detección de IOA, accede al listado **Indicadores de ataque (IOA)** y haz clic en la detección. Consulta [Acceso a los listados](#). Si la detección tiene asociado un diagrama de grafos, se mostrará el botón **Ver gráfica del ataque** en su ventana de detalle.

Estructura de un diagrama de grafos

A continuación se muestran los paneles de información y herramientas de un diagrama de grafos.

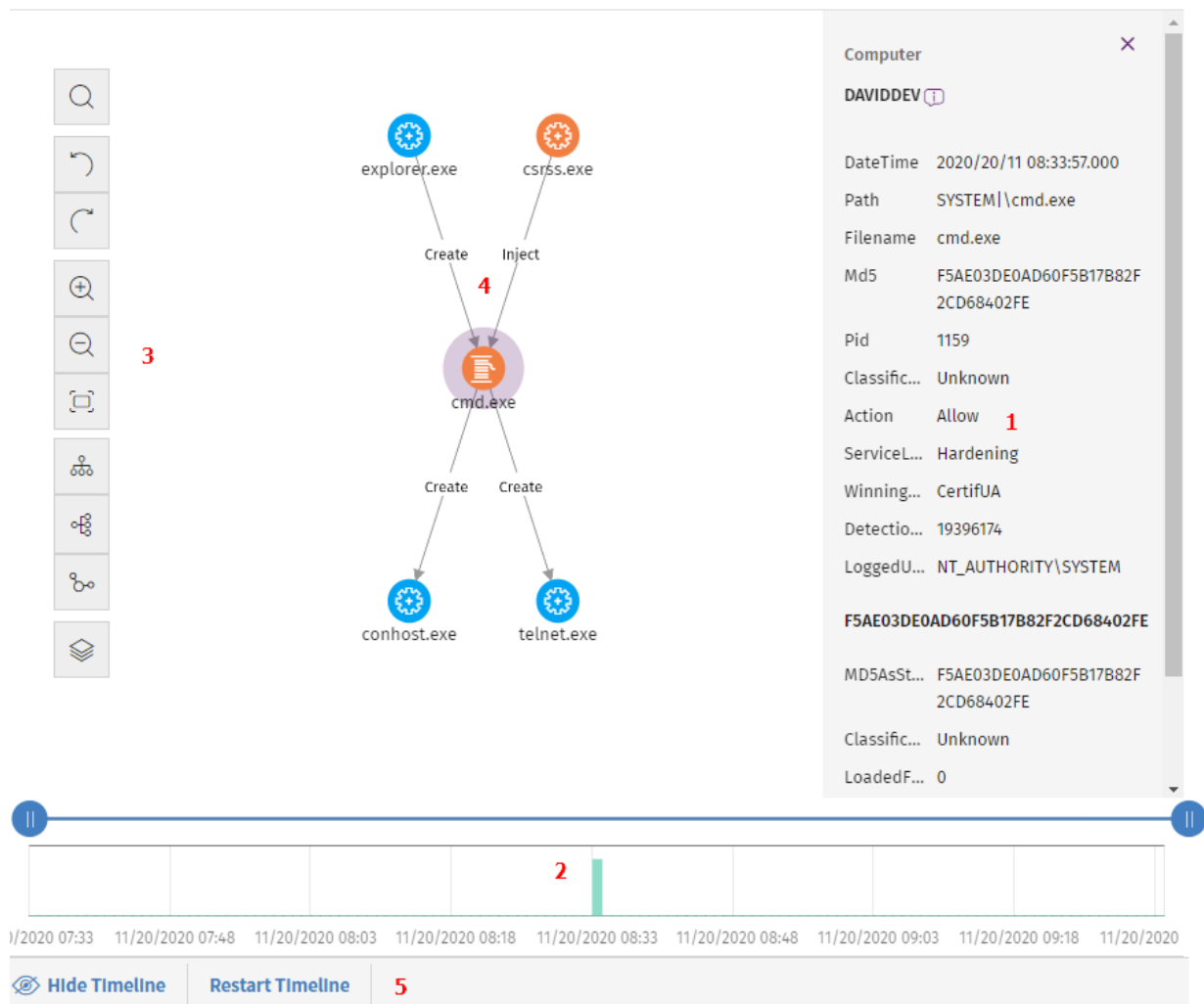


Figura 18.1: Diagrama de grafos y herramientas

- **Panel informativo del elemento seleccionado (1):** muestra información del nodo o de la línea seleccionada. Para obtener el significado de los campos incluidos, consulta [Formato de los eventos recogidos en la telemetría](#) en la página 867.
- **Línea de tiempo (2):** muestra un histograma de barras de color verde para representar el número de eventos registrados en cada momento. Permite ampliar o reducir el intervalo al que pertenecen los eventos mostrados. Para obtener información sobre cómo utilizar este recurso, consulta [Línea de tiempo](#).

- **Barra de herramientas del grafo (3):** permite modificar la forma en la que se visualiza el diagrama en la pantalla. Consulta [Configuración del diagrama de grafos](#).
- **Diagrama (4):** representación gráfica de un conjunto de eventos, que utiliza nodos y flechas para mostrar entidades y sus relaciones. Se indica mediante un número en cada flecha el orden en el que se ha registrado la creación de los eventos incluidos en el grafo.
- **Controles de la línea de tiempo (5):** oculta, muestra o restaura la línea de tiempo. Consulta [Línea de tiempo](#).

Configuración del diagrama de grafos

Para modificar el aspecto y la cantidad de información mostrada en un diagrama de grafos y acomodarlo a las necesidades del administrador, se implementan dos recursos principales:

- La barra de herramientas del diagrama de grafos, accesible desde la parte izquierda de la pantalla.
- Los menús contextuales, accesibles al hacer clic con el botón derecho del ratón sobre un nodo o sobre una agrupación de nodos.

Por defecto, el diagrama se muestra con orientación horizontal (6) y con un nivel de zoom suficiente para que todos los nodos sean visibles sin necesidad de desplazar la pantalla.

Barra de herramientas del diagrama de grafos

- Para resaltar de un color diferente los nodos que cumplan con el patrón de búsqueda introducido y facilitar su localización en el diagrama, haz clic en el icono (1).
- Para deshacer la última acción ejecutada sobre el diagrama, haz clic en el icono (2).
- Para rehacer la última acción desechada del diagrama, haz clic en el icono (3).
- Para ampliar el diagrama haz clic en el icono (4).
- Para alejar el diagrama haz clic en el icono (5).
- Para restaurar la configuración del nivel de zoom al establecido inicialmente, haz clic en el icono (6).
- Para cambiar la orientación del diagrama a horizontal, haz clic en el icono (7).
- Para cambiar la orientación del diagrama a vertical, haz clic en el icono (8).
- Para cambiar la orientación del diagrama de forma que los nodos se distribuyan libremente aprovechando el espacio disponible, haz clic en el icono (9).
- Para mostrar u ocultar las distintas capas de información incluidas en el grafo (10) consulta [Ocultar y mostrar capas](#).



Figura 18.2: Barra de herramientas

Menús de contexto

Al hacer clic con el botón derecho del ratón sobre un nodo o una agrupación, se muestra el menú de contexto. Las opciones que no es posible utilizar dependiendo del estado del nodo se deshabilitan, mostrándose con un color atenuado.

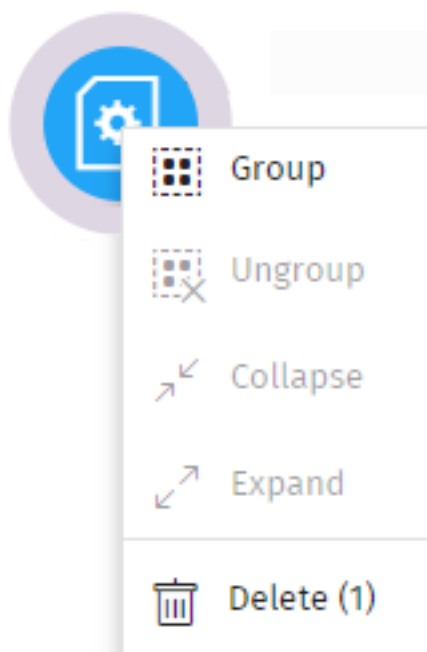


Figura 18.3: Menú de contexto

Ocultar y mostrar capas

Para ocultar parte de la información incluida en el grafo y mostrar sus características más relevantes del grafo, haz clic en el icono (10). Se mostrará un menú desplegable con las opciones:

- **Secuencia de ejecución:** oculta o muestra la numeración de los eventos que determina el orden de ejecución en el equipo del usuario. Consulta [Estilos de las flechas](#).
- **Nombres de la relaciones:** oculta o muestra el nombre de los eventos. Consulta [Formato de los eventos recogidos en la telemetría](#) en la página 867.
- **Nombres de las entidades.**

Seleccionar nodos del diagrama

- **Para seleccionar un único nodo del diagrama:** haz clic sobre el nodo con el botón izquierdo del ratón.
- **Para seleccionar varios nodos dispersos del diagrama:** mantén presionada la tecla Control o Mayúsculas y haz clic sobre los nodos con el botón izquierdo del ratón.
- **Para seleccionar varios nodos contiguos del diagrama:** mantén presionada la tecla Control o Mayúsculas, haz clic en una zona libre del diagrama y arrastra el ratón hasta abarcar los nodos a seleccionar.

Al seleccionar varios nodos del diagrama y hacer clic con el botón derecho del ratón, se muestran únicamente las opciones del menú de contexto comunes a todos los nodos seleccionados.

Mover y borrar nodos del diagrama

Para mover todos los nodos y líneas del diagrama:

Haz clic en un espacio libre y arrastra el ratón en la dirección apropiada.

Para mover un único nodo:

Selecciona el nodo y arrástralo en la dirección apropiada. Todas las líneas que conectan al nodo con sus vecinos se ajustarán a su nueva posición.

Para eliminar un nodo con el teclado:

- Selecciona el nodo deseado y presiona la tecla Supr. Se mostrará un mensaje indicando el número total de nodos que se eliminarán del grafo: el propio nodo y todos sus descendientes.
- Haz clic en el botón **Aceptar**.

Para eliminar un nodo con el ratón:

- Haz clic con el botón derecho del ratón sobre el nodo a borrar. Se mostrará el menú de contexto.
- Selecciona la opción **Borrar (x)**. Se mostrará un mensaje indicando el número total de nodos que se eliminarán del grafo: el propio nodo y todos sus descendientes.
- Haz clic en el botón **Aceptar**.

Para borrar varios nodos:

- Selecciona los nodos a borrar y haz clic en cualquiera de ellos con el botón derecho del ratón. Se mostrará el menú de contexto.
- Selecciona la opción **Borrar (x)**. Se mostrará un mensaje indicando el número total de nodos que se eliminarán del grafo: los nodos seleccionados y todos sus descendientes.
- Haz clic en el botón **Aceptar**.

Agrupar nodos

En los grafos que contienen una gran cantidad de elementos, el administrador puede agrupar nodos que guarden algún tipo de relación para simplificar el diagrama.

Las agrupaciones de nodos tienen dos estados:

- **Expandida**: si muestra los nodos que la forman.
- **Colapsada**: si oculta los nodos que la forman.

Una agrupación de nodos es una entidad por sí misma, con las siguientes características:

- Las acciones aplicadas sobre un grupo de nodos afectan a todos los nodos que lo componen.
- Se pueden agrupar nodos de diferentes tipos.
- Eliminar una agrupación equivale a eliminar del grafo todos los nodos que la componen.

- Al colapsar un grupo, todas las relaciones de sus miembros con nodos externos se representan como si estuvieran establecidas con la agrupación. Las flechas que reflejen relaciones de un mismo tipo (mismo tipo de evento) también se agrupan (consulta [Información de una agrupación colapsada](#)).
- El espacio vacío de una agrupación expandida, representa al conjunto de nodos agrupados. Por ejemplo, para mostrar el menú de contexto de todos los nodos de una agrupación haz clic con el botón derecho del ratón en un espacio vacío de la agrupación expandida. De la misma forma, si seleccionas la opción **Eliminar**, borrarás todos los nodos que pertenecen a la agrupación.
- Un nodo que pertenece a una agrupación expandida conserva el comportamiento normal de un nodo del grafo sin agrupar: se podrá mover de forma individual, mostrar su menú de contexto, borrar, etc.
- Una agrupación puede estar formada solo por nodos, solo por grupos, o por una mezcla de ambos.

Para agrupar un conjunto de nodos:

- Selecciona varios nodos del diagrama y haz clic con el botón de la derecha del ratón. Se abrirá el menú de contexto.
- En el menú selecciona **Agrupar** . Se creará un rectángulo de agrupación que contiene los nodos agrupados.

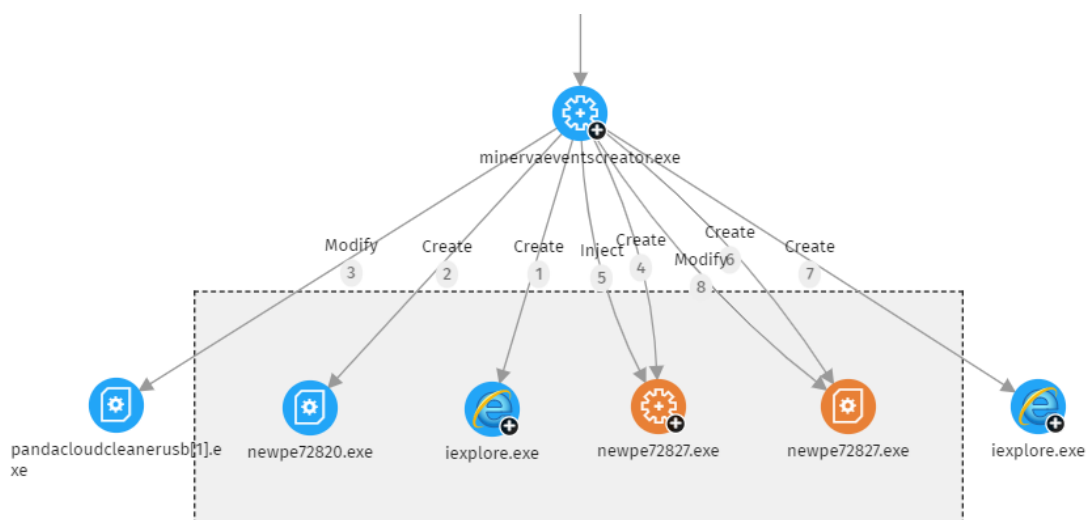


Figura 18.4: Agrupación de nodos

- Haz clic con el botón derecho del ratón en una zona despejada del rectángulo de agrupación. Se abrirá el menú de contexto de la agrupación.
- En el menú selecciona **Colapsar** . Los nodos agrupados se sustituyen por un cuadrado de tamaño inferior y todas las relaciones de los nodos agrupados se mueven al cuadrado de agrupación.

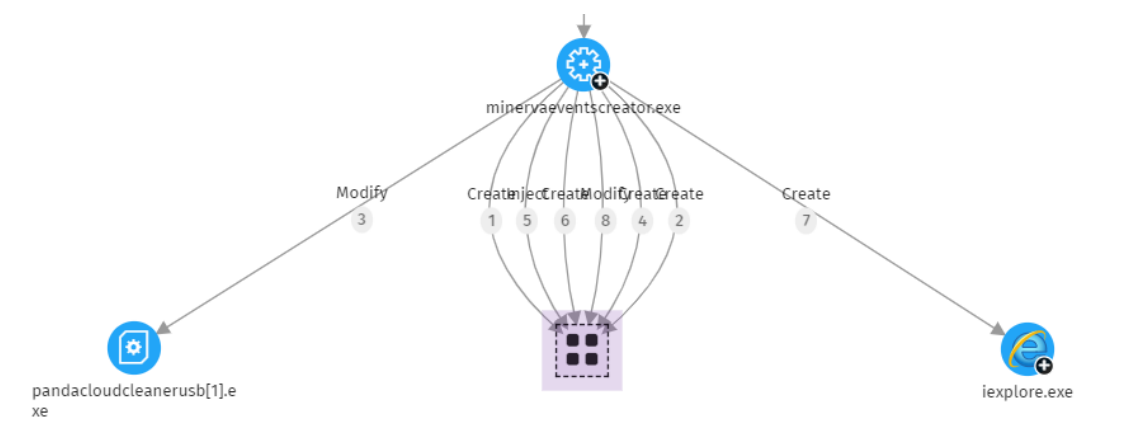


Figura 18.5: Grupo de nodos colapsado

Para expandir un grupo de nodos colapsado:

- Selecciona con el botón derecho del ratón el grupo de nodos colapsado. Se abrirá el menú de contexto.
- Selecciona la opción **Expandir** . Los nodos colapsados se mostrarán junto al rectángulo de agrupación.

Para deshacer una agrupación de nodos:

- Selecciona con el botón derecho del ratón el grupo de nodos. Se abrirá el menú de contexto.
- Selecciona la opción **Desagrupar** . Los nodos agrupados se mostrarán en el grafo y el rectángulo de agrupación desaparecerá.

Información de una agrupación colapsada

Tipo de nodos agrupados

Una agrupación puede contener nodos clasificados como goodware, malware o sin clasificar. Esta situación se refleja en el color utilizado para representar la agrupación.

Color	Descripción
	Agrupación con elementos bloqueados.
	Agrupación con elementos clasificados como goodware.

Tabla 18.13: Códigos de color utilizados en las agrupaciones

Número de nodos agrupados

En la esquina superior izquierda se muestra el número de nodos que se mostrarían en el diagrama en caso de que la agrupación no estuviera colapsada. Este número no tiene nada que ver con el número de nodos total (padres, hijos, etc) que puede contener la agrupación, ya que solo se cuentan los nodos que se han expandido previamente.

Buscar nodos

La barra de búsqueda permite resaltar los nodos que interesan al administrador y acceder de forma rápida a sus detalles.

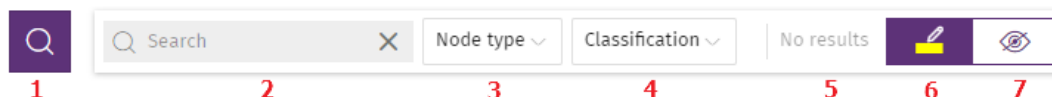


Figura 18.6: Barra de búsqueda de grafos

- (1): Haz clic para mostrar u ocultar la barra de búsqueda.
- (2): Escribe la cadena de caracteres a buscar. La búsqueda se ejecuta en tiempo real sobre el nombre y el detalle de los nodos, y se excluye el contenido de las flechas. Para limpiar la búsqueda, haz clic en el icono ✕.



Para evitar mostrar nodos huérfanos en los resultados de las búsquedas siempre se incluye el nodo padre, aunque no coincida con el patrón introducido.

- (3): Limita las búsquedas en el grafo a determinados tipos de entidades. Para extender la búsqueda a más de un tipo de entidad, expande el desplegable y selecciona los tipos de entidad que desees. Para volver a buscar en todos los tipos de entidad, haz clic en la opción **Limpiar búsqueda**. El operador lógico aplicado al establecer una búsqueda sobre varios tipos de entidad es OR.
- (4) Limita las búsquedas en el grafo a las entidades que han sido clasificadas por Advanced EDR a los valores indicados en el desplegable. Para extender la búsqueda a más de una clasificación, expande el desplegable y selecciona las clasificaciones que desees. Para volver a buscar sin tener en cuenta la clasificación de las entidades, haz clic en la opción **Limpiar búsqueda**. El operador lógico aplicado al establecer una búsqueda sobre nodos con distintas clasificaciones es OR.
- El operador lógico al definir a la vez una búsqueda por entidad y una búsqueda por clasificación es AND.
- (5): Indica el número de nodos que coinciden con el patrón de búsqueda introducido. Cuando la herramienta de resaltado está activada (4), al hacer clic en el icono ▼ se muestra un desplegable:
 - **Seleccionar los nodos encontrados:** selecciona los nodos que coinciden con el patrón de búsqueda introducido. Para mostrar el menú de contexto, haz clic con el botón derecho del ratón en cualquier elemento seleccionado.

- **Seleccionar todos los nodos menos los encontrados:** selecciona los nodos que no coinciden con el patrón de búsqueda introducido. Para mostrar el menú de contexto, haz clic con el botón derecho del ratón en cualquier elemento seleccionado.
- **(6):** Resalta los elementos encontrados con el color amarillo.
- **(7):** Oculta los elementos que no coinciden con el patrón de búsqueda introducido.

Las búsquedas realizadas sobre nodos agrupados expandidos se comportan de la forma indicada, pero si se trata de un grupo colapsado, tienen un comportamiento diferente:

- Si la búsqueda se realiza en modo resaltado **(4)**, se iluminará la agrupación si uno de los nodos que la componen coincide con la búsqueda. En caso contrario, la agrupación no se iluminará.
- Si la búsqueda se realiza en modo ocultación **(5)**, la agrupación se mostrará si por lo menos uno de los nodos que la componen coincide con la búsqueda. En caso contrario, la agrupación no se mostrará en el grafo.

Línea de tiempo

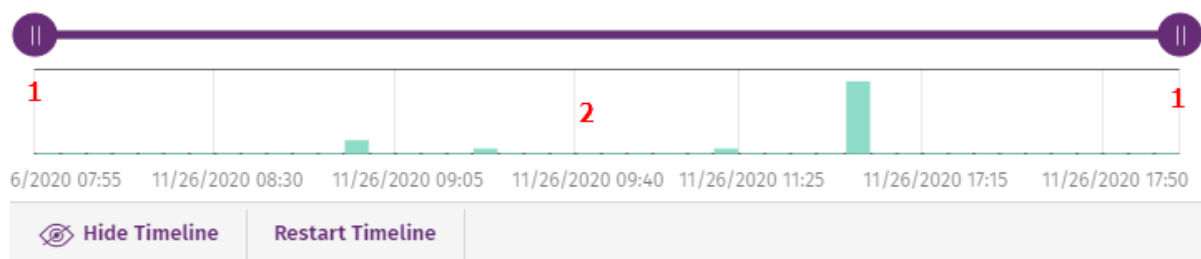


Figura 18.7: Controles de la línea de tiempo

La línea de tiempo permite atenuar los nodos y las relaciones que se registraron fuera del intervalo definido por el administrador. De esta manera, los eventos del océano de datos que no resultan de interés pasan a un segundo plano en el diagrama, y permiten al administrador centrarse en los más relevantes.

La línea de tiempo utiliza un histograma de barras de color verde situado en su parte inferior **(2)** para representar el número de eventos registrados en cada momento. Al pasar el puntero del ratón sobre las barras, se muestra una etiqueta que indica el número de eventos y la fecha en la que se registraron.

Para definir un intervalo mediante la línea de tiempo:

- Haz clic en **(1)** y arrástralo hacia izquierda y derecha. El histograma se ampliará o reducirá para adaptarse al nuevo intervalo definido.
- Se atenuarán los nodos y relaciones del diagrama de grafos que queden fuera del nuevo intervalo definido.

Para ocultar / mostrar la línea de tiempo:

- Para eliminar el panel haz clic en **Ocultar línea de tiempo**.
- Para volver a visualizar el panel haz clic en **Mostrar línea de tiempo**.

- Haz clic en **Reiniciar la línea de tiempo** para restaurar la línea de tiempo a su configuración original.

Información contenida en diagramas de grafos

Los diagramas de grafos representan de forma gráfica el árbol de ejecución de una detección de IOA, donde cada nodo represental a una entidad que participó en una operación (procesos, ficheros o destino de una comunicación u operación) y las flechas la operación propiamente dicha. Para ello se utilizan códigos de color, paneles y otros recursos que aportan información sobre las entidades representadas y sus relaciones.

Los recursos utilizados para reflejar la información son:

- **Colores de los nodos:** indican la clasificación del elemento.
- **Iconos de los nodos:** indican el tipo de elemento.
- **Iconos de estado:** indican la acción que se ejecutó sobre el elemento.
- **Colores de las flechas:** indican si el elemento fue bloqueado.
- **Estilos de las flechas:** indican el número y el sentido de las acciones ejecutadas entre los dos nodos.
- **Etiquetas de las flechas:** al hacer clic en ellas, muestran información en el panel de la derecha sobre la acción ejecutada por el proceso.
- **Etiquetas del nodo:** al hacer clic en ellas, muestra información en el panel de la derecha sobre la entidad.

Colores de los nodos

Color	Descripción
	Elemento clasificado como malware.
	• Elemento clasificado como PUP. • Elemento clasificado como sospechoso. • Elemento sin clasificar.
(Color Original)	Elemento clasificado como goodware.

Tabla 18.14: Códigos de color utilizados en los nodos de un grafo

Iconos de los nodos

Icono	Descripción	Icono	Descripción
	Proceso. Si pertenece a un paquete de software conocido, se mostrará su icono.		Archivo comprimido
	Hilo remoto		Archivo ejecutable
	Librería		Archivo de tipo script
	Protección		Valor de la rama del registro Windows
	Carpeta		URL en una comunicación
	Archivo no ejecutable		Dirección IP en una comunicación

Tabla 18.15: Códigos de color utilizados en los nodos de un grafo

Iconos de estado

Icono	Descripción	Icono	Descripción
	Fichero borrado		Fichero en cuarentena

Icono	Descripción	Icono	Descripción
	Fichero desinfectado		Proceso eliminado

Tabla 18.16: Iconos utilizados para indicar el estado del nodo

Etiquetas de los nodos

Indican el nombre de la entidad. Al hacer clic sobre ellas, se muestra el panel derecho con los campos que las describen.

Colores de las flechas

Indican si Advanced EDR o Advanced EDR bloquearon la ejecución de la acción por haber clasificado al proceso como una amenaza.

- **Rojo:** la acción fue bloqueada por el software de protección. Consulta el significado de las acciones siguientes en el campo action de **Formato de los eventos recogidos en la telemetría** en la página 867.
- **Negro:** la acción fue permitida.

Estilos de las flechas

- **Grosor de la flecha:** representa el número de acciones de un mismo tipo ejecutadas entre un par de nodos. Cuanto mayor sea el número de acciones agrupadas, mayor será el grosor de la flecha dibujada. Al hacer clic en la flecha, el panel informativo mostrará la fecha en la que se ha producido la primera y la última acción de la agrupación.
- **Sentido de la flecha:** refleja el sentido de la acción.
- **Numeración:** cada flecha incluye un número que refleja el orden en el que se registró el evento al que representa.

Etiquetas utilizadas en las flechas

Indican el nombre de la acción ejecutada por el proceso. Al hacer clic en ellas, se muestra el panel derecho con los campos del evento registrado.

Niveles representados por defecto

Inicialmente se muestra como centro del diagrama el nodo que desencadenó la generación de la detección de IOA, junto a un subconjunto de nodos vecinos que lo rodean, de todos los registrados en la detección:

- **3 niveles superiores de nodos:** se muestran los nodos padres, abuelos y bisabuelos del nodo principal.
- **1 nivel inferior de nodos:** se muestran los nodos hijos del nodo principal.

El número máximo de nodos del mismo nivel que se muestran es 25. Por encima de este número no se representarán nodos, para evitar la generación de gráficos muy sobrecargados.

Mostrar los nodos hijos

Si un nodo del grafo tiene nodos hijos ocultos, se indica con el icono  en su parte inferior derecha. Para mostrar sus nodos hijos, haz clic sobre el nodo con el botón derecho del ratón. Se mostrará un menú de contexto. Dependiendo del tipo de nodo se mostrarán las siguientes opciones:

- **Mostrar padre:** muestra los nodos padre del nodo seleccionado.
- **Mostrar toda su actividad (número):** muestra todos los nodos hijos del nodo seleccionado, sin importar su tipo. El número máximo de nodos mostrados es 25. Se indica el número total de eventos que relacionan el nodo padre con sus hijos.
- **Mostrar hijos:** muestra un desplegable con el tipo de nodos hijo a mostrar y el número de nodos de cada tipo:
 - **Archivos de datos:** ficheros que contienen información de tipo no identificado.
 - **Archivos de script:** ficheros con secuencias de comandos.
 - **Descargas:** ficheros de datos descargados de la red.
 - **DNS:** dominios que fallaron al resolver su IP.
 - **Entradas del registro de Windows**
 - **Ficheros comprimidos**
 - **Ficheros PE:** ficheros ejecutables.
 - **Hilos remotos**
 - **IPs:** dirección IP del extremo de la comunicación.
 - **Librerías**
 - **Procesos**
 - **Protección:** acción del antivirus.

Al seleccionar varios nodos del diagrama y hacer clic con el botón derecho del ratón se mostrarán únicamente las opciones del menú de contexto comunes a todos los nodos seleccionados.

Paneles / widgets del módulo Indicadores de ataque

Para acceder al panel de control haz clic en el menú superior **Estado**, panel lateral **Seguridad**.

Permisos requeridos

Permisos	Acceso a widgets
Visualizar detecciones y amenazas	- Servicio Threat Hunting - Evolución de las detecciones - Indicadores de ataque situados en la matriz de MITRE ATT&CK - Indicadores de ataque (IOA) detectados - Indicadores de ataque (IOA) por equipo

Tabla 18.17: Permisos requeridos para el acceso a los widgets de Programas bloqueados

Todos los widgets excepto Servicio Threat Hunting, muestran únicamente la información generada por los equipos del parque informático sobre los que tiene visibilidad el rol asociado a la cuenta del administrador utilizada para acceder a la consola.

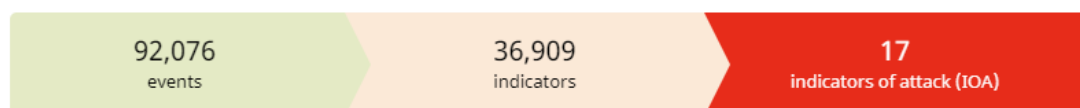
Advanced EDR muestra en los distintos widgets las detecciones en estado Pendiente cuando registra actividad sospechosa en la red el cliente. Consulta [Introducción a los conceptos de IOAs](#).

Para obtener información sobre las estrategias de agrupación de detecciones de IOAs que implementa Advanced EDR consulta [Agrupación de detecciones generadas por IOAs](#).

Servicio Threat Hunting

Muestra datos sobre la información recogida de los equipos del cliente que la plataforma Cytomic utiliza como base para determinar si existen intentos de intrusión en los equipos protegidos.

THREAT HUNTING SERVICE



78 Computers in "RDP attack containment" mode. [View all](#)

Figura 18.8: Panel de control Servicio Threat Hunting

Significado de las series

Serie	Descripción
Eventos	Número de acciones ejecutadas por los programas instalados en los equipos protegidos de todo el parque informático del cliente, y monitorizados por Advanced EDR. Estos eventos son recibidos como parte del flujo de telemetría y se almacenan en la plataforma Cytomicen busca de patrones sospechosos. En este contador se incluyen todas las detecciones del cliente, sin importar la

Serie	Descripción
	visibilidad de la cuenta que accede a la consola de Advanced EDR.
Indicios	Número de patrones sospechosos detectados en el flujo de eventos recibidos. En este contador se incluyen todas las detecciones del cliente, sin importar la visibilidad de la cuenta que accede a la consola de Advanced EDR.
Indicadores de ataque (IOA)	Número de patrones sospechosos con una alta probabilidad de pertenecer a la CKC de un ataque informático.
Equipos en modo contención de ataque RDP	Número de equipos que han recibido un ataque por el protocolo RDP y han sido configurados en modo contención de ataque RDP.

Tabla 18.18: Descripción de las series de Servicio Threat Hunting

Filtros preestablecidos desde el panel

THREAT HUNTING SERVICE

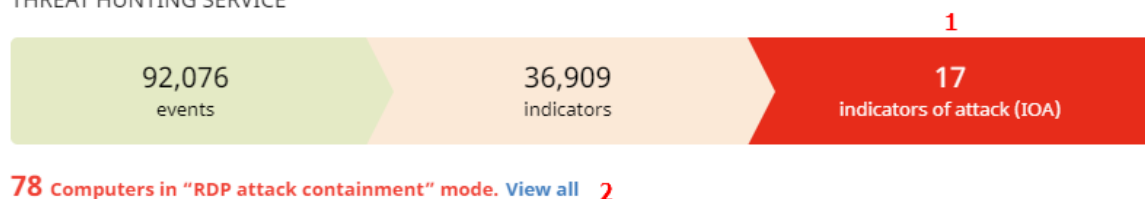


Figura 18.9: Zonas activas del panel Servicio Threat Hunting

Haz clic en las zonas indicadas en **Zonas activas del panel Servicio Threat Hunting** para abrir el listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Indicadores de ataque (IOA)	Sin filtros
(2)	Estado de protección de los equipos	Modo "Contención de ataque RDP" = Sí

Tabla 18.19: Definición de filtros del panel de control Servicio Threat Hunting

Evolución de las detecciones

Muestra en un gráfico de líneas y barras la evolución de los indicios, detecciones de IOAs pendientes y detecciones de IOAs archivados registrados en los equipos de la red.

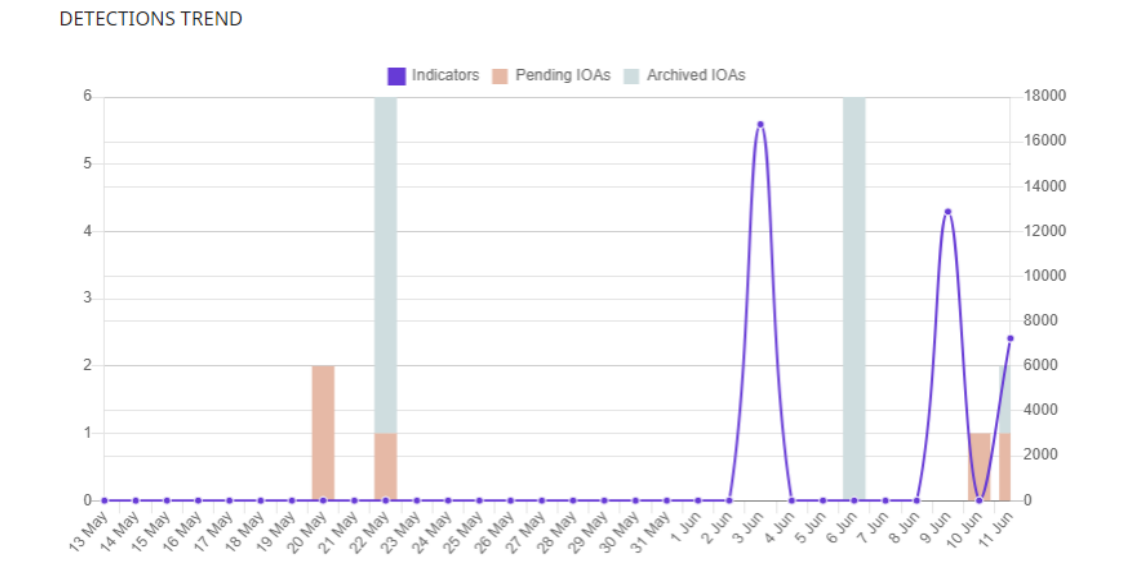


Figura 18.10: Panel de control Evolución de las detecciones

Para representar las diferentes escalas en un mismo diagrama, el gráfico tiene dos ejes Xs:

- El eje X de la izquierda se refiere a las detecciones archivados y pendientes detectados.
- El eje X de la derecha se refiere a los indicios detectados.

Significado de las series

Series	Descripción
Indicios	Evolución del número de patrones sospechosos detectados en el flujo de eventos recibidos.
IOA pendiente	Evolución del número de patrones sospechosos con una alta probabilidad de pertenecer a la CKC de un ataque informático, y que el administrador tiene pendiente su estudio o resolución.
IOA archivado	Evolución del número de patrones sospechosos con una alta probabilidad de pertenecer a la CKC de un ataque informático, y que el administrador ya ha estudiado y resuelto, si no se trató de un falso positivo.

Tabla 18.20: Descripción de las series de Evolución de las detecciones

DETECTIONS TREND

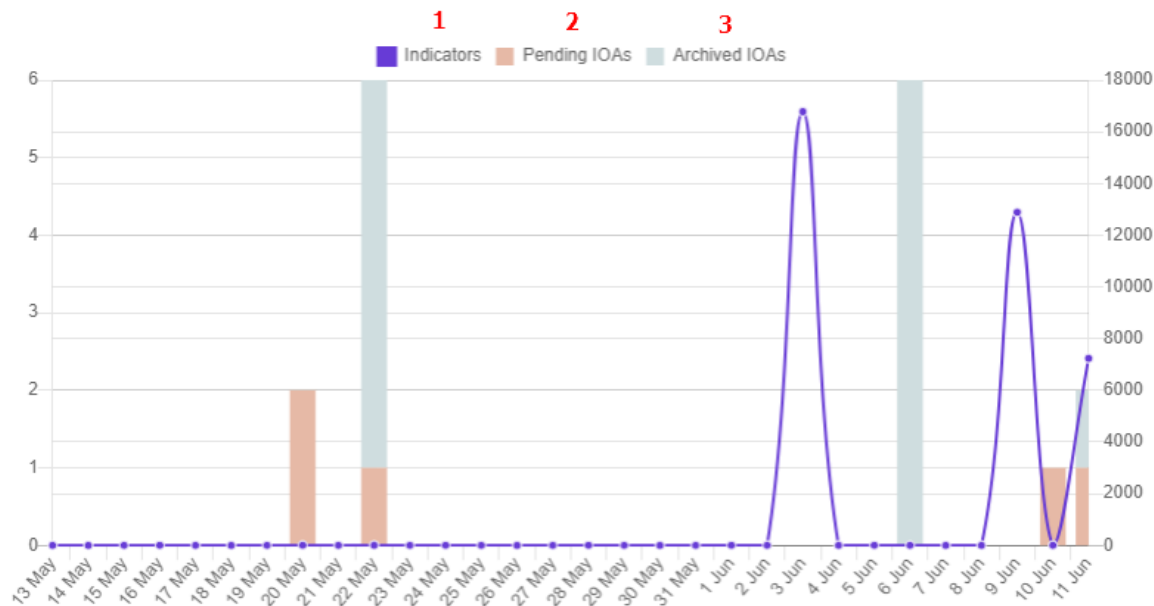


Figura 18.11: Zonas activas del panel Evolución de las detecciones

Haz clic en las zonas indicadas en **Zonas activas del panel Evolución de las detecciones** para abrir el listado Indicadores de ataque (IOA) con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Ninguno
(2)	Estado = Pendiente
(3)	Estado = Archivado

Tabla 18.21: Definición de filtros del listado Indicadores de ataque (IOA)

Indicadores de ataque situados en la matriz de MITRE ATT&CK

Muestra en una matriz la distribución de indicadores de ataque detectados en el intervalo elegido y ordenados por táctica y técnica.

Al pasar el ratón por encima de las casillas, se muestra:

- Nombre y código de la táctica/técnica
- Número de detecciones totales
- Número de detecciones pendientes

Una detección de IOA tiene al menos una táctica y una técnica asociadas; en cuanto a las subtécnicas, pueden tener más de una asociada, si bien no todos los IOAs las tienen.

Para ver las subtécnicas de las detecciones de IOAs, haz clic en el enlace **Mostrar subtécnicas**.

INDICATORS OF ATTACK (IOA) MAPPED TO THE MITRE ATT&CK MATRIX

Persistence	Privilege Escalation	Defense Evasion	Credential Access
1 Accessibility Features	2 Bypass User Account Control	1 Abuse Elevation Control Mechanism	1 Brute Force
	1 Process Injection	Show sub-techniques	Show sub-techniques
		1 Disabling Security Tools	2 OS Credential Dumping

Figura 18.12: Panel de control Indicadores de ataque situados en la matriz de MITRE ATT&CK

Significado de las series

Series	Descripción
Número Rojo	Número de detecciones registradas en estado pendiente que utilizan la táctica, técnica y subtécnica indicadas para el intervalo elegido.
Número Negro	Número total (pendientes + archivados) de detecciones registradas que utilizan la táctica, técnica y subtécnicas indicadas para el intervalo elegido.
Enlace Mostrar subtécnicas	Desplegable con las subtécnicas. Por cada subtécnica se indica el número total de detecciones pendientes (número rojo) o pendientes + archivadas (número negro) que tienen esa subtécnica asociada.

Tabla 18.22: Descripción de las series de Indicadores de ataque situados en la matriz de MITRE ATT&CK

Filtros preestablecidos desde el panel

INDICATORS OF ATTACK (IOA) MAPPED TO THE MITRE ATT&CK MATRIX



Figura 18.13: Zonas activas del panel Indicadores de ataque situados en la matriz de MITRE ATT&CK

Haz clic en las zonas indicadas en la figura **Zonas activas del panel Indicadores de ataque situados en la matriz de MITRE ATT&CK** para abrir el listado **Indicadores de ataque (IOA)** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Táctica = táctica elegida en el widget
(2)	- Táctica = táctica elegida en el widget - Técnica = técnica elegida en el widget
(3)	Subtécnica = subtécnica elegida en el widget

Tabla 18.23: Definición de filtros del listado Indicadores de ataque (IOA)

Indicadores de ataque (IOA) detectados

Muestra la distribución de detecciones de IOAs según su tipo registrados en el intervalo elegido. Cuanto mayor sea comparativamente el número de detecciones de un tipo concreto con respecto al resto, mayor será la superficie del polígono representado en el widget.

DETECTED INDICATORS OF ATTACK (IOA)

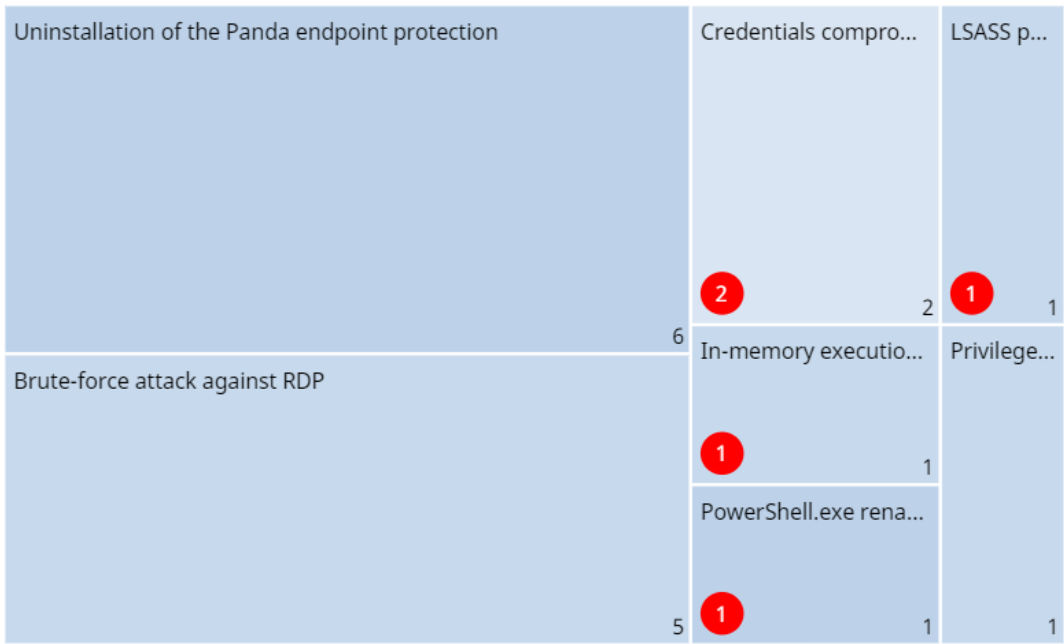


Figura 18.14: Panel de control Indicadores de ataque (IOA) detectados

Significado de las series

Serie	Descripción
Número Rojo	Número de detecciones del tipo indicado en el intervalo elegido y en estado pendiente.
Número Blanco	Número total (pendientes + archivados) de detecciones del tipo indicado en el intervalo elegido.

Tabla 18.24: Descripción de las series de Indicadores de ataque (IOA) detectados

Filtros preestablecidos desde el panel

DETECTED INDICATORS OF ATTACK (IOA)

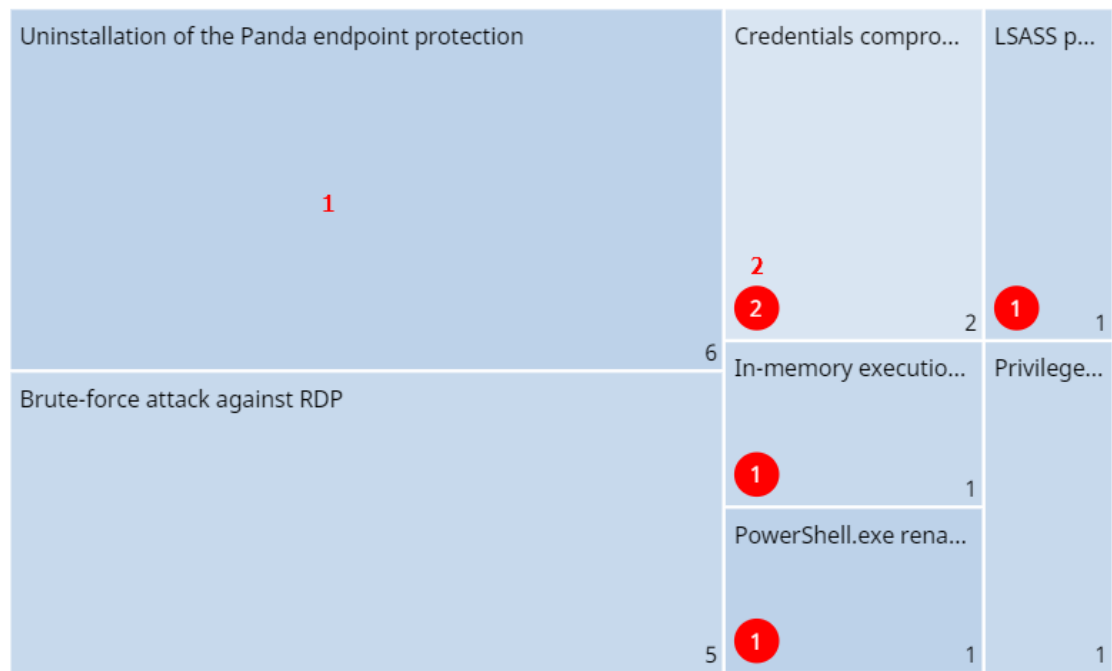


Figura 18.15: Panel de control Indicadores de ataque (IOA) detectados

Haz clic en las zonas indicadas en **Panel de control Indicadores de ataque (IOA) detectados** para abrir el listado Indicadores de ataque (IOA) con los filtros preestablecidos mostrados a continuación:

Zona Activa	Filtro
(1)	Indicador de ataque = Indicador de ataque elegido en el widget
(2)	- Indicador de ataque = Indicador de ataque elegido en el widget - Estado = Pendiente

Tabla 18.25: Definición de filtros del listado Indicadores de ataque (IOA)

Indicadores de ataque (IOA) por equipo

Muestra la distribución de detecciones registradas por cada equipo de la red en el intervalo elegido. Cuanto mayor sea comparativamente el número de detecciones en un mismo equipo con respecto al resto, mayor será la superficie del polígono representado en el widget.

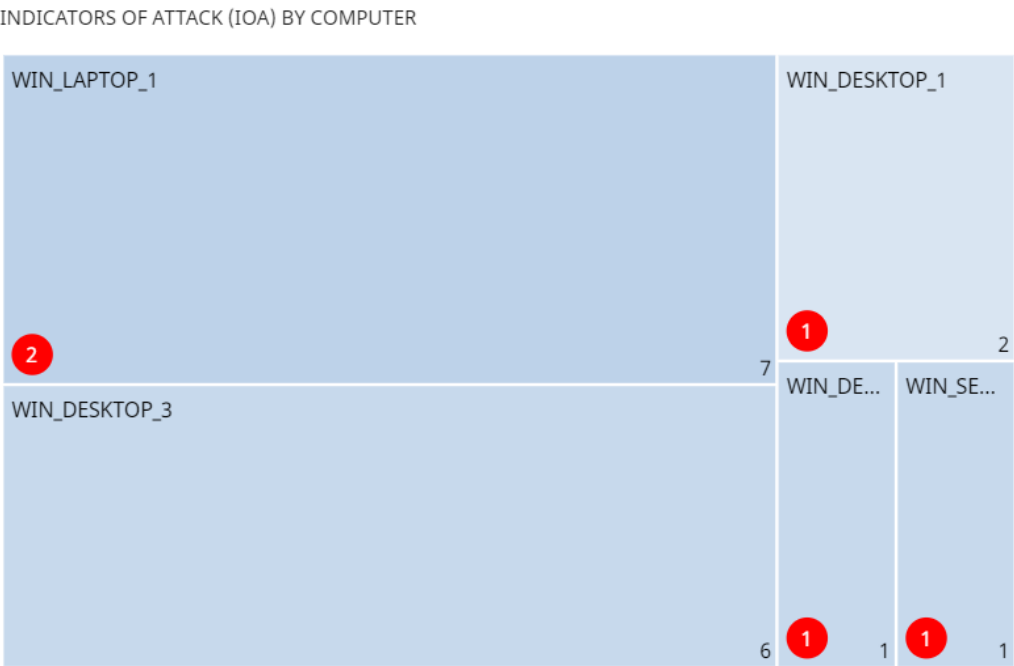


Figura 18.16: Panel de control Indicadores de ataque (IOA) por equipo

Significado de las series

Series	Descripción
Número Rojo	Número de detecciones en estado pendiente registradas en el equipo indicado para el intervalo elegido.
Número Blanco	Número total de detecciones (pendientes + archivados) registradas en el equipo indicado para el intervalo elegido.

Tabla 18.26: Descripción de las series de Indicadores de ataque (IOA) por equipo

Filtros preestablecidos desde el panel

INDICATORS OF ATTACK (IOA) BY COMPUTER

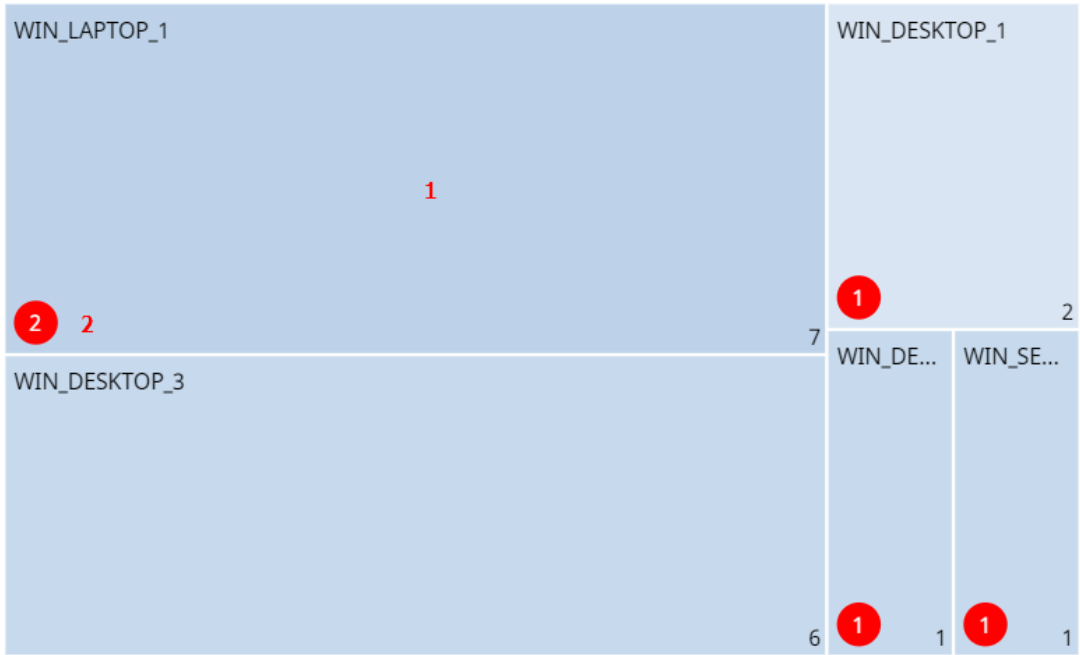


Figura 18.17: Panel de control Indicadores de ataque (IOA) por equipo

Haz clic en las zonas indicadas en **Panel de control Indicadores de ataque (IOA) por equipo** para abrir el listado Indicadores de ataque (IOA) con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Equipo
(2)	- Equipo - Estado = Pendiente

Tabla 18.27: Definición de filtros del listado Indicadores de ataque (IOA)

Configuración del servicio MDR



La configuración del servicio MDR solo se muestra en la consola de Advanced EDR si el cliente tiene contratado este servicio con su partner. Antes de empezar a escribir este formulario consulta con tu partner.

WatchGuard MDR (Managed Detection and Response) es un servicio de ciberseguridad 24 / 7 que permite a los partners ofrecer a sus clientes un servicio gestionado de detección y respuesta, con una inversión mínima en un SOC (Security Operations Center). El servicio monitoriza la seguridad de los equipos de la empresa, busca amenazas, detecta ataques, investiga y ofrece recomendaciones guiadas para resolver los activos afectados y mejorar la seguridad de los clientes.

El servicio MDR está impulsado por innovadoras tecnologías que utilizan algoritmos de inteligencia artificial. Además, es un servicio completamente administrado por expertos en ciberseguridad, lo que mejora de forma general la protección y resiliencia cibernética de los clientes, minimizando el tiempo de detección y respuesta frente a las amenazas.



Para obtener información adicional sobre los distintos apartados del módulo MDR consulta las referencia siguientes:

Crear y gestionar configuraciones en la página **258**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.

Acceso, control y supervisión de la consola de administración en la página **59**: gestión de cuentas de usuario y asignación de permisos.

Contenido del capítulo

Configuración del servicio MDR	604
Opciones de configuración de MDR	604

Configuración del servicio MDR

Acceso a la configuración

Selecciona el menú superior **Configuración**, menú lateral **MDR**. Solo se permite una configuración, que se establece a nivel de cuenta y se aplica a todos los equipos del parque informático administrado.

Permisos requeridos

Permiso	Tipo de acceso
Configurar MDR	Crear, modificar y borrar la configuración de MDR.
Ver configuración de MDR	Visualizar la configuración de MDR.

Tabla 18.28: Permisos requeridos para acceder a la configuración MDR

Opciones de configuración de MDR

La configuración MDR permite al cliente enviar a su partner información actualizada sobre el parque informático que administra. De esta forma, el partner podrá dimensionar los recursos de ciberseguridad necesarios para suministrar de forma conveniente el servicio de detección, protección y respuesta.

Para reportar la configuración MDR o modificarla cuando la infraestructura informática sufra algún cambio, escribe la información en los campos mostrados a continuación.

General

Campo	Descripción
Sector de la empresa del cliente	Indica el sector / industria a la que pertenece tu empresa.
Número de delegaciones de la empresa	Indica el número de delegaciones que forman tu empresa.
Número de empleados	Indica el número de trabajadores en plantilla que poseen uno o más dispositivos administrados.
Incluye empleados remotos	Indica el número de personas que poseen uno o más dispositivos administrados y que desempeñan su labor fuera de las oficinas de la empresa.

Tabla 18.29: Configuración general MDR

Tecnología

Campo	Descripción
Sistemas operativos	Indica los sistemas operativos instalados en los equipos de la red. Incluye los no protegidos por Cytomic.
Dispositivos de hardware	Indica la marca y el tipo de hardware instalado en la red para identificar de forma temprana las posibles vulnerabilidades existentes. Incluye los no protegidos por Cytomic.
Equipos críticos	Indica los equipos que consideras críticos en el funcionamiento de tu empresa. Puedes añadir equipos individuales o grupos de equipos.

Tabla 18.30: Configuración de la tecnología instalada en la red

Plan de respuesta

Campo	Descripción
Permitir que el Centro de Operaciones de Seguridad de WatchGuard aisle equipos en la red del cliente	Indica si Cytomic está autorizada a utilizar la funcionalidad de aislar equipos como medida de respuesta ante un sistema comprometido. Para más información sobre aislar equipos consulta Aislar un equipo en la página 804 .
Excepciones	Indica los equipos en los que el Cytomic no tiene permitido usar la funcionalidad de aislar equipos como medida de respuesta ante un sistema comprometido. Para más información sobre aislar equipos consulta Aislar un equipo en la página 804 .

Tabla 18.31: Configuración del plan de respuesta

Capítulo 19

Visibilidad del malware y del parque informático

Advanced EDR ofrece al administrador tres grandes grupos de herramientas para visualizar el estado de la seguridad y del parque informático que gestiona:

- El panel de control, con información actualizada en tiempo real.
- Listados personalizables de incidencias, malware detectado y dispositivos gestionados junto a su estado.
- Informes con información del estado del parque informático, recogida y consolidada a lo largo del tiempo.



Los informes consolidados se tratan en *Envío programado de informes y listados* en la página **785** para más información.

Las herramientas de visualización y monitorización determinan en tiempo real el estado de la seguridad de la red y el impacto de las brechas de seguridad que se puedan producir para facilitar la adopción de las medidas de seguridad apropiadas.

Contenido del capítulo

Paneles/Widgets del módulo de seguridad	608
Listados del módulo de seguridad	621

Paneles/Widgets del módulo de seguridad

Advanced EDR muestra mediante widgets el estado de la seguridad del parque informático, o de un equipo concreto:

- **Parque informático:** haz clic en el menú superior **Estado** y en el menú lateral **Seguridad** . Se mostrarán los contadores relativos a la seguridad de los equipos visibles para el administrador. Consulta [Gestión de roles y permisos](#) en la página 67 para establecer los grupos de equipos que serán visibles para la cuenta que accede a la consola de administración, e [Icono Filtro por grupo](#) en la página 39 para restringir la visibilidad de los grupos ya establecida en el rol.
- **Equipo:** haz clic en el menú superior **Equipos**, elige un equipo de la red y haz clic en la pestaña **Detecciones**. Se mostrarán los contadores relativos a la seguridad del equipo seleccionado. Consulta [Sección Detecciones \(4\) en Windows, Linux y macOS](#) en la página 238.

A continuación, se detallan los distintos widgets implementados en el dashboard de Advanced EDR, las distintas áreas y zonas activas incorporadas y los tooltips y su significado.

Estado de protección

Muestra los equipos donde Advanced EDR funciona correctamente y aquellos con errores y problemas en la instalación o en la ejecución del módulo de protección. El estado de los equipos es representado mediante un círculo con distintos colores y contadores asociados.

En la parte inferior del widget se indica el número de equipos que se encuentran en modo auditoría, si los hubiera. Para más información, consulta [Modo auditoría](#) en la página 306



La suma de los porcentajes de las diferentes series puede resultar más de un 100% debido a que los estados no son mutuamente excluyentes, y un mismo equipo puede encontrarse en varias series a la vez.

El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

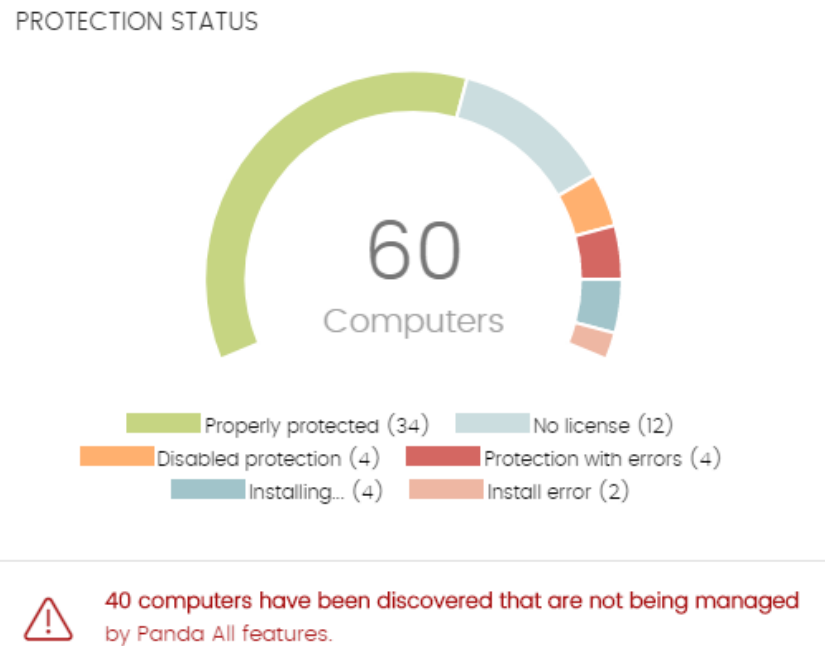


Figura 19.1: Panel de Estado de protección

Descripción de las series

Serie	Descripción
Correctamente protegido	Porcentaje de equipos en los que Advanced EDR se instaló sin errores y su ejecución no presenta problemas.
Instalando...	Porcentaje de equipos en los que Advanced EDR se encuentra en proceso de instalación.
Sin licencia	Equipos sin protección por la falta de suficientes licencias, o por no haberse asignado una licencia disponible.
Protección desactivada	Equipos sin activar la protección avanzada.
Protección con error	Equipos con Advanced EDR instalado cuyo módulo de protección no responde a las peticiones desde los servidores de Cytomic.
Error instalando	Equipos cuya instalación no se pudo completar.
Parte central	Equipos con un agente Cytomic instalado.

Tabla 19.1: Descripción de la serie Equipos desprotegidos

Filtros preestablecidos desde el panel

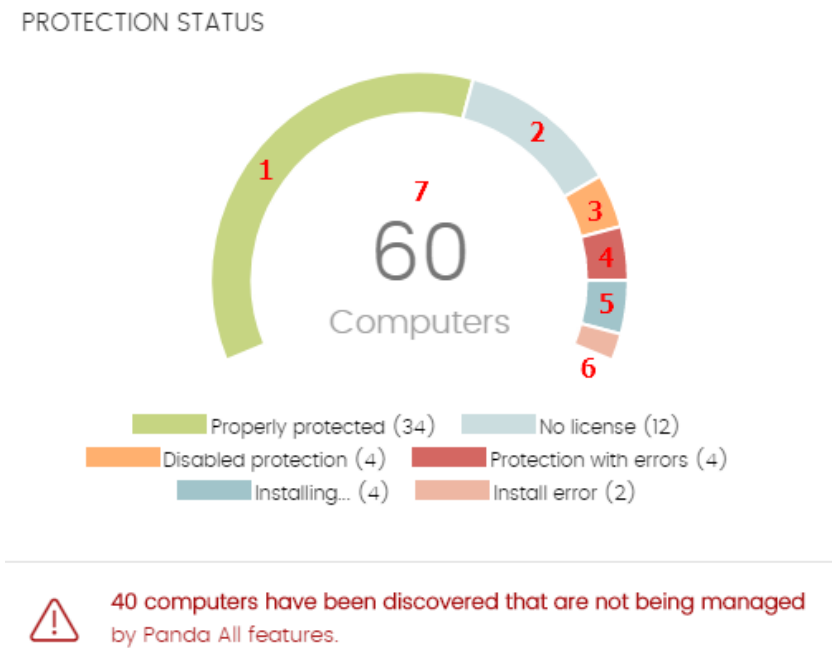


Figura 19.2: Zonas activas del panel Estado de protección

Haz clic en las zonas indicadas en **Zonas activas del panel Estado de protección** para abrir el listado **Estado de protección de los equipos** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de protección = Correctamente protegido.
(2)	Estado de protección = Instalando...
(3)	Estado de protección = Protección desactivada.
(4)	Estado de protección = Protección con error.
(5)	Estado de protección = Sin licencia.
(6)	Estado de protección = Error instalando.
(7)	Sin filtro.

Tabla 19.2: Definición de filtros del listado Estado de protección de los equipos

Equipos sin conexión

Muestra los equipos de la red que no han conectado con la nube de Cytomic en un determinado periodo de tiempo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.



Figura 19.3: Panel Equipos sin conexión

Descripción de las series

Serie	Descripción
72 horas	Número de equipos que no enviaron su estado en las últimas 72 horas.
7 días	Número de equipos que no enviaron su estado en las últimas 7 días.
30 días	Número de equipos que no enviaron su estado en las últimas 30 días.

Tabla 19.3: Descripción de la serie Equipos sin conexión

Filtros preestablecidos desde el panel



Figura 19.4: Zonas activas del panel Equipos sin conexión

Haz clic en las zonas indicadas en [Zonas activas del panel Equipos sin conexión](#) para abrir el listado **Equipos sin conexión** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 72 horas.
(2)	Última conexión = Hace más de 7 días.
(3)	Última conexión = Hace más de 30 días.

Tabla 19.4: Definición de los filtros del listado Equipos sin conexión

Protección desactualizada

Muestra los equipos cuya última versión del fichero de firmas instalada difiere en más de 3 días del fichero publicado por Cytomic. También muestra los equipos cuya versión del motor de protección difiere en más de 7 días del publicado por Cytomic. Por lo tanto, estos equipos pueden ser vulnerables frente a los ataques de amenazas.

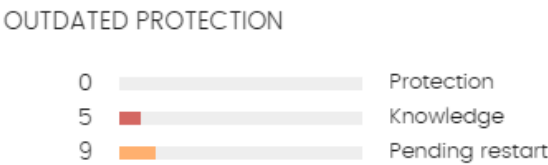


Figura 19.5: Panel Protección desactualizada

Descripción de las series

El panel muestra el porcentaje y el número de equipos vulnerables por estar desactualizados, divididos en tres conceptos:

Serie	Descripción
Protección	Desde hace 7 días el equipo tiene un motor de protección instalado anterior a la última versión publicada por Cytomic.
Conocimiento	Desde hace 3 días el equipo no se actualiza con el fichero de firmas publicado.
Pendiente de reinicio	El equipo requiere un reinicio para completar la actualización.

Tabla 19.5: Descripción de la serie Protección desactualizada

Filtros preestablecidos desde el panel

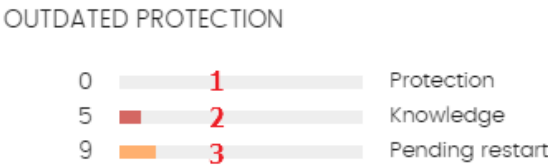


Figura 19.6: Zonas activas del panel Protección desactualizada

Haz clic en las zonas indicadas en **Zonas activas del panel Protección desactualizada** para abrir el listado **Estado de protección de los equipos** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Protección actualizada = No.

Zona activa	Filtro
(2)	Conocimiento = No.
(3)	Protección actualizada = Pendiente de reinicio.

Tabla 19.6: Definición de los filtros del listado Equipos con protección desactualizada

Actividad de malware / PUP

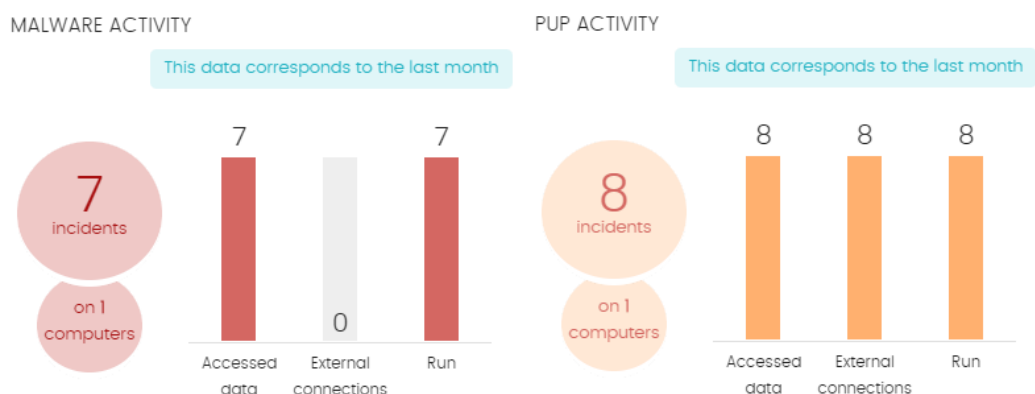


Figura 19.7: Panel de Actividad de malware / PUP

Muestra las incidencias detectadas en los procesos ejecutados por los equipos de usuario y servidores Windows, así como en sus sistemas de ficheros. Estas incidencias son reportadas por el análisis en tiempo real.

Cuando en alguno de los equipos sobre los que el administrador tiene visibilidad se produce una infección al copiar un fichero alojado en otro equipo de la red, se muestran la IP origen de la infección y el número de veces que esta IP ha sido origen de alguna detección (entre paréntesis). Haz clic en el enlace de la IP para acceder al listado Actividad del Malware. Consulta [Actividad de malware / PUP](#).

Para evitar la aparición de muchas repeticiones de una misma amenaza, Advanced EDR muestra como máximo 2 incidencias cada 24 horas por cada tipo de malware encontrado en cada equipo. Además, para registrar la segunda incidencia, debe haber transcurrido al menos 5 minutos desde la primera.

Para algunos tipos de malware específicos, Advanced EDR genera un máximo de 5 incidencias cada 24 horas por cada tipo de malware encontrado en cada equipo.

Descripción de las series

Serie	Descripción
Número de incidencias	Número de incidencias / avisos en Número de equipos detectadas.
Acceso a datos	Número de avisos que incluyen uno o varios accesos a información del usuario contenida en el disco duro de su equipo.

Serie	Descripción
Conexiones exteriores	Número de avisos que establecieron conexiones con otros equipos.
Ejecutado	Número de muestras malware que se llegaron a ejecutar.
Amenazas copiadas desde equipos de la red	Dirección IP origen de la amenaza y número de veces que esta dirección ha sido origen de detección.

Tabla 19.7: Descripción de la serie Actividad de malware / PUP



Actividad de malware, Actividad de PUPs y Actividad de exploits muestran datos con un intervalo máximo de 1 mes. En el caso de que el administrador establezca un periodo de tiempo mayor, se mostrará un texto explicativo en la parte superior del panel.

Filtros preestablecidos desde el panel

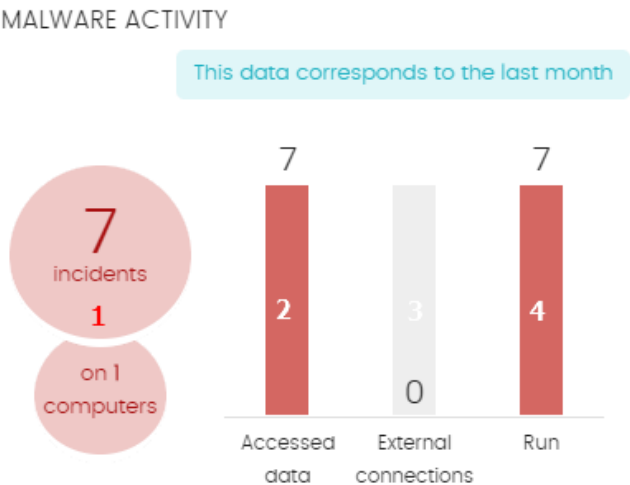


Figura 19.8: Zonas activas del panel Actividad de malware / PUP

Haz clic en las zonas indicadas en **Zonas activas del panel Actividad de malware / PUP** para abrir el listado **Actividad del malware y PUPs** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Tipo de amenaza = (Malware O PUP).
(2)	Acceso a datos = Verdadero.
(3)	Conexiones externas = Verdadero.

Zona activa	Filtro
(4)	Ejecutado = Verdadero.

Tabla 19.8: Definición de los filtros del listado Actividad de malware / PUP

Actividad de exploits

EXPLOIT ACTIVITY

This data corresponds to the last month



Figura 19.9: Panel de Actividad de exploits

Advanced EDR muestra incidencias en el panel Actividad de exploits cuando detecta ataques por explotación de vulnerabilidades en los equipos Windows de la red del cliente.

Para evitar la aparición de muchas repeticiones de una misma amenaza, Advanced EDR muestra como máximo 10 incidencias cada 24 horas por cada tipo de amenaza encontrada en cada equipo .

Descripción de las series

Serie	Descripción
Número de incidencias / ataques	Número de incidencias / ataques en Número de equipos detectadas.

Tabla 19.9: Descripción de la serie Actividad de exploits

Filtros preestablecidos desde el panel

Al hacer clic en cualquier zona del widget se mostrará el listado **Actividad de exploits** filtrado por el último mes.

Actividad de ataques de red

NETWORK ATTACK ACTIVITY



Figura 19.10: Panel de Actividad de ataques de red

Muestra el número de incidencias de Protección contra ataques de red en equipos Windows de la red y el número de equipos en los que se han detectado.

Advanced EDR muestra una incidencia por cada grupo de ataques del mismo tipo recibidos durante el intervalo de una hora y que tengan como destino una misma IP.

Para más información sobre los tipos de ataques de red detectados consulta <https://www.pandasecurity.com/es/support/card?id=700145>.

Descripción de las series

Serie	Descripción
Número de incidencias	Número de incidencias detectadas.
Equipos	Número de equipos en los que se han detectado o bloqueado ataques de red.

Tabla 19.10: Descripción de la serie Actividad de ataques de red

Filtros preestablecidos desde el panel

Al hacer clic en cualquier zona del widget se mostrará el listado **Actividad de ataques de red** filtrado por los últimos 7 días.

Clasificación de todos los programas ejecutados y analizados

CLASSIFICATION OF ALL PROGRAMS RUN AND SCANNED



Figura 19.11: Panel de Clasificación de todos los programas ejecutados y analizados

Localiza de forma rápida el porcentaje de aplicaciones goodware y malware vistas y clasificadas en la red del cliente, para el intervalo de tiempo establecido por el administrador.

Descripción de las series

El panel consta de cuatro barras horizontales junto al número de eventos asociado y el porcentaje sobre el total.



Este panel muestra datos de elementos clasificados para todo el parque informático, y no solo de aquellos equipos sobre los cuales el administrador tenga permisos según sus credenciales de acceso a la consola. Los elementos no clasificados no se muestran en este panel.

Serie	Descripción
Aplicaciones confiables	Aplicaciones vistas en el parque del cliente que han sido analizadas y su clasificación ha sido goodware.
Aplicaciones maliciosas	Programas que han intentado ejecutarse o han sido analizados en el parque del cliente, y han sido clasificadas como malware o ataques dirigidos.
Exploits	Número de intentos de explotación de aplicaciones detectados en la red.
Aplicaciones potencialmente no deseadas	Programas que han intentado ejecutarse o han sido analizados en el parque del cliente, y han sido clasificadas como malware de tipo PUP.

Tabla 19.11: Descripción de la serie Clasificación de todos los programas ejecutados y analizados

Filtros preestablecidos desde el panel

CLASSIFICATION OF ALL PROGRAMS RUN AND SCANNED



Figura 19.12: Zonas activas del panel Clasificación de todos los programas ejecutados y analizados

Haz clic en las zonas indicadas en **Zonas activas del panel Clasificación de todos los programas ejecutados y analizados** para abrir diferentes listados sin filtros preestablecidos:

Zona activa	Filtro
(1)	Listado Actividad del malware.
(2)	Listado Actividad de exploit.
(3)	Listado Actividad de PUPs.

Tabla 19.12: Listados accesibles desde el panel Clasificación de todos los programas ejecutados y analizados

Detecciones mediante políticas avanzadas de seguridad

Muestra los bloqueos de ejecución de scripts sospechosos y programas desconocidos que utilizan técnicas avanzadas de infección.

DETECTIONS BY ADVANCED SECURITY POLICIES

This data corresponds to the last month

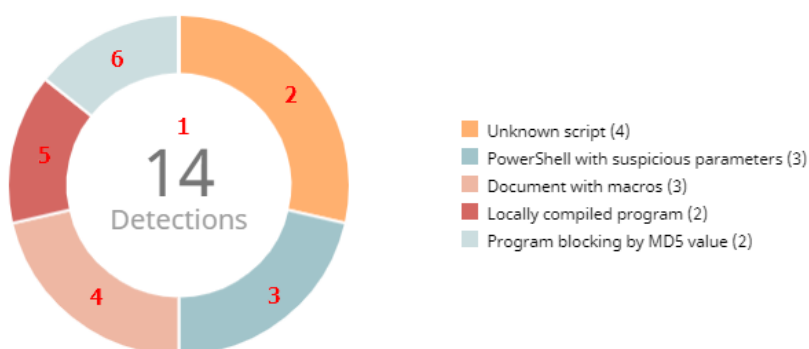


Figura 19.13: Panel Detecciones mediante políticas avanzadas de seguridad

Advanced EDR muestra incidencias en el panel Detecciones mediante políticas avanzadas de seguridad cuando detecta actividad sospechosa en la red del cliente.

Agrupación de detecciones

Para evitar la aparición de muchas repeticiones de una misma detección, Advanced EDR muestra la primera detección sin agrupar, y agrupa en un único registro el resto de detecciones del mismo tipo al

finalizar cada hora.

Para saber si dos detecciones son del mismo tipo, Advanced EDR crea una clave para cada detección con los datos siguientes:

- Identificador del equipo
- Regla de la política avanzada de seguridad que generó la detección
- MD5 del elemento involucrado en la detección para las reglas:
 - Scripts desconocidos
 - Programas compilados localmente
 - Documentos con macros
 - Registro para arranque al inicio de Windows
 - Bloquear programas

Descripción de las series

Serie	Descripción
Detecciones	Número de detecciones totales efectuadas por las políticas de seguridad avanzadas.
PowerShell con parámetros sospechosos	Número de veces que el intérprete Powershell recibe parámetros sospechosos que pueden derivar en la ejecución de operaciones peligrosas en el equipo protegido.
PowerShell ejecutado por el usuario	Número de veces que se intenta ejecutar un script PowerShell monitorizado por una cuenta de tipo interactivo, y por tanto susceptible de ejecutar operaciones peligrosas en el equipo protegido.
Script desconocido	Número de veces que se intenta ejecutar un script que todavía no han sido clasificado por la inteligencia de seguridad de Cytomic.
Programa compilado localmente	Número de veces que se intenta ejecutar un programa desconocido por la inteligencia de seguridad de Cytomic por haber sido compilado en el equipo del usuario.
Documento con macros	Número de veces que se intenta abrir un documento de tipo ofimático que incorpora macros.
Registro para arranque al inicio de Windows	Número de veces que un programa intenta añadir una rama en el registro que le permite ganar persistencia en el equipo para cargarse junto al sistema operativo en cada reinicio.

Serie	Descripción
Bloqueos de programas por MD5	Número de veces que un programa es bloqueado por pertenecer a la lista de MD5s bloqueados establecida por el administrador.
Bloqueos de programas por nombre	Número de veces que un programa es bloqueado por pertenecer a la lista de nombres de programas establecida por el administrador.

Tabla 19.13: Descripción de la serie Detecciones mediante políticas avanzadas de seguridad

Filtros preestablecidos desde el panel

DETECTIONS BY ADVANCED SECURITY POLICIES

This data corresponds to the last month

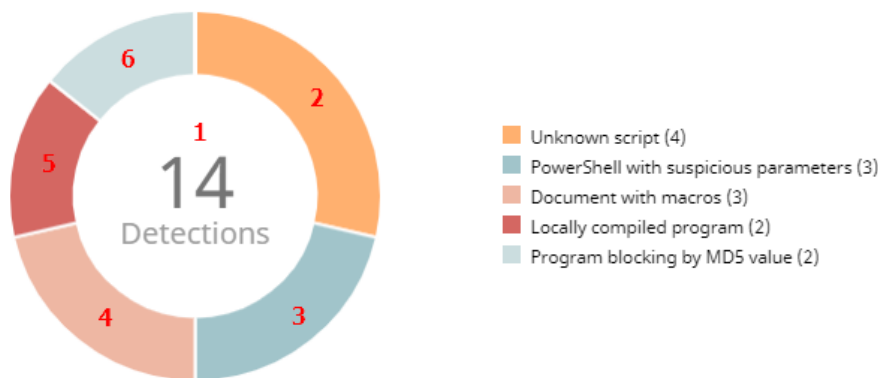


Figura 19.14: Zonas activas del Panel Detecciones mediante políticas avanzadas de seguridad

Haz clic en las zonas indicadas en **Zonas activas del Panel Detecciones mediante políticas avanzadas de seguridad** para abrir el listado **Bloqueos por políticas avanzadas de seguridad** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtro.
(2)	Política aplicada = Script desconocido.
(3)	Política aplicada = PowerShell con parámetros sospechosos.
(4)	Política aplicada = Documento con macros.
(5)	Política aplicada = Programa compilado localmente.

Zona activa	Filtro
(6)	Política aplicada = Bloqueos de programas por MD5.

Tabla 19.14: Definición de filtros del listado Bloqueos por políticas avanzadas de seguridad

Listados del módulo de seguridad

Los listados de seguridad muestran la información de la actividad relativa a la protección de los equipos de la red recogida por Advanced EDR, y cuentan con un grado de detalle muy alto al contener la información en bruto utilizada para generar los widgets.

Para acceder a los listados de seguridad elige uno de los dos procedimientos mostrados a continuación:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad** y en widget para abrir su listado asociado. Dependiendo del lugar donde se haga clic dentro del widget se aplicará un filtro distinto asociado al listado.
- o
- En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una ventana donde se muestran todos los listados disponibles en Advanced EDR.
- Haz clic en un listado de la sección **Seguridad**. Se mostrará el listado apropiado sin filtros establecidos.

Al hacer clic en una entrada del listado se mostrará la ventana de detalle, que se ajustará al tipo de información mostrada.

Estado de protección de los equipos

Muestra en detalle todos los equipos de la red, incorporando filtros que permiten localizar aquellos puestos de trabajo o dispositivos móviles que no estén protegidos por alguno de los conceptos mostrados en el panel asociado.

Para garantizar el buen funcionamiento de la protección, los equipos de la red deben comunicarse con la nube de Cytomic. Consulta el listado de URLs accesibles desde los equipos en [Acceso a URLs del servicio](#) en la página 863.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Estado del equipo	Reinstalación del agente:  Reinstalando agente.	Icono

Campo	Descripción	Valores
	 Error en la reinstalación del agente. Reinstalación de la protección:  Reinstalando la protección.  Error en la reinstalación de la protección.  Pendiente de reinicio. Estado de aislamiento del equipo:  Equipo en proceso de entrar en aislamiento.  Equipo aislado.  Equipo en proceso de salir del aislamiento. Modo Contención de ataque RDP:  Equipo en modo contención de ataque RDP.  Finalizando modo de contención de ataque RDP. Modo detallado del equipo:  Equipo en modo detallado	
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres  Grupo Todos  Grupo nativo  Grupo Directorio activo

Campo	Descripción	Valores
Protección avanzada	Estado de la protección avanzada.	•  Instalando •  Error. Si es conocido se mostrará su origen, si es desconocido se mostrará el código de error •  Activado •  Desactivado •  Sin licencia
Protección actualizada	El módulo de la protección instalado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se muestra la versión de la protección instalada.	•  Actualizado •  No actualizado (7 días sin actualizar desde la publicación) •  Pendiente de reinicio.
Conocimiento	El fichero de firmas descargado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se muestra la fecha de actualización de la versión descargada.	•  Actualizado •  No actualizado (3 días sin actualizar desde la publicación)
Conexión con conocimiento	Indica si el equipo es capaz de comunicarse con la nube de Cytomic para enviar los eventos monitorizados y descargar la inteligencia de seguridad.	•  Conexión correcta •  Uno o varios servicios no son accesibles •  Información no disponible
Última conexión	Fecha del último envío del estado de Advanced EDR a la nube de Cytomic.	Fecha

Tabla 19.15: Campos del listado Estado de protección de los equipos

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del módulo agente Cytomic.	Cadena de caracteres
Fecha instalación	Fecha en la que el Software Advanced EDR se instaló con éxito en el equipo.	Fecha
Fecha de la última actualización	Fecha de la última actualización del agente.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	El módulo de la protección instalado en	Binario

Campo	Descripción	Valores
	el equipo es la última versión publicada.	
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Conocimiento actualizado	El fichero de firmas descargado en el equipo es la última versión publicada.	Binario
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Protección avanzada Antivirus de archivos Bloqueo de programas	Estado de la protección asociada.	• No instalado • Error: si es conocido se mostrará su origen, si es desconocido se mostrará el código de error • Activado • Desactivado • Sin licencia
Modo Protección avanzada (Windows)	Configuración actual del módulo de protección avanzada. Modo de funcionamiento.	• Audit • Hardening • Lock
Modo Protección avanzada (Linux)	Configuración actual del módulo de protección avanzada. Detección de actividad maliciosa.	• Auditar • No detectar • Bloquear
Estado de aislamiento	El equipo esta aislado de la red.	• Aislado • No aislado
Fecha de error	Se produjo un error en la instalación de Advanced EDR en la fecha y hora indicadas.	Fecha
Error instalación	Descripción del error producido en la	Cadena de caracteres

Campo	Descripción	Valores
	instalación de Advanced EDR en el equipo.	
Código error instalación	Muestra código que permite detallar el error producido durante la instalación.	Los códigos se muestran separados por “;”: • Código de error • Código extendido error • Subcódigo extendido error
Otros productos de seguridad	Nombre del antivirus de terceros fabricantes encontrado en el equipo en el momento de la instalación de Advanced EDR.	Cadena de caracteres
Conexión para inteligencia colectiva	Muestra el estado de la conexión del equipo con los servidores que almacenan los ficheros de firmas y la inteligencia de seguridad.	• Correcta • Con problemas
Conexión para envío de eventos	Muestra el estado de la conexión del equipo con los servidores que reciben los eventos monitorizados en los equipos protegidos.	• Correcta • Con problemas
Modo “Contención de ataque RDP”	Estado del modo de Contención de ataque RDP.	• Todos • No • Si

Tabla 19.16: Campos del fichero exportado Estado de protección de los equipos

Herramienta de filtrado

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor

Campo	Descripción	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Advanced EDR a la nube de Cytomic.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Protección actualizada	La protección instalada coincide con la última versión publicada o no.	• Todos • Si • No • Pendiente de reinicio
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS • Android
Conocimiento actualizado	Indica si el fichero de firmas encontrado en el equipo es o no el último publicado.	Binario
Conexión con	Indica si el equipo es capaz de comunicarse con la	• Todos

Campo	Descripción	Valores
servidores de conocimiento	nube de Cytomic para enviar los eventos monitorizados y descargar la inteligencia de seguridad.	• Correcta • Con problemas: uno o varios servicios no son accesibles
Estado de protección	Estado del módulo de protección instalado en el equipo.	• Instalando... • Correctamente protegido • Protección con error • Protección desactivada • Sin licencia • Error instalando
Estado de aislamiento	Configuración del aislamiento del equipo.	• No aislado • Aislado • Aislando • Dejando de aislar
Modo "Contención de ataque RDP"	Estado del modo de Contención de ataque RDP.	• Todos • No • Si

Tabla 19.17: Campos de filtrado para el listado Estado de protección de los equipos

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Para obtener más información, consulta [Información de equipo](#) en la página 218.

Actividad de malware / PUP

Muestra el listado de las amenazas encontradas en los equipos protegidos con Advanced EDR. Este detalle es necesario para poder localizar el origen de los problemas, determinar la gravedad de las incidencias y, si procede, tomar las medidas necesarias de resolución y de actualización de la política de seguridad de la compañía.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres
Amenaza	Nombre de la amenaza detectada.	Cadena de caracteres
Ruta	Ruta completa donde reside el fichero infectado.	Cadena de caracteres
Ejecutado alguna vez	La amenaza se llegó a ejecutar y el equipo puede estar comprometido.	Binario
Ha accedido a datos	La amenaza ha accedido a datos que residen en el equipo del usuario.	Binario
Se ha comunicado con equipos externos	La amenaza se comunica con equipos remotos para enviar o recibir datos.	Binario
Acción	Acción aplicada sobre el malware.	• Movido a cuarentena • Bloqueado • Desinfectado • Eliminado • Detectado • Permitido (modo auditoría)
Fecha	Fecha de la detección de la amenaza en el equipo.	Fecha

Tabla 19.18: Campos del listado de Actividad del malware / PUP

Campos mostrados en fichero exportado



En el menú de contexto de **Listado de actividad Malware / PUP** se muestra un desplegable con dos entradas diferentes: **Exportar** y **Exportar listado y detalles**. En este apartado se muestra el contenido de **Exportar**. Para obtener información sobre **Exportar listado y detalles** consulta **Ficheros exportados Excel** en la página **764**

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres
Amenaza	Nombre de la amenaza detectada.	Cadena de caracteres
Ruta	Ruta completa donde reside el fichero infectado.	Cadena de caracteres
Acción	Acción aplicada sobre el malware.	• Movido a cuarentena • Bloqueado • Desinfectado • Eliminado • Permitido • Permitido (modo auditoría)
Ejecutado	La amenaza se llegó a ejecutar y el equipo puede estar comprometido.	Binario
Acceso a datos	La amenaza ha accedido a datos que residen en el equipo del usuario.	Binario
Conexiones externas	La amenaza se comunica con equipos remotos para enviar o recibir datos.	Binario
Excluido	La amenaza ha sido excluida por el administrador para permitir su ejecución.	Binario

Campo	Comentario	Valores
Fecha	Fecha de la detección de la amenaza en el equipo.	Fecha
Tiempo de exposición	Tiempo que la amenaza ha permanecido en el parque del cliente sin clasificar.	Cadena de caracteres
Usuario	Cuenta de usuario bajo la cual la amenaza se ha ejecutado.	Cadena de caracteres
MD5	Código MD5 del archivo detectado.	Cadena de caracteres
SHA-256	Código SHA-256 del archivo detectado.	Cadena de caracteres
Equipo origen de la infección	Nombre del equipo si el intento de infección viene de un equipo de la red del cliente.	Cadena de caracteres
IP origen de la infección	Dirección IP del equipo si el intento de infección viene de un equipo de la red del cliente.	Cadena de caracteres
Usuario origen de la infección	Usuario registrado en la máquina origen de la infección.	Cadena de caracteres

Tabla 19.19: Campos del fichero exportado Actividad del malware / PUP

Herramienta de filtrado

Campo	Comentario	Valores
Buscar	Equipo: dispositivo donde se realizó la detección. Amenaza: nombre de la amenaza. Hash: Cadena resumen de identificación del archivo. Origen de la infección: busca por el usuario, la IP o el nombre del equipo origen del fichero infectado.	Cadena de caracteres
Tipo	Tipo de amenaza a mostrar.	- Malware - PUP
Fechas	Establece un intervalo de fechas desde el día presente	Últimas 24 horas

Campo	Comentario	Valores
	hacia el pasado.	- Últimos 7 días - Último mes - Último año
Ejecutado	La amenaza se llegó a ejecutar y el equipo puede estar comprometido.	Binario
Acción	Acción aplicada sobre la amenaza.	- Movido a cuarentena - Bloqueado - Desinfectado - Eliminado - Permitido - Detectado
Acceso a datos	La amenaza ha accedido a datos que residen en el equipo del usuario.	Binario
Conexiones externas	La amenaza se comunica con equipos remotos para enviar o recibir datos.	Binario

Tabla 19.20: Campos de filtrado para el listado Actividad del malware / PUP

Ventana de detalle

Muestra información detallada del programa clasificado como malware / PUP. Consulta [Detección del malware y PUP](#) en la página 740.

Actividad de exploits

Muestra el listado de equipos con programas comprometidos por intentos de explotación de vulnerabilidades. Este detalle es necesario para poder localizar el origen los problemas, determinar la gravedad de las incidencias y, si procede, tomar las medidas necesarias de resolución y de actualización de la política de seguridad de la compañía.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres

Campo	Comentario	Valores
Programa o driver comprometido	Programa que recibió el ataque de tipo exploit, o carga de driver vulnerable detectada.	Cadena de caracteres
Técnica de exploit	Identificador de la técnica utilizada para explotar las vulnerabilidades de los programas o drivers.	Cadena de caracteres
Exploit ejecutado	El exploit se llegó a ejecutar o fue bloqueado antes de afectar al programa vulnerable.	Binario
Acción	• Permitido (modo auditoría): se informa al usuario de que el exploit ha realizado las acciones para las que fue programado. Al estar el modo auditoría activado, las amenazas se detectan pero no se bloquean ni eliminan. Consulta Modo auditoría en la página 306 • Permitido: la protección anti-exploit está configurada en modo “Auditar”. El exploit se ejecutó. • Permitido: la protección anti-exploit está configurada en modo “Auditar”. El exploit se ejecutó. No aplicable si la técnica del exploit es Driver vulnerable • Bloqueado: el exploit fue bloqueado antes de su ejecución. • Permitido por el usuario: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continuara ejecutándose. • Proceso finalizado: el exploit fue eliminado, pero se llegó a ejecutar parcialmente. No aplicable si la técnica del exploit es Driver vulnerable. • Pendiente de reinicio: se informó al usuario de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto éste se seguirá ejecutando. No aplicable si la técnica del exploit es Driver vulnerable.	Enumeración
Fecha	Fecha de la detección del intento de exploit en el equipo.	Fecha

Tabla 19.21: Campos del listado de Actividad de exploits

Campos mostrados en fichero exportado



En el menú de contexto de **Actividad de exploits** se muestra un desplegable con dos entradas diferentes: **Exportar** y **Exportar listado y detalles**. En este apartado se muestra el contenido de **Exportar**. Para obtener información sobre **Exportar listado y detalles** consulta **Ficheros exportados Excel** en la página **764**

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres
Programa o driver comprometido	Programa que recibió el ataque de tipo exploit, o driver vulnerable detectado.	Cadena de caracteres
Técnica de exploit	Identificador de la técnica utilizada para explotar las vulnerabilidades de los programas.	Enumeración
Usuario	Cuenta de usuario bajo la cual se ejecutaba el programa que recibió el exploit.	Cadena de caracteres
Acción	• Permitido: la protección anti-exploit está configurada en modo "Auditar". El exploit se ejecutó. No aplicable si la técnica del exploit es Driver vulnerable • Bloqueado: el exploit fue bloqueado antes de su ejecución. • Permitido por el usuario: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continuara ejecutándose. • Proceso finalizado: el exploit fue eliminado, pero se llegó a ejecutar parcialmente. No aplicable si la técnica del exploit es Driver vulnerable. • Pendiente de reinicio: se informó al usuario de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto éste se seguirá ejecutando. No aplicable si la técnica del exploit es Driver vulnerable • Permitido (modo auditoría): se informa al usuario de	Enumeración

Campo	Comentario	Valores
	que el exploit ha realizado las acciones para las que fue programado. Al estar el modo auditoría activado, las amenazas se detectan pero no se bloquean ni eliminan. Consulta Modo auditoría en la página 306	
Exploit ejecutado	El exploit se llegó a ejecutar o fue bloqueado antes de afectar al programa vulnerable.	Binario
Fecha	Fecha de la detección del intento de exploit en el equipo.	Fecha

Tabla 19.22: Campos del fichero exportado Actividad de exploits

Herramienta de búsqueda

Campo	Comentario	Valores
Buscar	• Equipo: dispositivo donde se realizó la detección. • Hash: Cadena resumen de identificación del programa comprometido. • Programa comprometido: nombre del fichero comprometido o de su ruta.	Enumeración
Fechas	Intervalo de fechas desde el día presente hacia el pasado.	• Últimas 24 horas • Últimos 7 días • Último mes
Exploit ejecutado	El exploit se llegó a ejecutar o fue bloqueado antes de afectar al programa vulnerable.	Binario
Acción	• Permitido (modo auditoría): se informa al usuario de que el exploit ha realizado las acciones para las que fue programado. Al estar el modo auditoría activado, las amenazas se detectan pero no se bloquean ni eliminan. Consulta Modo auditoría en la página 306 • Permitido: la protección anti-exploit está configurada en modo "Auditar". El exploit se ejecutó. No aplicable si la técnica del exploit es Driver vulnerable.	Enumeración

Campo	Comentario	Valores
	• Bloqueado: el exploit fue bloqueado antes de su ejecución. • Permitido por el usuario: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continuara ejecutándose. • Proceso finalizado: el exploit fue eliminado, pero se llegó a ejecutar parcialmente. No aplicable si la técnica del exploit es Driver vulnerable. • Pendiente de reinicio: se informó al usuario de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto éste se seguirá ejecutando. No aplicable si la técnica del exploit es Driver vulnerable.	

Tabla 19.23: Campos de filtrado para el listado Actividad de exploits

Ventana de detalle

Muestra información detallada del programa clasificado como exploit. Consulta [Detección exploit](#) en la página [743](#).

Si se trata de un exploit de técnica driver vulnerable, consulta [Detalles del driver](#) en la página [746](#)

Bloqueos por políticas avanzadas de seguridad

Muestra el listado de los programas bloqueados mediante las políticas avanzadas de seguridad. Estas políticas impiden la ejecución de scripts y programas desconocidos que utilizan técnicas avanzadas de infección.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres
Usuario	Cuenta de usuario bajo la cual la amenaza se intentó ejecutar.	Cadena de caracteres
Ruta	Ruta completa donde reside el fichero bloqueado.	Cadena de caracteres
Acción	Acción aplicada sobre el fichero.	• Detectado • Bloqueado • Permitido (modo

Campo	Comentario	Valores
		auditoría)
Política	Para obtener más información, consulta Políticas avanzadas de seguridad en la página 299.	• Powershell con parámetros sospechosos • PowerShell ejecutado por el usuario • Script desconocido • Programa compilado localmente • Documento con macros • Registro para arranque al inicio de Windows • Bloqueos de programas por MD5 • Bloqueos de programas por nombre
Fecha	Fecha de la detección de la amenaza en el equipo.	Fecha

Tabla 19.24: Campos del listado de Bloqueos por políticas avanzadas de seguridad

Campos mostrados en fichero exportado



En el menú de contexto de Bloqueos por políticas avanzadas de seguridad se muestra un desplegable con dos entradas diferentes: Exportar y Exportar listado y detalles. En este apartado se muestra el contenido de Exportar. Para obtener información sobre Exportar listado y detalles, consulta [Ficheros exportados Excel](#) en la página 764

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres

Campo	Comentario	Valores
Política	Consulta Políticas avanzadas de seguridad en la página 299 para obtener más información.	- PowerShell con parámetros sospechosos - PowerShell ejecutado por el usuario - Script desconocido - Programa compilado localmente - Documento con macros - Registro para arranque al inicio de Windows - Bloqueos de programas por MD5 - Bloqueos de programas por nombre
Ruta	Ruta completa donde reside el fichero.	Cadena de caracteres
Acción	Acción aplicada sobre el fichero.	- Detectado - Bloqueado - Permitido (modo auditoría)
Fecha	Fecha de la detección de la amenaza en el equipo.	Fecha
Usuario	Cuenta de usuario bajo la cual la amenaza se intentó ejecutar.	Cadena de caracteres
MD5	MD5 del programa bloqueado.	Cadena de caracteres
SHA-256	SHA-256 del programa bloqueado.	Cadena de caracteres

Tabla 19.25: Campos del fichero exportado Bloqueos por políticas avanzadas de seguridad

Herramienta de filtrado

Campo	Comentario	Valores
Buscar	• Equipo: nombre del dispositivo donde se realizó la detección. • Programa comprometido: nombre del programa bloqueado por la política de seguridad. • Usuario: busca por el nombre del usuario logeado en el equipo cuando se realizó la detección.	Cadena de caracteres
Fechas	Establece un intervalo de fechas desde el día presente hacia el pasado.	• Últimas 24 horas • Últimos 7 días • Último mes • Último año
Acción	Acción aplicada sobre la amenaza.	• Bloqueado • Detectado

Campo	Comentario	Valores
Política aplicada	Para obtener más información, consulta Políticas avanzadas de seguridad en la página 299.	• Powershell con parámetros sospechosos • PowerShell ejecutado por el usuario • Script desconocido • Programa compilado localmente • Documento con macros • Registro para arranque al inicio de Windows • Bloqueos de programas por MD5 • Bloqueos de programas por nombre

Tabla 19.26: Campos de filtrado para el listado Bloqueos por políticas avanzadas de seguridad

Ventana de detalle

Muestra información detallada del programa bloqueado por las políticas de seguridad avanzadas. Consulta [Bloqueo por política avanzada de seguridad](#) en la página 748.

Actividad de ataques de red

Muestra el listado de los ataques de red detectados y bloqueados mediante el módulo Protección contra ataques de red.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Ataque de red	Nombre del ataque de red. Para más información, consulta https://www.pandasecurity.com/es/support/card?id=700145	Cadena de caracteres.
Dirección IP	Dirección IP local del equipo.	Dirección IP

Campo	Descripción	Valores
Local		
Acción	Acción realizada.	• Detectado • Bloqueado
Dirección IP Remota	Dirección IP de origen del ataque.	Dirección IP
Fecha	Fecha de la detección o bloqueo.	Fecha

Tabla 19.27: Campos del listado Actividad de ataques de red

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Ataque de red	Tipo de ataque de red.	Cadena de caracteres
Acción	Acción realizada sobre el ataque.	• Detectar • Bloquear
Dirección IP Local	Dirección IP local del equipo.	Dirección IP
Dirección IP Remota	Dirección IP remota del ataque.	Dirección IP
Puerto local	Puerto local en el que se detecta o bloquea el ataque.	Cadena de caracteres
Puerto remoto	Puerto remoto desde el que se detecta o bloquea el ataque.	Cadena de caracteres
Fecha	Fecha en la detección del ataque.	Fecha
Number of occurrences	Número de detecciones	Cadena de caracteres

Campo	Descripción	Valores
	registradas con el mismo tipo de ataque y la misma IP de origen en una hora.	

Tabla 19.28: Campos del fichero exportado Actividad de ataques de red

Herramienta de búsqueda

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Ataques de red	Tipo de ataque de red.	Cadena de caracteres
Fechas	Rango de fechas.	- Últimas 24 horas - Últimos 7 días - Último mes
Acción	Acción realizada sobre la amenaza.	- Detectado - Bloqueado

Tabla 19.29: Campos de filtrado para el listado Actividad de ataques de red

Ventana de detalle

Campo	Descripción	Valores
Ataque de red	Tipo de ataque de red. Haz clic en el  icono para ver más información.	Cadena de caracteres
Acción	Acción realizada sobre la detección. Consulta No volver a detectar la llegada de tráfico de red sospechoso en la página 708 para obtener información de como gestionar los bloqueos de las amenazas detectadas.	- Detectado - Bloqueado
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.	Nombre: nombre del equipo. Dirección IP: IP del

Campo	Descripción	Valores
		equipo que ha recibido el ataque. • Grupo: carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.
Dirección IP Local	Dirección IP local del equipo.	Dirección IP
Dirección IP Remota	Dirección IP remota del ataque de red.	Dirección IP
Puerto local	Puerto local en el que se detecta o bloquea el ataque de red.	Cadena de caracteres
Puerto remoto	Puerto remoto desde el que se detecta o bloquea el ataque de red.	Cadena de caracteres
Fecha de detección	Fecha en la que se detectó el ataque de red.	Fecha
Número de repeticiones	Numero de detecciones registradas con el mismo tipo de ataque y la misma IP de origen en una hora.	Cadena de caracteres

Tabla 19.30: Campos de la sección Información general en Actividad de ataques de red

Capítulo 20

Evaluación de riesgos

La funcionalidad de evaluación de riesgos permite al administrador de la consola web monitorizar el estado global del riesgo de seguridad de los equipos que gestiona.

Advanced EDR monitoriza y evalúa de forma individual cada configuración y cada módulo de seguridad instalado en los equipos de la red. Cada característica evaluada se compara con una configuración o estado ideal definido por Cytomic. Cuando la configuración ideal y la encontrada en el equipo del usuario difieren, se le asigna un nivel de riesgo a esa característica en concreto.

Al configurar la funcionalidad de evaluación de riesgos, el administrador puede elegir qué aspectos de la seguridad desea monitorizar en el equipo y cuáles no. En el caso de que la funcionalidad evaluada difiera de la configuración ideal, Cytomic establece un nivel de riesgo particular (Medio, Alto o Crítico), aunque el administrador puede cambiarlo en función de sus prioridades.

Una vez evaluado el funcionamiento del software de seguridad del usuario desde todos los ángulos posibles, Advanced EDR calcula un nivel de riesgo global aplicable para todo el equipo, que será el del mayor nivel de riesgo asignado a las distintas configuraciones y características evaluadas.

No todas las características a evaluar son aplicables a todos los sistemas operativos instalados en la red. Cytomic añadirá nuevas comprobaciones con cada versión futura del producto para mejorar progresivamente la evaluación de riesgos.



Para obtener información adicional sobre los distintos recursos de la evaluación de riesgos, consulta las referencias siguientes:

Acceso, control y supervisión de la consola de administración en la [página 59](#) información sobre cómo gestionar cuentas de usuario y asignar permisos.

Gestión de listados en la [página 47](#): información sobre cómo gestionar listados.

Contenido del capítulo

Configuración de la evaluación de riesgos	646

Listados del módulo Evaluación de riesgos	651
Paneles/widgets del módulo Evaluación de riesgos	659

Configuración de la evaluación de riesgos

Permisos requeridos

La evaluación de riesgos es visible para todos los usuarios de la consola web, pero para su configuración es necesario disponer del rol control total. Para más información, consulta [Gestión de roles y permisos](#) en la página 67. La configuración de la evaluación de riesgos se aplica por igual a todos los equipos del parque informático.

Acceso a la configuración

Haz clic en el menú superior **Configuración**, menú lateral **Riesgos**. Se abrirá la ventana **Riesgos**. La información se distribuye en dos zonas principales: la lista de riesgos y los desplegables para asignar los niveles de riesgo correspondientes.

Lista de riesgos

La mayoría de los riesgos tienen que ver con las diferentes configuraciones implementadas por Advanced EDR. Otros riesgos están relacionados con la información sobre el estado de la protección que los equipos envían a los servidores de Cytomic.



Los riesgos disponibles para su evaluación varían en función del sistema operativo instalado en los equipos.

Riesgo	Comentario
Sin protección	El equipo presenta errores en la instalación de la protección o no dispone de licencia. Consulta Estado de protección en la página 608
Protección desactualizada	La versión del motor de la protección instalada en el equipo no está actualizada. El equipo es vulnerable frente a las amenazas. Consulta Sección Detalles (3) en la página 230.
Conocimiento desactualizado (más de 30 días)	La versión del fichero de firmas instalada en el equipo no está actualizada, por lo que el equipo es vulnerable frente a las amenazas. Consulta Protección desactualizada en la página 612.
Sin conectividad con servidores de	Las comunicaciones entre el equipo y los servidores de Cytomic no están funcionando correctamente. El equipo no está debidamente protegido.

Riesgo	Comentario
conocimiento	Consulta Funcionalidades del producto y requisitos en la página 847 para comprobar que el equipo cumple los requisitos de conexión necesarios.
Sin protección ante desinstalación	El equipo no está protegido con contraseña para evitar la desinstalación o modificación de la protección. Consulta Configurar la seguridad frente a manipulaciones no deseadas de las protecciones en la página 285 .
Protección antitamper desactivada	El funcionamiento de la protección podría ser modificado y manipulado. Consulta Configurar la seguridad frente a manipulaciones no deseadas de las protecciones en la página 285 .
Protección avanzada Windows en modo Audit o desactivada	La protección avanzada no está activa o solo informa de las amenazas, pero no bloquea ni desinfecta el malware. Consulta Protección avanzada en la página 296
Protección avanzada Windows en modo Hardening	La configuración de la protección avanzada permite la ejecución de programas desconocidos ya instalados en el equipo y bloquea los provenientes del exterior. Consulta Protección avanzada en la página 296
Protección avanzada Linux en modo Auditar o No detectar o desactivada	La protección avanzada no está activa o se limita a informar de las amenazas pero no las bloquea. Consulta Detectar actividad maliciosa (Sólo Linux) en la página 298 .
Antiexploits en modo Auditar o desactivado	La protección antiexploit no está activa o se limita a informar de la detección pero no emprende acciones contra las amenazas. Consulta Configuración de la detección anti - exploits en la página 303 .
Exclusiones de carpetas, archivos o extensiones	Hay extensiones, archivos o carpetas que no están siendo analizados en busca de malware. • Para saber cómo configurar los elementos que no serán bloqueados, borrados o desinfectados, consulta Archivos y rutas excluidas del análisis en la página 294 • Para saber cómo evitar el bloqueo de determinados programas, consulta

Riesgo	Comentario
	Software autorizado y exclusiones de elementos en la página 526. Para tener más información sobre cómo añadir exclusiones de carpetas, archivos o extensiones, sin que ello repercuta en el nivel de riesgo del equipo, consulta Gestión de las exclusiones.
Indicadores de ataque recientes	El equipo ha informado de la detección de alguna detección de IOA en los últimos 30 días. Solo se tienen en cuenta las detecciones de IOAs en estado Pendiente. Consulta Gestión de detecciones de indicadores de ataque en la página 559.
Parches críticos pendientes de instalación	El equipo tiene instalado Cytomic Patch y notifica la existencia de parches críticos pendientes de instalar. Esta notificación puede producirse de forma inmediata o una vez transcurrido un determinado número de días desde la publicación de los parches. Por defecto el número de días es 30, pero el administrador puede modificarlo al activar este riesgo para su evaluación. Consulta Configuración del descubrimiento de parches sin aplicar en la página 396.
Modo auditoría activado	Al activar el modo auditoría en una configuración, no se modifica el estado global de las diferentes protecciones en los equipos asignados a esa configuración, ni la configuración de las protecciones en la consola web. Las protecciones continúan detectando amenazas en los equipos e informando de ellas, pero no se llevan a cabo labores de bloqueo o desinfección. Consulta Modo auditoría en la página 306
Network Attack Protection disabled or in "Audit" mode	Debido a la configuración de esta protección, el análisis en tiempo real del tráfico de red no está detectando ni deteniendo los movimientos laterales de las amenazas fileless (sin fichero) y ataques avanzados mediante exploits. Consulta Protección contra ataques de red en la página 305

Tabla 20.1: Lista de riesgos

Funcionamiento de la evaluación de riesgos

De forma predeterminada, Cytomic asigna un nivel de riesgo específico a cada riesgo detectado en el equipo. Este nivel de riesgo asignado por defecto se muestra al acceder por vez primera a la ventana **Configuración, Riesgos**. El administrador puede cambiar el nivel de riesgo asignado por defecto y seleccionar el que desee, en función de sus necesidades.

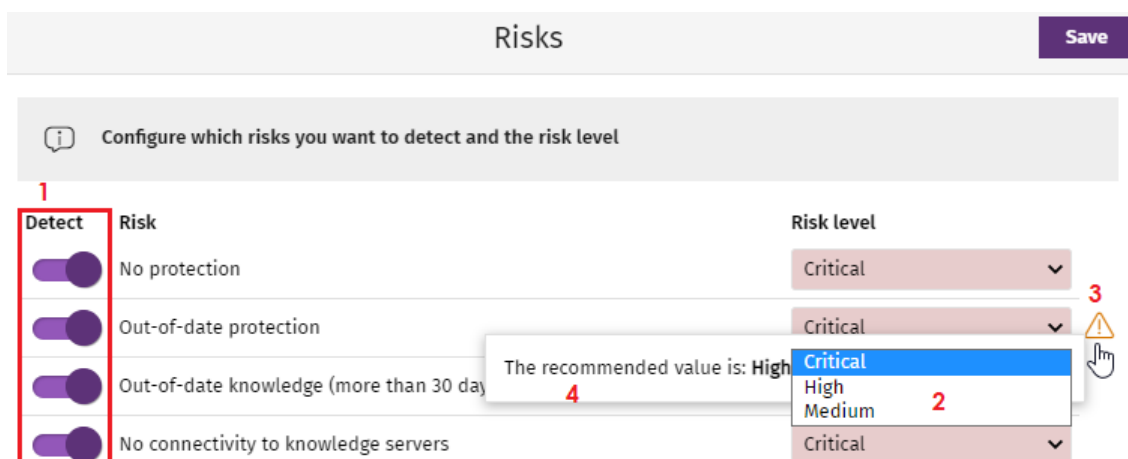


Figura 20.1: Configurar la evaluación de riesgos

Para configurar la evaluación de riesgos:

- En la lista de riesgos (1), activa los que quieres detectar. Para ello, utiliza los controles deslizantes.
- Utiliza el desplegable **Nivel de riesgo** (2), para asignar a cada riesgo su nivel : **Crítico**, **Alto**, **Medio**.
Si el nivel de riesgo que has seleccionado no coincide con el recomendado por Cytomic, se mostrará el icono  (3). Al situar el cursor sobre el icono se mostrará el mensaje (4) recordando cuál es el nivel de riesgo recomendado por Cytomic.
- Haz clic en el botón **Guardar**.



La actualización de riesgos es asíncrona, es decir, puede transcurrir un pequeño margen de tiempo entre la aplicación de la configuración de riesgos y la aparición de los datos en los listados y widgets.

Establecer el nivel de riesgo para IOAs recientes

El riesgo **Indicadores de ataque recientes** se activa cuando se detecta un IOA en el equipo.

A la hora de establecer su nivel de riesgo, el usuario puede:

- Seleccionar en el desplegable **Nivel de riesgo** (2) el nivel **Crítico**, **Alto** o **Medio**.
- Seleccionar en el desplegable **Nivel de riesgo** (2) la opción **Riesgo de los indicadores de ataque**.
De esta forma, el nivel de riesgo se corresponderá con el nivel más alto de riesgo de entre todos los IOAs detectados en el equipo.

Solo se evalúan aquellos IOAs que no han sido previamente archivados o cuya fecha de detección es menor a 30 días.

Por ejemplo:

Se reciben 25 IOAs: algunos de nivel bajo, otros de nivel medio, y uno de nivel alto. El nivel de riesgo para **Indicadores de ataque recientes**, será **Alto**.

Si se archiva el IOA de nivel alto recibido o transcurren los 30 días de plazo, al existir más IOAs sin archivar se establecerá de nuevo el nivel de riesgo que, de acuerdo con la lógica anterior, será de nivel **Medio**.

Por ejemplo:

El equipo informa de la detección de 25 IOAs, todos ellos de nivel bajo excepto 2 de nivel medio. En este caso, el nivel de riesgo es **Medio**.

Si se archiva un IOA de nivel medio el riesgo seguirá siendo el mismo, ya que existe otro IOA de ese nivel. Una vez archivado el IOA de riesgo medio que queda, el nivel del riesgo pasará a ser **Bajo**, que corresponde con el nivel de los 25 IOAs que permanecen sin archivar.

Monitorización de la evaluación de riesgos

Los resultados de la evaluación de riesgos se reflejan en los widgets y listados correspondientes. Para más información, consulta [Listados del módulo Evaluación de riesgos](#) y [Paneles/widgets del módulo Evaluación de riesgos](#).

Modificación y recálculo de los valores recomendados

Cytomic puede modificar los niveles de riesgo recomendados para los diferentes riesgos, pero este cambio no tendrá efecto inmediato sobre los riesgos seleccionados por el administrador, salvo si actualiza a una nueva versión de Advanced EDR, en cuyo caso:

- Los riesgos cuyo nivel de riesgo no haya sido modificado por el usuario, se actualizarán automáticamente con el nuevo valor por defecto recomendado por Cytomic.
- Advanced EDR calculará otra vez el riesgo de todos los equipos y la configuración por defecto mostrará los nuevos niveles de riesgo recomendados.

Cálculo del nivel de riesgo global asignado a cada equipo

La evaluación del nivel de riesgo asignado a cada equipo se produce en dos momentos:

- Para todo el parque informático, con cada actualización de la versión de Advanced EDR.
- Para un equipo concreto, cuando suceden determinadas circunstancias, como por ejemplo asignar configuraciones al equipo, mover los equipos o dispositivos de un grupo a otro, registrar nuevos dispositivos o equipos y, en algunos casos, modificar su asignación de licencias.

El nivel de riesgo global del equipo coincide con el nivel mayor alcanzado en la evaluación de los riesgos.

Por ejemplo:

- En el equipo hay 5 riesgos activos, de los cuáles 1 es de nivel **Alto** y los otros 4 de nivel **Medio**. El nivel de riesgo global del equipo será **Alto**.

- En el equipo hay 5 riesgos, 4 activos (1 de nivel **Alto**, 3 de nivel **Medio**) y 1 riesgo inactivo de nivel **Crítico**. El nivel de riesgo global del equipo será **Alto**.

Gestión de las exclusiones

Para evitar incrementar el riesgo de un equipo al añadir exclusiones a su configuración de Estaciones y servidores, el administrador puede seleccionar cuales de ellas se utilizarán en el calculo del nivel de riesgo del equipo, y cuáles no.

Configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Riesgos**. Se abrirá la ventana **Riesgos**.
- En la lista de riesgos (1), activa el riesgo **Exclusiones de carpetas, archivos o extensiones**.
- Haz clic en el enlace **Gestionar el impacto de las exclusiones**.

La ventana **Gestionar el impacto de las exclusiones** distribuye la información en dos partes:

- En la parte izquierda se muestran todas las exclusiones de carpetas, archivos y extensiones añadidas a todas las configuraciones de Estaciones y servidores creadas en la consola de administración. Estas exclusiones afectan al riesgo de la seguridad y se utilizan para calcular el nivel de riesgo de los equipos. Consulta [Funcionamiento de la evaluación de riesgos y Cálculo del nivel de riesgo global asignado a cada equipo](#).
- En la parte derecha se muestran las exclusiones seleccionadas para que no afecten al estado del riesgo de seguridad, y que no se utilizarán en el cálculo del riesgo global del equipo.

Utiliza  para desplazar a la derecha las exclusiones que NO afectarán al nivel de riesgo de seguridad, y  para devolver las exclusiones a la parte izquierda.

- Para seleccionar varios elementos a la vez, haz clic + Ctrl. Para excluir o devolver todos los elementos, utiliza el enlace **Seleccionar todo**.
- Haz clic en **Guardar**.

Visualizar las exclusiones

El número de exclusiones seleccionadas para que no afecten al estado del riesgo del equipo, se muestra en la ventana de estado de riesgos. Consulta [Paneles/widgets del módulo Evaluación de riesgos](#).

Listados del módulo Evaluación de riesgos

Acceso a los listados

Accede a los listados de evaluación de riesgos siguiendo dos rutas:

- Haz clic en el menú superior **Estado**.
- Haz clic en el menú lateral **Riesgos** y en el widget relacionado.
o
- Haz clic en el menú superior **Estado**.
- En el panel lateral, haz clic en el enlace **Añadir** situado junto a **Mis listados**. Se mostrará la ventana **Añadir listado** con los listados disponibles.
- En la sección **General**, selecciona qué listado de riesgos deseas utilizar: **Riesgos por equipo** o **Riesgos detectados**. Se abrirá la plantilla del listado y podrás modificarla y guardarla. Después, el listado se añadirá a la sección **Mis listados** del panel lateral.

Listado Riesgos por equipo

Este listado ofrece información sobre los riesgos detectados en el equipo o dispositivo y el nivel de los mismos.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Grupo al que pertenece el equipo.	Cadena de caracteres
Última conexión	Fecha y hora del último envío del estado del equipo a la nube de Cytomic.	Fecha/hora
Nivel de riesgo	Nivel de riesgo del equipo o dispositivo. Coincide con el nivel de riesgo mayor detectado en los riesgos activados durante la evaluación.	• Sin riesgo: ninguno de los riesgos ha sido evaluado como crítico, alto o medio. • Crítico: al menos uno de los riesgos ha sido evaluado como crítico. • Alto: el nivel mayor de riesgo detectado durante la evaluación ha sido alto. • Medio: el nivel mayor de riesgo detectado durante la evaluación ha sido medio.
Riesgos del equipo	Gráfica de distribución de los riesgos detectados en el equipo o dispositivo durante la evaluación de riesgos.	• Rojo: número de riesgos críticos. • Naranja: número de riesgos

Campo	Comentario	Valores
		altos. • Amarillo : número de riesgos medios. • Verde: número de riesgos sin impacto en la seguridad. • Gris claro: número de riesgos no compatibles con el sistema operativo del equipo o dispositivo. • Gris oscuro: número de riesgos no evaluados por no haber sido activados por el administrador.

Tabla 20.2: Campos del listado Riesgos por equipo

Al hacer clic en una de las filas del listado, se mostrará la ventana de detalle del equipo. Consulta [Información de equipo](#) en la página 218 y [Sección Detalles \(3\)](#) en la página 230

Campos mostrados en fichero exportado

La información del listado se puede exportar en formato .CSV. Para ello, haz clic en el icono . En el fichero exportado se muestran los datos siguientes:

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres

Campo	Comentario	Valores
Fecha de última conexión	Fecha del último envío del estado del equipo a la nube de Cytomic.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Nivel de riesgo	Nivel de riesgo global del equipo o dispositivo.	• Sin riesgo • Medio • Alto • Crítico
Riesgos críticos	Número de riesgos críticos por equipo.	Numérico
Riesgos altos	Número de riesgos altos por equipo.	Numérico
Riesgos medios	Número de riesgos medios por equipo.	Numérico
Sin riesgo	Número de riesgos sin impacto en la seguridad por equipo.	Numérico
Riesgos no aplican	Número de riesgos no aplicables al equipo según el sistema operativo instalado.	Numérico
Riesgos sin evaluar	Número de riesgos por equipo no activados por el administrador para su evaluación.	Numérico

Tabla 20.3: Campos del fichero exportado Riesgos por equipo

Herramienta de filtrado

Para acceder a la herramienta de filtrado, haz clic en el enlace **Filtros**, situado junto a la caja de búsqueda de la ventana **Riesgos por equipo**. Los campos de filtrado son los siguientes:

Campo	Comentario	Valores
Buscar equipo	Filtra los equipos según su nombre.	Cadena de caracteres
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil

Campo	Comentario	Valores
		• Servidor
Última conexión	Fecha del último envío de riesgos por equipo a la nube de Cytomic.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Riesgo detectado	Riesgo que ha sido activado por el administrador para su evaluación.	• Todos • Sin protección • Protección desactualizada • Sin conectividad con servidores de conocimiento • Sin protección ante desinstalación • Protección antitamper desactivada • Protección avanzada Windows en modo Audit o desactivada • Protección avanzada Windows en modo Hardening • Protección avanzada Linux en modo Auditar o No detectar o desactivada • Antiexploits en modo Auditar o desactivado • Exclusiones de carpetas, archivos o extensiones

Campo	Comentario	Valores
		- Indicadores de ataque recientes - Parches críticos pendientes de instalación - Modo auditoría activado - Network Attack Protection disabled or in "Audit" mode
Nivel de riesgo	Nivel de riesgo asignado	- Crítico - Alto - Medio - Sin riesgo

Tabla 20.4: Campos de filtrado para el listado Riesgos por equipo

Listado Riesgos

El listado **Riesgos** muestra los riesgos activados por el administrador para su evaluación y el número de equipos afectados según el nivel de cada riesgo. Al hacer clic sobre una de las líneas del listado, accederás al listado **Riesgos por equipo**.

El listado **Riesgos** muestra los datos siguientes:

Campo	Comentario	Valores
Riesgo	Nombre del riesgo.	Cadena de caracteres
Equipos	Número de equipos en los que ha sido detectado el riesgo.	Numérico
Nivel de riesgo	Nivel de riesgo asignado.	- Crítico - Alto - Medio - Riesgo de los indicadores de ataque (consulta Configuración de la evaluación de riesgos).
Riesgo por	Gráfica de distribución que indica el número de	Rojo: número de equipos

Campo	Comentario	Valores
equipos	equipos en los que el riesgo ha sido detectado y con determinado nivel de riesgo asignado (Crítico, Alto, Medio) o sin riesgo (seleccionados por el administrador pero no detectados).	en los que el riesgo ha sido detectado con nivel Crítico asignado. • Naranja: número de equipos en los que el riesgo ha sido detectado con nivel Alto asignado. • Amarillo: número de equipos en los que el riesgo ha sido detectado con nivel Medio asignado. • Gris claro: número de equipos en los que el riesgo no ha sido evaluado por no ser compatible con el sistema operativo. • Gris oscuro: numero de equipos en los que el riesgo no ha sido evaluado por no haber sido activado para su evaluación por el administrador.

Tabla 20.5: Campos del listado Riesgos

Campos del fichero exportado

La información del listado se puede exportar en formato .CSV. Para ello, haz clic en el icono . En el fichero exportado se muestran los datos siguientes:

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Riesgo	Nombre del riesgo activado por el administrador para su evaluación.	Cadena de caracteres

Campo	Comentario	Valores
Nivel de riesgo	Nivel de riesgo asignado.	- Crítico - Alto - Medio
Equipos con riesgo detectado	Número de equipos en los que se ha detectado el riesgo.	Numérico
Crítico	Número de equipos de la cuenta con nivel de riesgo Crítico.	Numérico
Alto	Número de equipos de la cuenta con nivel de riesgo Alto.	Numérico
Medio	Número de equipos de la cuenta con nivel de riesgo Medio.	Numérico
Equipos sin riesgo	Número de equipos en los que no se ha detectado el riesgo.	Numérico
Equipos a los que no aplica	Número de equipos en los que no se evalúa el riesgo por ser incompatible con el sistema operativo instalado.	Numérico
Equipos con riesgo no evaluado	Número de equipos en los que el riesgo no ha sido activado para su detección.	Numérico

Tabla 20.6: Campos del fichero exportado Riesgos

Herramienta de filtrado

Para acceder a la herramienta de filtrado, haz clic en el enlace **Filtros**, situado junto a la caja de búsqueda de la ventana **Riesgos**. Los campos de filtrado son los siguientes:

Campo	Comentario	Valores
Tipo de equipo	Filtra los equipos según su clase.	- Estación - Portátil - Servidor

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	- Windows - Linux - macOS

Tabla 20.7: Campos de filtrado para el listado Riesgos



Para programar el envío periódico de los listados de riesgos, consulta [Envío programado de informes y listados](#) en la página 785

Paneles/widgets del módulo Evaluación de riesgos

Acceso al panel de control

Para acceder al panel de control haz clic en el menú superior **Estado**, menú lateral **Riesgos**.

Riesgo de la compañía

Indica el número de equipos sobre los que el usuario tiene visibilidad y cuáles de ellos se encuentran en alguno de los niveles de riesgo establecidos. El estado de los equipos se representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

En la parte inferior del widget se indica el número de exclusiones que no son consideradas riesgo, si las hubiera, de acuerdo con la gestión de las exclusiones realizada. Al hacer clic sobre el mensaje, se accede a la ventana **Gestionar el impacto de las exclusiones**. Consulta [Gestión de las exclusiones](#)

COMPANY RISK

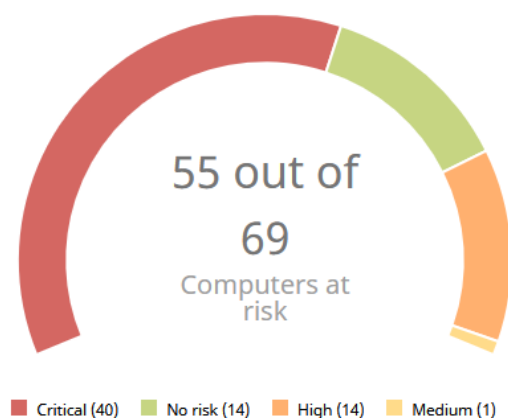


Figura 20.2: Panel Riesgo de la compañía

Significado de las series

Serie	Descripción
Crítico	Número de equipos que se encuentran en nivel de riesgo crítico.
Alto	Número de equipos que se encuentran en nivel de riesgo alto.
Medio	Numero de equipos que se encuentran en nivel de riesgo medio.
Sin riesgo	Número de equipos que no están en situación de riesgo.
Parte central	Suma de todos los equipos que se encuentran en algún nivel de riesgo.

Tabla 20.8: Descripción de la serie Riesgo de la compañía

Filtros preestablecidos desde el panel

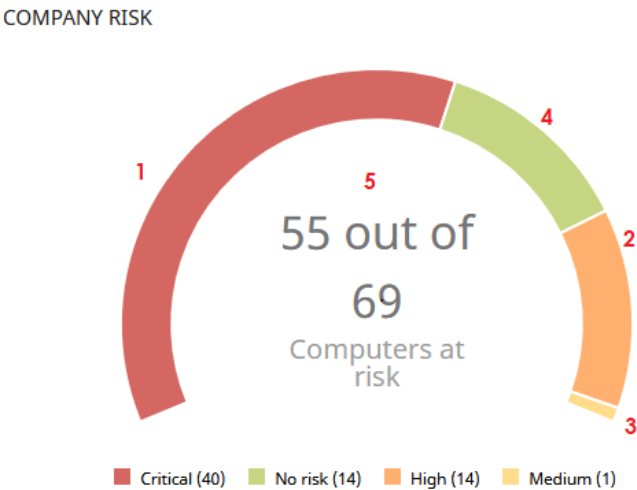


Figura 20.3: Zonas activas del panel Riesgo de la compañía

Al hacer clic en las zonas indicadas en **Zonas activas del panel Riesgo de la compañía** se abre el listado **Riesgos por equipo** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Riesgo = Alto
(2)	Riesgo = Crítico
(3)	Riesgo = Sin riesgo
(4)	Riesgo = Medio

Zona activa	Filtro
(5)	Sin filtros

Tabla 20.9: Zonas activas del panel Riesgo de la compañía

Evolución del riesgo

Indica cómo cambia a lo largo del tiempo el número de equipos que están en un determinado nivel de riesgo.

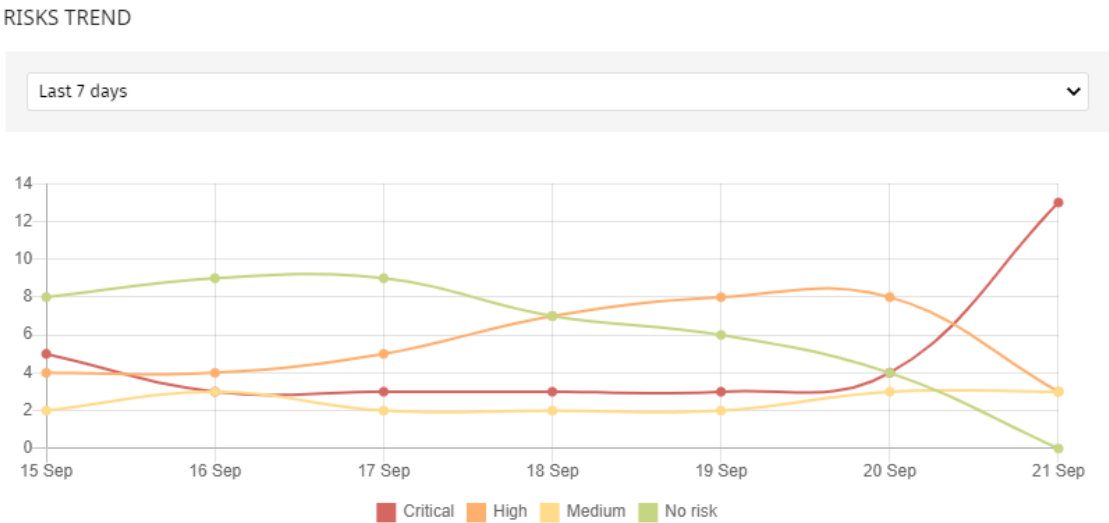


Figura 20.4: Gráfico de Evolución de riesgos

Significado de las series

Serie	Descripción
Riesgo crítico	Evolución del número de equipos en riesgo crítico.
Riesgo alto	Evolución del número de equipos en riesgo alto.
Riesgo medio	Evolución del número de equipos en riesgo medio.
Sin riesgo	Evolución del número de equipos sin riesgo.

Tabla 20.10: Descripción de la serie Evolución del riesgo

Al situar el cursor del ratón sobre uno de los nodos se muestra una etiqueta con la siguiente información:

- Fecha
- Nivel de riesgo
- Número de equipos

Filtros preestablecidos desde el panel

Haz clic sobre los elementos de la leyenda debajo de la gráfica para acceder al listado **Riesgos por equipo** con el filtro correspondiente al tipo seleccionado. Para acceder al listado completo de **Riesgos por equipo** sin aplicar ningún filtro, haz clic sobre cualquier espacio en blanco de la gráfica.

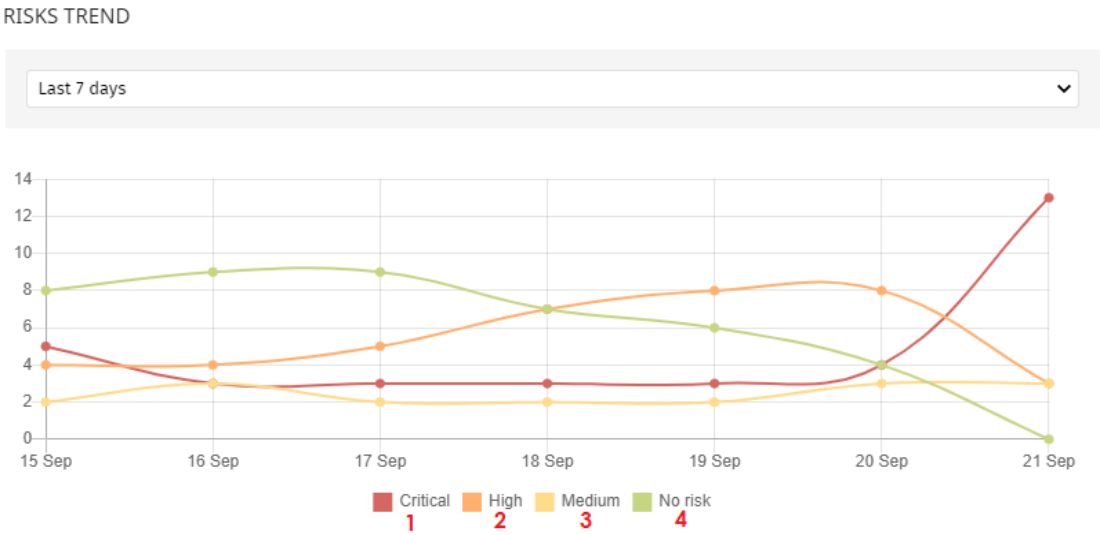


Figura 20.5: Series mostradas en el gráfico Evolución del riesgo

Zona activa	Filtro
(1)	Riesgo= Crítico
(2)	Riesgo= Alto
(3)	Riesgo= Medio
(4)	Sin riesgos

Tabla 20.11: Zonas activas del panel Evolución del riesgo

Riesgos detectados

Muestra una lista de los riesgos que más se han detectado en los equipos.

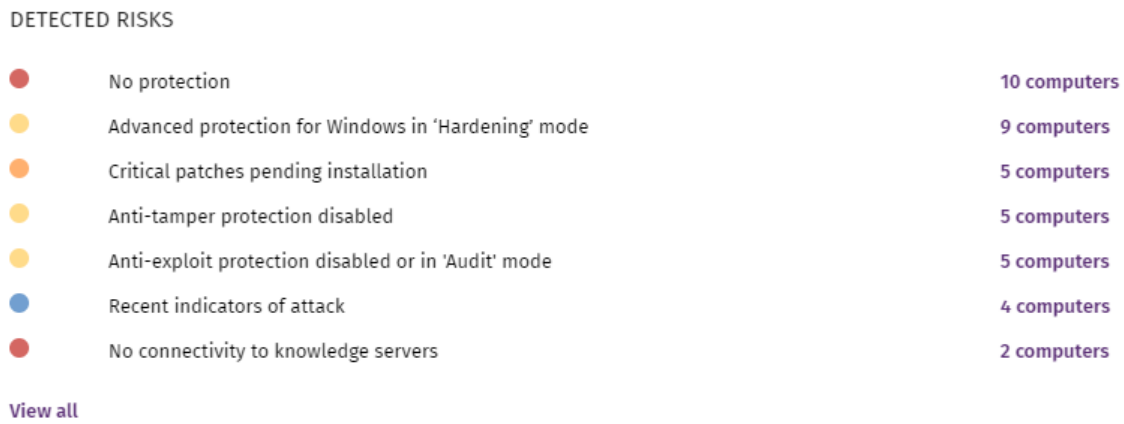


Figura 20.6: Panel Riesgos detectados

Significado de las series

Serie	Descripción
Icono	Nivel del riesgo definido por el administrador. • Rojo: Crítico • Naranja: Alto • Amarillo: Medio • Azul: Personalizado
Nombre	Nombre del riesgo.
Número	Número de equipos en los que se ha detectado el riesgo.
Ver todos	Enlace al listado completo de riesgos detectados.

Tabla 20.12: Descripción de las series del panel Riesgos detectados

Filtros establecidos desde el panel

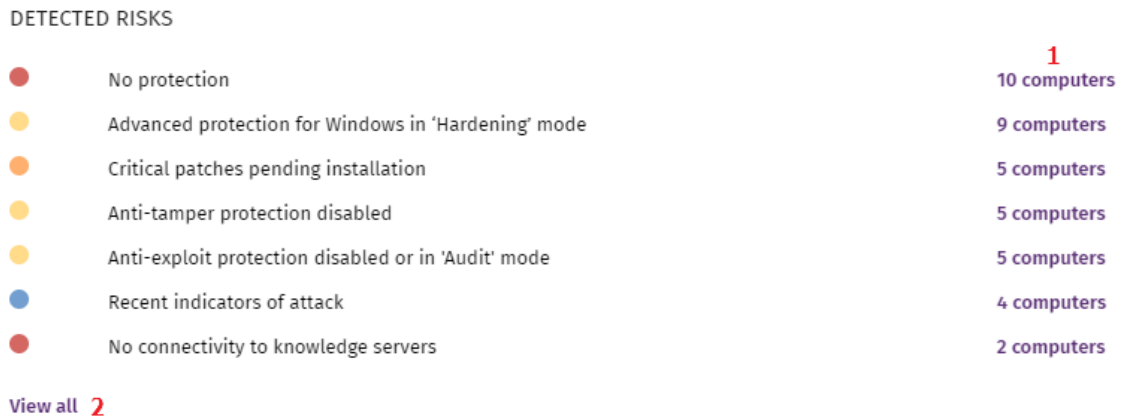


Figura 20.7: Series mostradas en el panel Riesgos detectados

Al hacer clic en las zonas indicadas, se muestran listados con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(3)	Riesgos por equipo	Riesgo detectado = Riesgo seleccionado en el widget
(4)	Riesgos	Sin filtros

Tabla 20.13: Zonas activas del panel Riesgos detectados

Equipos en riesgo (Top 10)

Muestra una lista de los diez equipos con el nivel de riesgo global más elevado.

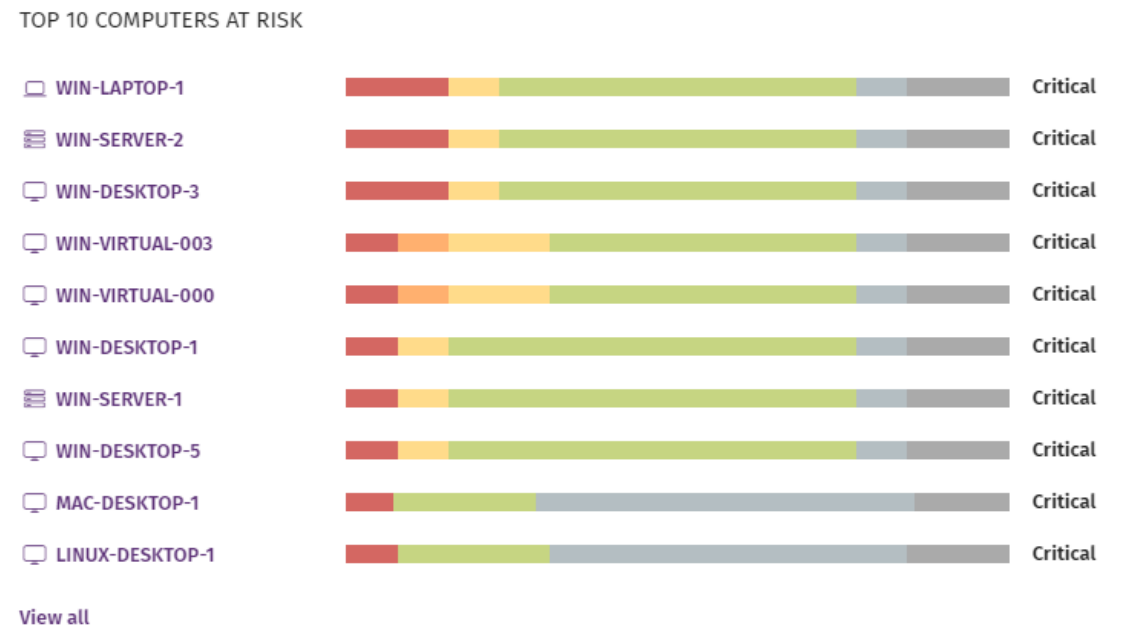


Figura 20.8: Panel Equipos en riesgo (Top 10)



El nivel de riesgo global del equipo coincide con el del riesgo de mayor nivel detectado en el equipo. Para obtener más información consulta [Cálculo del nivel de riesgo global asignado a cada equipo](#)

Significado de las series

Serie	Descripción
Nombre	Nombre y tipo del equipo o dispositivo.
Barra de colores	Gráfica de distribución de riesgos del equipo.
Nivel de riesgo	Nivel de riesgo global asignado al equipo.
Enlace Ver Todos	Acceso al listado completo de riesgos por equipo.

Tabla 20.14: Descripción de las series del panel Equipos en riesgo (Top 10)

Filtros establecidos desde el panel

TOP 10 COMPUTERS AT RISK

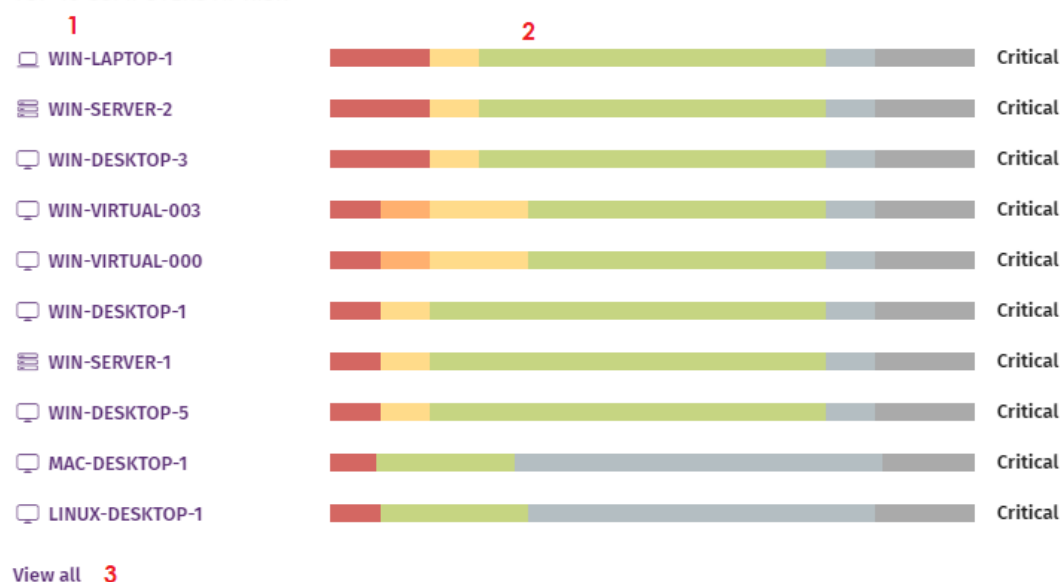


Figura 20.9: Zonas activas del panel Equipos en riesgo (Top 10)

Al hacer clic en las zonas indicadas, se muestran listados con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Detalle del equipo	
(2)	Riesgos	Equipo seleccionado en el widget.
(3)	Riesgos por equipo	Sin filtros

Tabla 20.15: Zonas activas del panel Equipos en riesgo (Top 10)

La información sobre el estado de los riesgos en el equipo está disponible también en la ventana **Detalles del equipo**. Para más información, consulta [Información de equipo](#) en la página 218

Capítulo 21

Evaluación de vulnerabilidades

El módulo Evaluación de vulnerabilidades integrado en la plataforma Cytomic localiza los equipos de la red que contienen software con vulnerabilidades conocidas, e informa sobre la disponibilidad de parches para evitar su impacto en los equipos.

Evaluación de vulnerabilidades es compatible con sistemas operativos Windows macOS y Linux, y detecta aplicaciones de terceros pendientes de actualizar o en EoL (End of Life), así como los parches y actualizaciones publicados por Microsoft para todos sus productos (sistemas operativos, bases de datos, suites ofimáticas, etc.).

Evaluación de vulnerabilidades no instala los parches detectados en los equipos gestionados. El administrador de la red puede instalar los parches necesarios por su cuenta o adquirir el módulo Cytomic Patch para instalar los parches de forma centralizada y desde la misma consola de Advanced EDR.

Para obtener información adicional sobre los distintos apartados del módulo Evaluación de vulnerabilidades, consulta las referencias siguientes:



Crear y gestionar configuraciones en la página **258**: información sobre cómo crear, modificar, borrar o asignar configuraciones a los equipos de la red.

Acceso, control y supervisión de la consola de administración en la página **59**: gestión de cuentas de usuario y asignación de permisos.

Gestión de listados en la página **47**: información sobre cómo gestionar listados.

Contenido del capítulo

Requisitos de la evaluación de vulnerabilidades	668
Configuración de Evaluación de vulnerabilidades	669
Paneles/widgets de Evaluación de vulnerabilidades	671
Listados del módulo Evaluación de vulnerabilidades	686

Requisitos de la evaluación de vulnerabilidades



A partir de la fecha 30/09/2024 no será posible añadir a la consola de administración nuevos equipos que utilicen los siguientes sistemas operativos: Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008 (no afecta a Windows Server 2008 R2). Los equipos instalados en una fecha anterior seguirán protegidos. Consulta <https://www.watchguard.com/wgrd-trust-center/end-of-life-policy>.

Versiones de sistemas operativos Windows compatibles

Estaciones

- Windows 7 (32 y 64 bits)
- Windows 8 (32 y 64 bits)
- Windows 8.1 (32 y 64 bits)
- Windows 10 (32 y 64 bits)
- Windows 11 (64 bits)

Servidores

- Windows 2008 (32 y 64 bits) y 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2 y 2016
- Windows Server 2022

Comportamiento en equipos Windows no compatibles con Evaluación de vulnerabilidades

- No se instalará el módulo en los equipos.
- Los equipos conservarán las configuraciones de evaluación de vulnerabilidades que tenían asignadas, pero no les serán aplicadas.
- En el listado **Parches disponibles por equipos** no se incluirá información sobre estos equipos.

Versiones de sistemas operativos macOS compatibles

- macOS 10.15 Catalina
- macOS 11 Big Sur
- macOS 12 Monterey
- macOS Ventura.
- macOS Sonoma

Versiones de sistemas operativos Linux compatibles

Distribuciones de 64 bits soportadas:

- **Red Hat:** 7.0, 8.0
- **CentOS:** 7.0
- **SuSE Linux Enterprise:** 12, 15.

Configuración de Evaluación de vulnerabilidades

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Evaluación de vulnerabilidades**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración.

Permisos requeridos

Permiso	Tipo de acceso
Configurar evaluación de vulnerabilidades	Crear, modificar, borrar, copiar o asignar las configuraciones de Evaluación de vulnerabilidades.

Permiso	Tipo de acceso
Visualizar parches disponibles	Visualizar las configuraciones de Evaluación de vulnerabilidades.

Tabla 21.1: Permisos requeridos para acceder a la configuración de Evaluación de vulnerabilidades

Configuración general

Haz clic en el selector **Buscar parches automáticamente** para activar la búsqueda de parches. Si el selector no está activado, los parches pendientes de instalación no se mostrarán en los listados.

El administrador de la red puede decidir entre instalar los parches de forma manual o utilizar herramientas de terceros para ello. Sin embargo, al adquirir el módulo Cytomic Patch podrá llevar a cabo la instalación de los parches de forma centralizada y automática, y desde la misma consola de Advanced EDR.

Frecuencia de la búsqueda

Buscar parches con la siguiente frecuencia establece cada cuanto tiempo consulta la evaluación de vulnerabilidades los parches instalados en los equipos y los compara con las bases de datos de parches disponibles.

Criticidad de los parches

Establece la criticidad de los parches que Evaluación de vulnerabilidades busca en las bases de datos de parches disponibles.

En el caso de los equipos y dispositivos con sistema operativo macOS o Linux, no se aplican parches de tipo Windows Service Pack.

La criticidad de cada parche está establecida por cada proveedor del software afectado por la vulnerabilidad. Este criterio de clasificación no es uniforme y se recomienda comprobar previamente la descripción del parche para aquellos que no estén clasificados como “críticos”, con el objetivo de evitar su instalación si no se padecen los síntomas descritos.



*Las criticidades relacionadas con parches de resolución de bugs y mejoras para macOS y Linux, se incluyen dentro de la categoría **Otros parches (no de seguridad)**.*

Paneles/widgets de Evaluación de vulnerabilidades

Descubre Cytomic Patch

Cytomic Patch es un módulo integrado en la plataforma Cytomic que localiza los equipos de la red que contienen software con vulnerabilidades conocidas, y los actualiza de forma automática y centralizada.

Para acceder a más información sobre Cytomic Patch, haz clic en los enlaces **Ver vídeo** o **Más información**.

Para cerrar el panel informativo o para que no se muestre de nuevo, haz clic en el icono .

Acceso al panel de control

Para acceder al panel de control, haz clic en el menú superior **Estado**, panel lateral **Evaluación de vulnerabilidades**

Permisos requeridos

Permisos	Acceso al widget
Sin permisos	• Estado de evaluación de vulnerabilidades • Tiempo desde la última comprobación
Visualizar parches disponibles	• Programas “End Of Life” • Parches disponibles • Evolución de los parches disponibles • Parches disponibles en más equipos • Programas con más parches disponibles

Tabla 21.2: Permisos requeridos para los widgets de Evaluación de vulnerabilidades

Estado de la evaluación de vulnerabilidades

Muestra los equipos donde la evaluación de vulnerabilidades está funcionando correctamente y aquellos con errores o problemas en la instalación o en la ejecución del módulo. El estado del módulo se representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

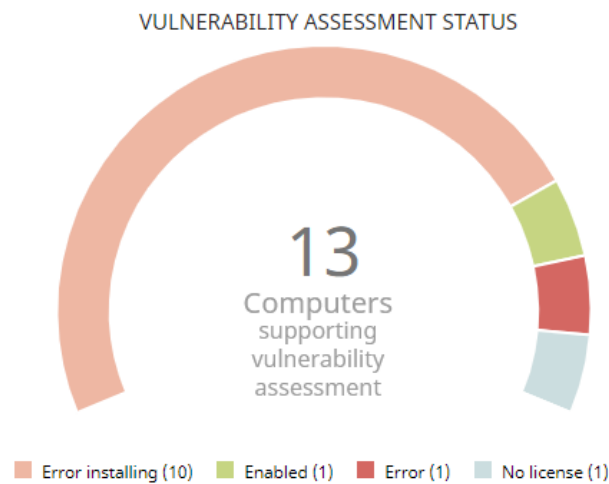


Figura 21.1: Panel de Estado de evaluación de vulnerabilidades

Significado de las series

Serie	Descripción
Activado	Indica el porcentaje de equipos en los que el módulo de evaluación de vulnerabilidades se instaló sin errores, su ejecución no presenta problemas y la configuración asignada permite buscar parches automáticamente.
Desactivado	Indica el porcentaje de equipos en los que el módulo de evaluación de vulnerabilidades se instaló sin errores, su ejecución no presenta problemas y la configuración asignada no permite buscar parches automáticamente.
Sin licencia	Equipos sin servicio de evaluación de vulnerabilidades, debido a que no se poseen licencias suficientes de Advanced EDR o no se les ha asignado una licencia disponible.
Error instalando	Indica los equipos donde el módulo no se pudo instalar.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con el agente sin actualizar.
Error	El módulo de evaluación de vulnerabilidades no responde a las peticiones del servidor y su configuración difiere de la establecida en la consola web.
Parte central	Refleja el número de total de equipos compatibles con la evaluación de vulnerabilidades.

Tabla 21.3: Descripción de la serie Estado de evaluación de vulnerabilidades

Filtros preestablecidos desde el panel

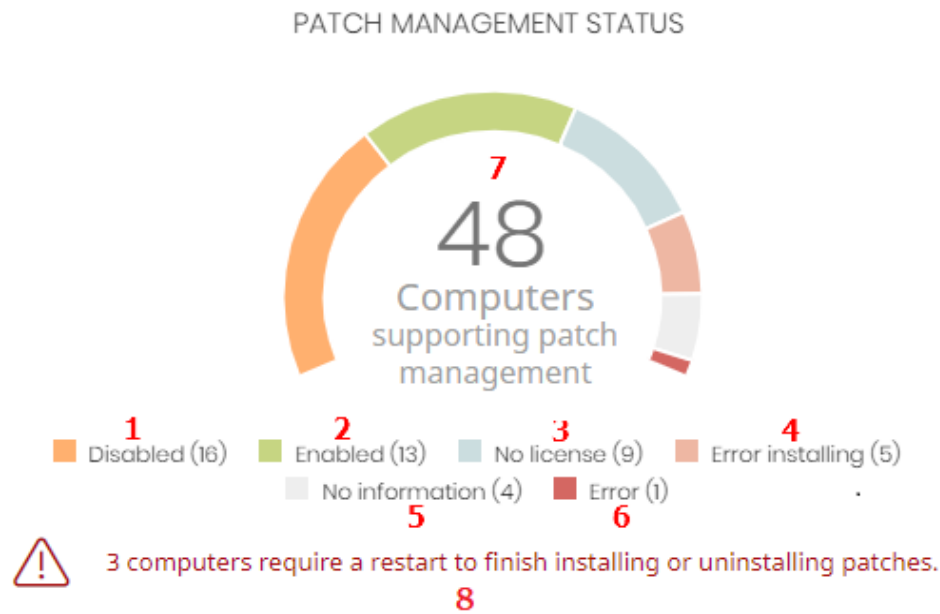


Figura 21.2: Zonas activas del panel Estado de evaluación de vulnerabilidades

Al hacer clic en las zonas indicadas en **Zonas activas del panel Estado de evaluación de vulnerabilidades** se abre el listado **Estado de la evaluación de vulnerabilidades** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de evaluación de vulnerabilidades = Desactivado.
(2)	Estado de evaluación de vulnerabilidades = Activado.
(3)	Estado de evaluación de vulnerabilidades = Sin licencia.
(4)	Estado de evaluación de vulnerabilidades = Error instalando.
(5)	Estado de evaluación de vulnerabilidades = Sin información.
(6)	Estado de evaluación de vulnerabilidades = Error.
(7)	Sin filtro.

Tabla 21.4: Definición de filtros del listado Estado de evaluación de vulnerabilidades

Tiempo desde la última comprobación

Muestra los equipos de la red que no han conectado con la nube de Cytomic en un determinado periodo de tiempo para comprobar su estado de parcheo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.



Figura 21.3: Panel Tiempo desde la última comprobación

Significado de las series

Serie	Descripción
72 horas	Número de equipos que no comprobaron su estado de parcheo en las últimas 72 horas.
7 días	Número de equipos que no comprobaron su estado de parcheo en las últimas 7 días.
30 días	Número de equipos que no comprobaron su estado de parcheo en los últimos 30 días.

Tabla 21.5: Descripción de la serie Tiempo desde la última comprobación

Filtros preestablecidos desde el panel

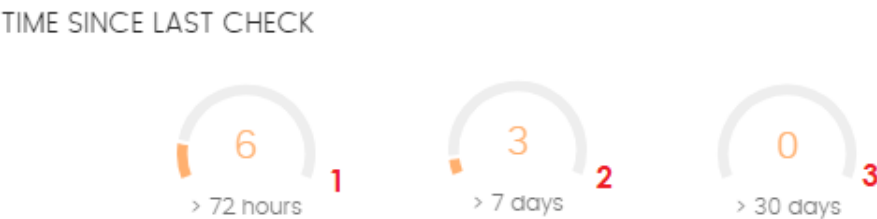


Figura 21.4: Zonas activas del panel Tiempo desde la última comprobación

Al hacer clic en las zonas indicadas en **Zonas activas del panel Tiempo desde la última comprobación** se abre el listado **Estado de la evaluación de vulnerabilidades** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 3 días y Estado de vulnerabilidades =

Zona activa	Filtro
	Activado o Desactivado o Sin información o Error.
(2)	Última conexión = Hace más de 7 días y Estado de vulnerabilidades = Activado o Desactivado o Sin información o Error.
(3)	Última conexión = Hace más de 30 días y Estado de vulnerabilidades = Activado o Desactivado o Sin información o Error.

Tabla 21.6: Definición de filtros del listado Estado de la evaluación de vulnerabilidades

Programas “End of life”

Muestra la información relativa al “end of life” de los programas instalados en los equipos de la red, agrupados según el plazo restante.



Figura 21.5: Panel Programas “End of life”

Significado de las series

Serie	Descripción
Actualmente en EOL	Programas instalados en el parque informático que ya entraron en EOL.
Actualmente o en 1 año en EOL	Programas instalados en el parque informático que ya han entrado en EOL o entrarán dentro de un año.
Con fecha EOL conocida	Programas instalados en el parque informático cuya fecha de EOL es conocida.

Tabla 21.7: Descripción de la serie Programas “End of life”

Filtros preestablecidos desde el panel



Figura 21.6: Zonas activas del panel Programas "End of life"

Al hacer clic en las zonas indicadas en **Zonas activas del panel Programas "End of life"** se abre el listado **Programas "End Of Life"** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Fecha de End Of Life = Actualmente en "End Of Life".
(2)	Fecha de End Of Life = Actualmente o en 1 año en "End Of Life".
(3)	Fecha de End Of Life = Todos.

Tabla 21.8: Definición de filtros del listado Programas "End Of Life"

Parches disponibles

Muestra un recuento de parches disponibles, distribuido por la categoría del parche. Cada parche no aplicado se contabiliza tantas veces como equipos no lo tengan instalado.

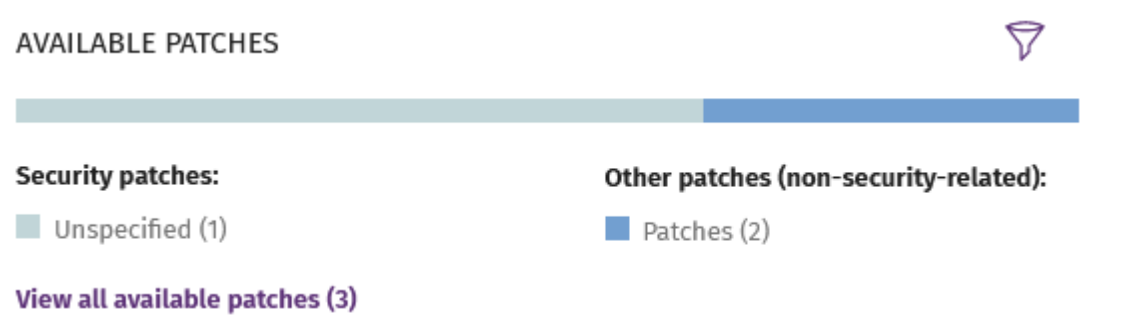


Figura 21.7: Panel parches disponibles

Significado de las series

Serie	Descripción
Parches de seguridad - Críticos	Número de parches clasificados como de importancia crítica relativos a la seguridad del sistema y que no han sido aplicados todavía.

Serie	Descripción
Parches críticos seguridad - Importantes	Número de parches clasificados de importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - Baja	Número de parches clasificados como de importancia baja relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - No clasificados	Número de parches sin determinar su importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Otros parches (no de seguridad)	Número de parches no relativos a la seguridad del sistema y que no han sido aplicados todavía.
Service Packs	Número de paquetes de parches y actualizaciones que no han sido aplicados todavía. No aplicable a equipos con sistema operativo Linux o macOS.

Tabla 21.9: Descripción de la serie Parches disponibles

Filtros preestablecidos desde el panel

AVAILABLE PATCHES



Figura 21.8: Zonas activas del panel Parches disponibles

Al hacer clic en las zonas indicadas en **Zonas activas del panel Parches disponibles** se abre un listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Criticidad = Crítica (de seguridad).
(2)	Criticidad = Importante (de seguridad).

Zona activa	Filtro
(3)	Criticidad = Baja (de seguridad).
(4)	Criticidad = No clasificado (de seguridad).
(5)	Criticidad = Otros parches (no de seguridad).
(6)	Criticidad = Service Pack.
(7)	Sin filtros.

Tabla 21.10: Definición de filtros del listado Parches disponibles por equipos

Filtros disponibles sobre el widget

Al hacer clic en el icono  se muestran los filtros disponibles, que se aplican sobre la información mostrada en el propio widget:

Filtro	Definición
Tipo de equipo	• Estación • Portátil • Servidor
Plataforma	• Todos • Windows • Linux • macOS
Tipo de parche	• Parches de sistema operativo: parches disponibles para sistemas operativos Windows, Linux y macOS. • Parches de aplicaciones: parches disponibles para las aplicaciones.

Tabla 21.11: Filtros disponibles para el widget Evolución de Parches disponibles

Evolución de los parches disponibles

Muestra la evolución de los parches pendientes de instalar en los equipos de la red según su criticidad.

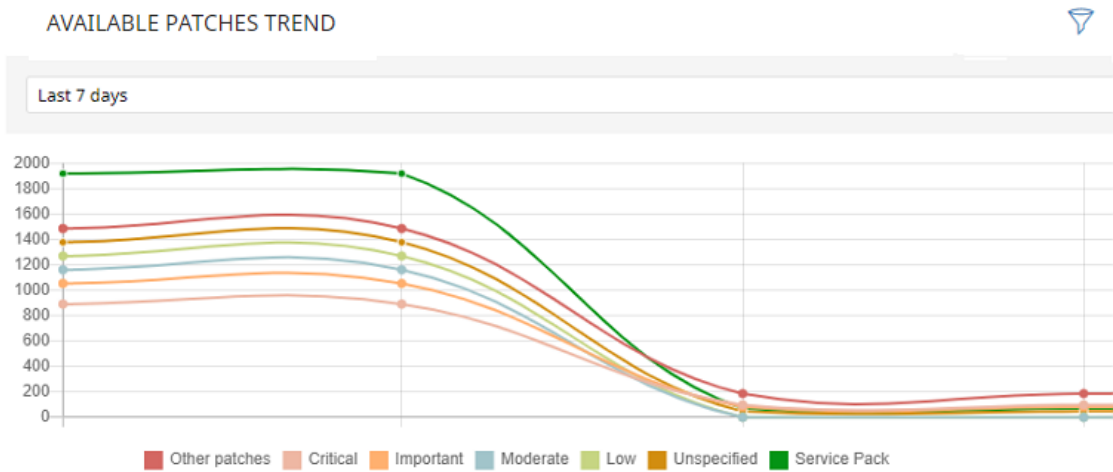


Figura 21.9: Gráfico de Evolución de los parches disponibles

Significado de las series

Serie	Descripción
Parches de seguridad - Críticos	Número de parches clasificados como de importancia crítica relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos seguridad - Importantes	Número de parches clasificados de importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - Baja	Número de parches clasificados como de importancia baja relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - No clasificados	Número de parches sin determinar su importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Otros parches (no de seguridad)	Número de parches no relativos a la seguridad del sistema y que no han sido aplicados todavía.
Service Packs	Número de paquetes de parches y actualizaciones que no han sido aplicados todavía. No aplicable a sistemas operativos macOS y Linux.

Tabla 21.12: Descripción de la serie Evolución de los parches disponibles

Al situar el cursor del ratón sobre uno de los nodos se muestra un tooltip con la siguiente información:

- Fecha
- Tipo

- Número de parches

Filtros preestablecidos desde el panel

Haz clic sobre los elementos de la leyenda debajo de la gráfica para acceder al listado **Parches disponibles por equipos** con el filtro correspondiente al tipo seleccionado. Haz clic sobre la gráfica, para acceder al listado completo de **Parches disponibles por equipos** sin aplicar ningún filtro.

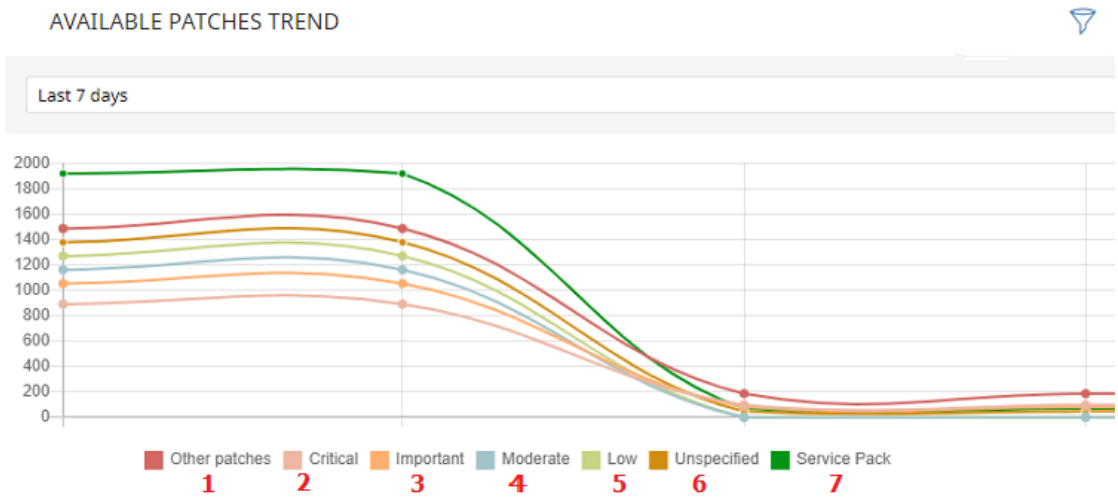


Figura 21.10: Series mostradas en el gráfico Evolución de los parches disponibles

Zona activa	Filtro
(1)	Criticidad = Otros parches (no de seguridad).
(2)	Criticidad = Critica (de seguridad).
(3)	Criticidad = Importante (de seguridad).
(4)	Criticidad = Moderada (de seguridad).
(5)	Criticidad = Baja (de seguridad).
(6)	Criticidad=No clasificado (de seguridad)
(9)	Criticidad = Service Pack.

Tabla 21.13: Definición de filtros del listado Parches disponibles por equipos

Filtros disponibles sobre el widget

Al hacer clic en el icono  se muestran los filtros disponibles, que se aplican sobre la información mostrada en el propio widget:

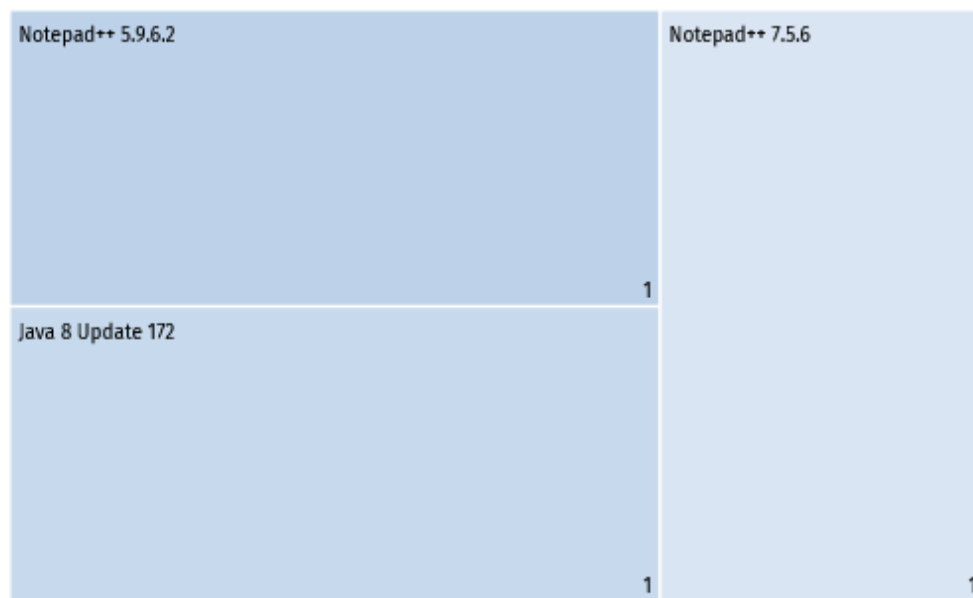
Filtro	Definición
Tipo de equipo	• Estación • Portátil • Servidor
Plataforma	• Todos • Windows • Linux • macOS
Tipo de parche	• Parches de sistema operativo: parches disponibles para sistemas operativos Windows, Linux y macOS. • Parches de aplicaciones: parches disponibles para las aplicaciones.

Tabla 21.14: Filtros disponibles para el widget Evolución de los parches disponibles

Parches disponibles en más equipos

Muestra el número de equipos afectados por cada parche disponible en estado **Pendiente**.

MOST AVAILABLE PATCHES FOR COMPUTERS



[View all available patches \(3\)](#)

Figura 21.11: Panel Parches disponibles en más equipos

Significado de las series

Serie	Descripción
Nombre	Nombre del parche disponible.
Número	Número de equipos con el parche disponible en estado Pendiente .
Enlace Ver todos los parches disponibles	Acceso al listado completo de parches disponibles por equipos.

Tabla 21.15: Descripción de las series de Parches disponibles en más equipos

Al situar el cursor del ratón sobre un cuadro, se muestra un tooltip con la siguiente información:

- Nombre del parche.
- Número de equipos que tienen disponible el parche.
- Programa (o familia del sistema operativo).
- Criticidad.
- Fecha de publicación
- Número CVE (Common Vulnerabilities and Exposures).

Filtros preestablecidos desde el panel

Al hacer clic en cualquiera de los cuadros del panel, se abre el listado **Parches disponibles por equipos**, filtrado por el parche seleccionado.

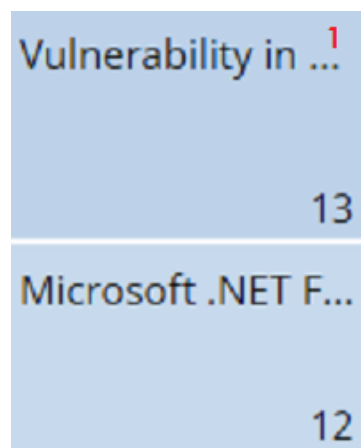


Figura 21.12: Zonas activas del panel Parches disponibles en más equipos

Zona activa	Filtro
(1)	Parche = Nombre del parche seleccionado

Tabla 21.16: Definición de filtros del listado Parches disponibles en más equipos

Filtros disponibles sobre el widget

Haz clic en el icono  para mostrar los filtros disponibles que se aplican sobre la información mostrada en el propio widget:

Filtro	Descripción	Valores
Criticidad	Importancia de la actualización y tipo.	- Otros parches (no de seguridad) - Crítica (de seguridad) - Importante (de seguridad) - Moderada (de seguridad) - Baja (de seguridad) - No clasificado (de seguridad) - Service Pack
Tipo de equipo	Clase de dispositivo al que se aplica el parche.	- Estación - Portátil - Servidor
Plataforma	Sistema operativo instalado en el equipo.	- Todos - Windows - Linux - macOS
Tipo de parche	Tipo de software al que se aplicará el parche.	- Parches de aplicaciones - Parches de sistema operativo

Tabla 21.17: Filtros del panel Parches disponibles en más equipos

Programas con más parches disponibles

Muestra los programas con más parches disponibles para instalar, y su número.

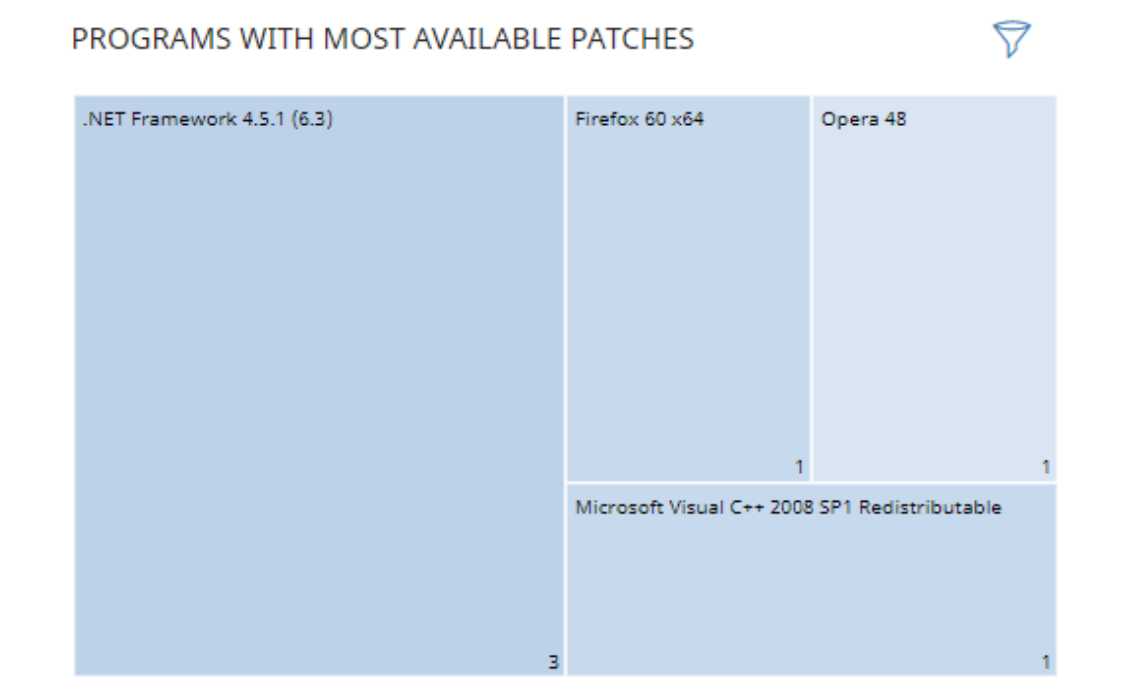


Figura 21.13: Panel Programas con más parches disponibles

Significado de las series

Serie		Descripción	
Nombre		Nombre del programa con más parches disponibles.	
Número		Número de parches disponibles para el programa.	

Tabla 21.18: Descripción de las series del panel Programas con más parches disponibles en más equipos

Al situar el cursor del ratón sobre un cuadro, se muestra una etiqueta con la siguiente información:

- Nombre del programa.
- Número de parches disponibles para el programa.

Filtros preestablecidos desde el panel

Al hacer clic en cualquiera de los cuadros del panel, se abre el listado **Parches disponibles por equipos**.

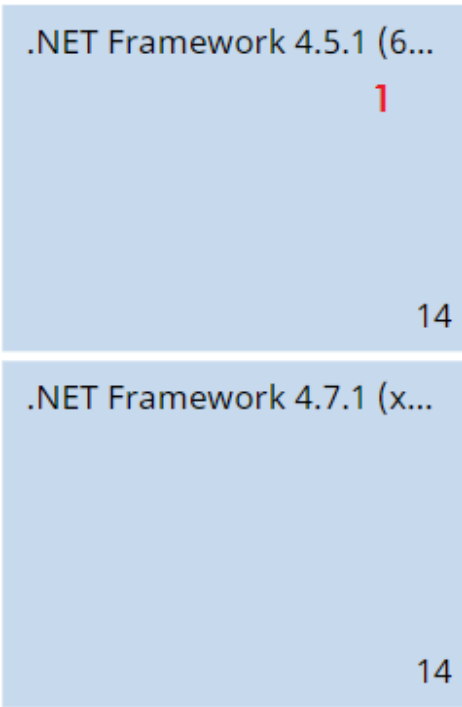


Figura 21.14: Zonas activas del panel Programas con más parches disponibles

Zona activa	Filtro
(1)	Equipo= Nombre del programa seleccionado

Tabla 21.19: Definición de filtros del listado Programas con más parches disponibles

Filtros disponibles sobre el widget

Haz clic en el icono  para mostrar los filtros disponibles:

Filtro	Descripción	Valores
Criticidad	Importancia de la actualización y tipo.	- Otros parches (no de seguridad) - Crítica (de seguridad) - Importante (de seguridad) - Moderada (de seguridad) - Baja (de seguridad) - No clasificado (de seguridad) - Service Pack

Filtro	Descripción	Valores
Tipo de equipo	Clase de dispositivo al que se aplica el parche.	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de parche	Tipo de software al que se aplicará el parche.	• Parches de aplicaciones. • Parches de sistema operativo.

Tabla 21.20: Definición de filtros del panel Programas con más parches disponibles

Listados del módulo Evaluación de vulnerabilidades

Acceso a los listados

El acceso a los listados se podrá hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Evaluación de vulnerabilidades** y en el widget relacionado.
ó
- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se abrirá una ventana emergente con los listados disponibles.
- Selecciona un listado de la sección **Evaluación de vulnerabilidades** para ver su plantilla asociada. Modifica la plantilla y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

Permisos	Acceso a listados
Sin permisos	• Estado de evaluación de vulnerabilidades
Visualizar parches disponibles	Acceso de solo lectura a los listados:

Permisos	Acceso a listados
	• Estado de la evaluación de vulnerabilidades • Parches disponibles por equipos • Programas "End Of Life"

Tabla 21.21: Permisos requeridos para los listados de Evaluación de vulnerabilidades

Estado de la evaluación de vulnerabilidades

Este listado muestra en detalle todos los equipos de la red compatibles con la evaluación de vulnerabilidades, e incorpora filtros que permiten localizar aquellos puestos de trabajo y servidores que no estén recibiendo el servicio por alguno de los conceptos mostrados en el panel asociado.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Estado del equipo	Reinstalación del agente: •  Reinstalando agente. •  Error en la reinstalación del agente Reinstalación de la protección: •  Reinstalando la protección. •  Error en la reinstalación de la protección. •  Pendiente de reinicio. Estado de aislamiento del equipo: •  Equipo en proceso de entrar en aislamiento. •  Equipo aislado. •  Equipo en proceso de salir del aislamiento. Modo Contención de ataque RDP: •  Equipo en modo contención de ataque RDP. •  Finalizando modo de contención: de ataque RDP.	Icono

Campo	Comentario	Valores
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Evaluación de vulnerabilidades	Estado del módulo.	 Activado  Desactivado  Error instalando (motivo del error)  Sin licencia  Sin información  Error
Última comprobación	Fecha en la que la evaluación de vulnerabilidades consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Última conexión	Fecha del último envío del estado de la evaluación de vulnerabilidades a la nube de Cytomic.	Fecha

Tabla 21.22: Campos del listado Estado de la evaluación de vulnerabilidades



Para visualizar los datos del listado gráficamente accede al widget **Estado de la evaluación de vulnerabilidades**

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el módulo se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha de la última vez que el agente se conectó con la nube de Cytomic.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada.	Booleano

Campo	Comentario	Valores
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Estado de la evaluación de vulnerabilidades	Estado del módulo.	• Activado • Desactivado • Error instalando • Sin licencia • Sin información • Error
Fecha de la última comprobación	Fecha en la que la evaluación de vulnerabilidades consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Estado de aislamiento	Indica si el equipo ha sido aislado de la red o se comunica con sus equipos vecinos de forma normal.	• Aislado • No aislado
Fecha error instalación	Fecha en la que se intentó la instalación del módulo y se produjo el error.	Fecha
Error instalación	Motivo del error de instalación.	• Error en la descarga • Error en la ejecución
Error de la evaluación de vulnerabilidades	Error en la búsqueda de parches disponibles.	Numérico

Tabla 21.23: Campos del fichero exportado Estado de la evaluación de vulnerabilidades

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Última comprobación	Fecha en la que la evaluación de vulnerabilidades consultó a la nube para comprobar si se han publicado nuevos parches.	• Todos • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Última conexión	Fecha de la última vez que el agente se conectó con la nube de Cytomic.	Fecha
Estado de la evaluación de vulnerabilidades	Estado del módulo.	• Activado • Desactivado • Error instalando • Sin licencia • Sin información • Error

Tabla 21.24: Campos de filtrado para el listado Estado de la evaluación de vulnerabilidades

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se abrirá la ventana de detalle del equipo. Consulta [Información de equipo](#) en la página 218 para obtener más información.

Parches disponibles por equipos

Muestra el detalle de los parches disponibles y la información sobre los parches que están en proceso de instalación.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Equipos	Número de equipos en los que está disponible el parche.	Numérico

Tabla 21.25: Campos del listado Parches disponibles por equipos



Para visualizar los datos del listado gráficamente accede al widget **Parches disponibles** en la página **407**

Campos mostrados en fichero exportado

Utiliza el menú de contexto para exportar los datos. La exportación puede incluir todos los datos del listado de parches disponibles o una versión más reducida que muestra los datos correspondientes a la evolución de los parches disponibles durante los últimos 7 días, último mes o el último año.

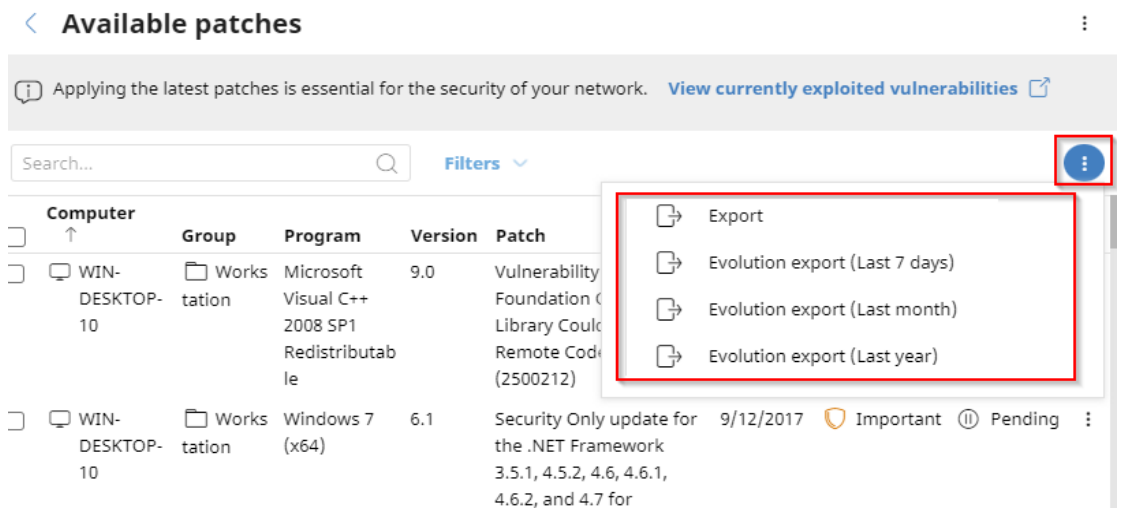


Figura 21.15: Menú de contexto para exportación

Campo	Comentario	Valores
Vendor	Compañía creadora del programa desactualizado.	Cadena de caracteres
Familia de producto	Nombre de producto con parches pendientes de aplicar o reiniciar.	Cadena de caracteres
Versión de programa	Número de versión del programa desactualizado.	Numérico
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información	Cadena de

Campo	Comentario	Valores
	adicional (fecha de publicación, número de la Knowledge base etc.).	caracteres
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador de KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Equipos	Número de equipos en los que está disponible el parche.	Numérico
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS

Tabla 21.26: Campos del fichero exportado Parches disponibles por equipos

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Tipo de parche	Clase de parche disponible.	• Parches de aplicaciones • Parches de sistema operativo
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Selecciona versión de programa, familia o vendor	La búsqueda se aplicará al programa, familia de productos o compañía seleccionada.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches

Campo	Comentario	Valores
		(no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Mostrar parches no descargables	Indica los parches que no son descargables directamente debido a requisitos adicionales del proveedor (aceptación de EULA, introducción de credenciales, captchas etc.).	Booleano

Tabla 21.27: Campos de filtrado para el listado Parches disponibles por equipos

Ventana Parche detectado

Al hacer clic en una de las filas del listado se abrirá la ventana **Parche detectado**, en la que se muestra información detallada sobre el parche. Los datos pueden variar según el sistema operativo instalado en los equipos.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base, etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión de programa	Número de versión del programa desactualizado. No disponible para parches de macOS o Linux.	Cadena de caracteres

Campo	Comentario	Valores
Familia	Nombre de producto con parches pendientes de aplicar o reiniciar. No disponible para parches de macOS o Linux.	Cadena de caracteres
Vendor	Compañía creadora del programa desactualizado. No disponible para parches de macOS o Linux.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera. No disponible para parches de macOS o Linux.	Cadena de caracteres
Descripción	Información sobre el impacto que la vulnerabilidad podría tener en los equipos. No disponible para parches de macOS o Linux.	Cadena de caracteres

Tabla 21.28: Campos de la ventana Parche detectado

Programas “End of Life”

Muestra los programas que ya no tienen soporte por parte de sus proveedores y que por tanto son un objetivo especialmente vulnerable para el malware y las amenazas.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software en EoL.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL.	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha (en rojo si el equipo entró en EOL)

Tabla 21.29: Campos del listado Programas EoL



Para visualizar los datos del listado gráficamente accede al widget **Programas “End of life”** en la página **402**

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux

Campo	Comentario	Valores
		• macOS
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL.	Cadena de caracteres
EoL	Fecha en la que el programa entró en EoL.	Fecha
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha

Tabla 21.30: Campos del fichero exportado Programas EoL

Herramienta de filtrado

Campo	Comentario	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux

Campo	Comentario	Valores
		• macOS
Fecha de "End Of Life"	Fecha en la que el programa entrará en EOL.	• Todos • Actualmente en "End of life" • Actualmente o en "End of life" en 1 año

Tabla 21.31: Campos de filtrado para el listado Programas EoL

Ventana Detalles del programa

Al hacer clic en uno de los programas del listado se accede a la ventana de **Detalles del programa**:

Campo	Comentario	Valores
Programa	Nombre del programa o versión del sistema operativo Windows que recibió el parche.	Cadena de caracteres
Familia	Bundle, suit o grupo de programas al que pertenece el software.	Cadena de caracteres
Editor/Empresa	Empresa que diseñó o publicó el programa.	Cadena de caracteres
Versión	Versión del programa.	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha

Tabla 21.32: Campos de la ventana Detalles del programa

Capítulo 22

Gestión de amenazas, elementos en clasificación y cuarentena

Advanced EDR equilibra la eficacia del servicio de seguridad con el impacto que perciben los usuarios protegidos en su actividad diaria a través de herramientas que gestionan los bloqueos de ejecución de los elementos encontrados:

- Programas clasificados como malware.
- Programas clasificados como PUPs.
- Programas clasificados como Exploits.
- Programas clasificados como virus.
- Programas desconocidos en proceso de clasificación.
- Ataques de red.



*Para obtener más información sobre permitir la ejecución de programas desconocidos en proceso de clasificación consulta [Configuración de software autorizado](#) en la página 525.
Para obtener más información sobre los modos de protección avanzados hardening y lock consulta [Protección avanzada](#) en la página 296.*

Contenido del capítulo

Introducción a las herramientas de gestión de amenazas	702
Permitir y volver a impedir la ejecución de elementos	705

Información de elementos bloqueados en clasificación	710
Listado de amenazas y programas desconocidos permitidos	723
Política de reclasificación	732
Estrategias para supervisar la clasificación de ficheros	735
Gestión de la zona de backup / cuarentena	736

Introducción a las herramientas de gestión de amenazas

El administrador de la red cambia el comportamiento de Advanced EDR con respecto a las amenazas encontradas y los ficheros desconocidos en proceso de clasificación mediante las herramientas siguientes:

- Desbloquear procesos desconocidos.
- Permitir ejecutar programas clasificados como malware, PUP, virus o Exploit.
- No volver a detectar ataques de red.
- Cambiar la política de reclasificación de Advanced EDR.
- Gestionar el backup / cuarentena.

Desbloquear procesos desconocidos

Advanced EDR analiza y clasifica en la nube los procesos desconocidos de forma automática dentro de las primeras 24 horas a partir de su descubrimiento en el equipo protegido. Este proceso genera una categoría no ambigua (goodware o malware) que se comparte entre todos los clientes de Cytomic .

Advanced EDR incorpora los modos **Hardening** y **Lock** en el perfil de protección avanzada para bloquear la ejecución de los procesos desconocidos en los equipos protegidos durante el tiempo de clasificación. El proceso de clasificación puede ser:

- **Automatizado:** en la mayor parte de los casos, los procesos de machine learning estudian la muestra en tiempo real.
- **Manual:** cuando el análisis automatizado no clasifica el proceso desconocido con el 99'999% de certeza, un experto en análisis de malware estudia de forma manual la muestra. En estos casos, el análisis puede demorarse por un corto espacio de tiempo.

En los casos donde la clasificación no es inmediata, el administrador puede asumir ciertos riesgos y permitir la ejecución del fichero sin esperas. Para ello Advanced EDR implementa varias estrategias:

- **Desbloqueo reactivo:** el administrador permite la ejecución de programas desconocidos en clasificación después de que un usuario intente utilizarlos y Advanced EDR los detecte y bloquee. Consulta [Permitir y volver a impedir la ejecución de elementos](#) para más información.
- **Desbloqueo proactivo:** el administrador garantiza que los programas desconocidos no se bloquean

y evita el impacto negativo en el rendimiento de los usuarios. Para más información consulta [Configuración de software autorizado](#) en la página 525.

Permitir ejecutar malware, PUP o Exploit

El administrador permite ejecutar el software que implementa algunas funcionalidades valoradas por los usuarios, pero que Advanced EDR clasificada como una amenaza. Este es el caso, por ejemplo, de PUPs, programas generalmente en forma de barras de navegador, que ofrecen capacidades de búsqueda, al tiempo que recogen información privada del usuario o confidencial de la empresa con objetivos publicitarios. Para más información consulta [Permitir y volver a impedir la ejecución de elementos](#).

No volver a detectar ataques de red

Cuando Advanced EDR detecta un patrón de tráfico sospechoso de pertenecer a un ataque de red, el módulo Protección contra ataques de red bloquea su llegada al equipo del usuario. El administrador añade excepciones para evitar el bloqueo cuando considera que el tráfico de red no es peligroso para su infraestructura. Estas excepciones se configuran según la tecnología empleada por el ataque y la dirección IP origen del mismo.

Cambiar la política de reclasificación.

Cuando el administrador desbloquea un elemento desconocido previamente bloqueado por Advanced EDR, al cabo de un tiempo el proceso de clasificación cataloga al elemento como malware o goodware. Si se trata de goodware, no se requiere ningún tipo de consideración adicional, ya que Advanced EDR permite su ejecución. Por el contrario, si se trata de malware, se aplica la política de reclasificación, que establece el comportamiento de Advanced EDR. Para más información consulta [Política de reclasificación](#).

Gestionar el backup / cuarentena

El administrador cuenta con herramientas para recuperar los elementos considerados como amenazas que han sido eliminados de los equipos de los usuarios.

Comportamiento del software de seguridad

Ficheros conocidos

Si Advanced EDR clasifica el fichero como malware / PUP / exploit y se aplica una política de protección avanzada **Hardering** o **Lock**, los ficheros se bloquean si el administrador ni permite su ejecución.

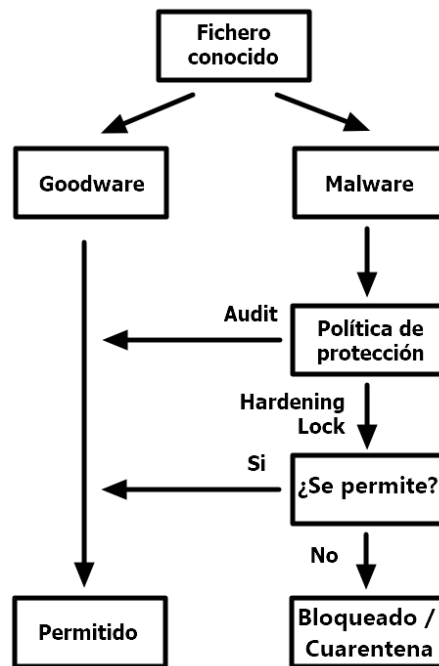


Figura 22.1: Diagrama de acciones para procesos conocidos y ya clasificados

Ficheros desconocidos

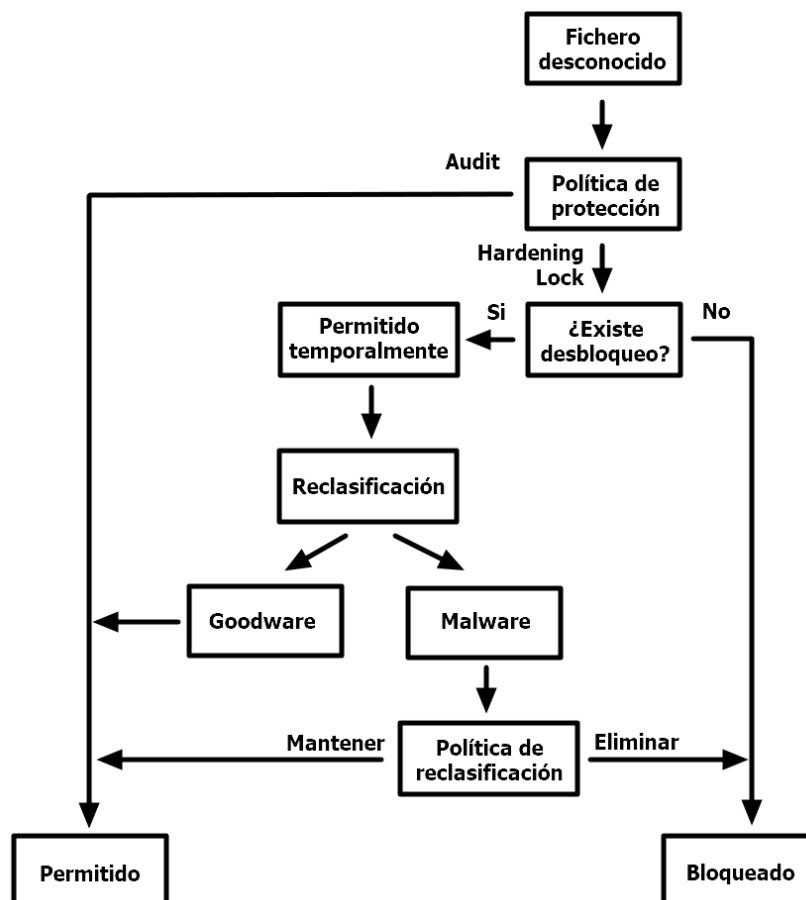


Figura 22.2: Diagrama de acciones para procesos desconocidos

Para un fichero desconocido en proceso de clasificación y una política de protección avanzada **Hardening o Lock**, el comportamiento de Advanced EDR es:

- Si el administrador no ha establecido un desbloqueo sobre el fichero desconocido:
 - El fichero se bloquea.
 - Si el resultado de la clasificación es goodware, Advanced EDR permite ejecutar el fichero.
 - Si el resultado de la clasificación es malware, Advanced EDR bloquea la ejecución del fichero.
- Si el administrador ha establecido un desbloqueo sobre el fichero desconocido:
 - El fichero se puede ejecutar mientras Advanced EDR completa el proceso de clasificación.
 - Si el resultado de la clasificación es goodware, Advanced EDR sigue permitiendo ejecutar el proceso.
 - Si el resultado de la clasificación es malware, Advanced EDR permite o impide ejecutar el proceso dependiendo de la política de reclasificación elegida por el administrador. Para más información consulta [Política de reclasificación](#).

Permitir y volver a impedir la ejecución de elementos

El administrador utiliza los paneles listados a continuación dependiendo del tipo de elemento cuya ejecución quiere permitir:

- **Programas actualmente bloqueados en clasificación:** desbloquea elementos en clasificación.
- **Actividad del Malware:** permite la ejecución de programas clasificados como malware.
- **Actividad de PUP:** permite la ejecución de programas clasificados como PUP.
- **Actividad de Exploits:** permite la ejecución de técnicas de explotación.
- **Ataques de red:** permite la llegada de tráfico clasificado como peligroso por el módulo Protección contra ataques de red.

Desbloquear elementos desconocidos pendientes de clasificación



De forma general se desaconseja desbloquear la ejecución de elementos sin clasificar, ya que pueden representar un riesgo para la integridad de los sistemas de IT de la empresa y sus datos.

Si los usuarios no pueden esperar a que Advanced EDR complete la clasificación para liberar el bloqueo de forma automática, el administrador puede desbloquearlos manualmente.

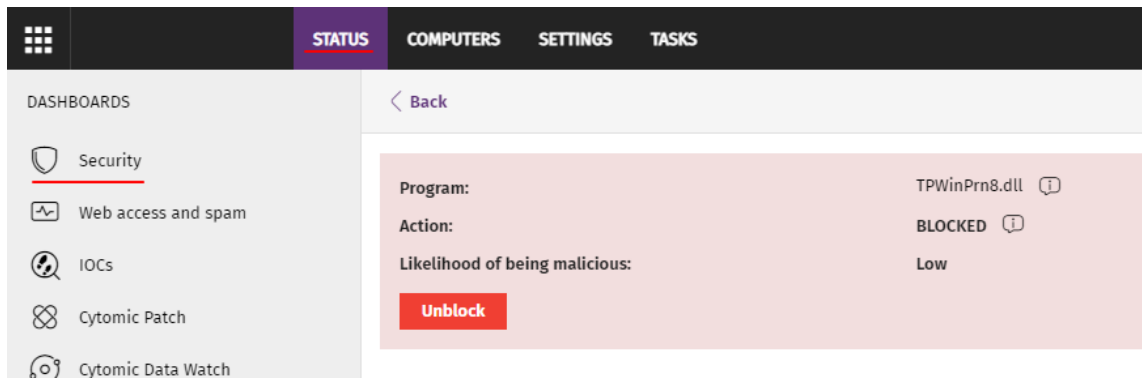


Figura 22.3: Desbloquear un elemento desconocido en clasificación

Para permitir ejecutar un elemento desconocido en clasificación:

- Selecciona el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en el panel **Programas actualmente bloqueados en clasificación** y selecciona en el listado el elemento a desbloquear.
- Haz clic en el botón **Desbloquear**. Se mostrará una ventana advirtiendo del peligro que supone desbloquear un elemento desconocido, junto a una valoración provisional de su peligrosidad.
- Haz clic en el botón **Desbloquear**. Advanced EDR ejecuta las siguientes acciones:
 - Advanced EDR permite ejecutar el elemento en todos los equipos gestionados del parque informático.
 - Advanced EDR permite ejecutar toda la cadena de librerías y binarios utilizados en el programa, excepto aquellos ya conocidas y clasificadas como amenazas.
 - El elemento se retira del listado **Programas actualmente bloqueados en clasificación**.
 - El elemento se incorpora al listado **Programas permitidos por el administrador**.
 - El elemento se incorpora al listado **Historial de programas permitidos por el administrador**.
 - Advanced EDR continuará analizando el elemento hasta completar su clasificación.

Permitir ejecutar elementos clasificados como malware, PUP o Exploit



De forma general se desaconseja desbloquear la ejecución de elementos clasificados como amenazas, ya que representan un riesgo evidente para la integridad de los sistemas de IT de la empresa y sus datos.

Si los usuarios requieren cierta funcionalidad incluida en un programa que ha sido clasificado como una amenaza, y el administrador considera que el peligro para la integridad del parque IT administrador es bajo, puede permitir su ejecución.

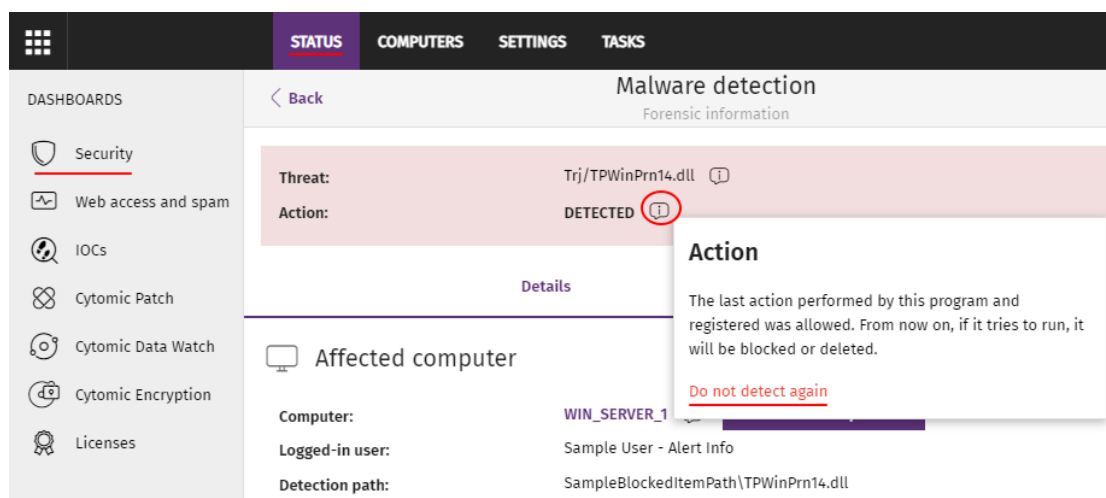


Figura 22.4: Permitir la ejecución de una amenaza

Para permitir la ejecución de un programa clasificado como malware, PUP o Exploit:

- Selecciona el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en panel **Actividad de malware / PUP / Exploit** y selecciona la amenaza cuya ejecución quieres permitir.
- Haz clic en el icono  del campo **Acción**. Se mostrará un ventana explicando la acción que ejecutará Advanced EDR.
- Haz clic en el enlace **No volver a detectar**. Advanced EDR ejecuta las siguientes acciones:
 - Advanced EDR permite ejecutar el elemento en todos los equipos gestionados por el administrador. En el caso de exploits, Advanced EDR permite ejecutar la técnica de explotación específicamente permitida, y únicamente desde el programa detectado.
 - Advanced EDR permite ejecutar automáticamente toda la cadena de librerías y binarios que utiliza el programa, excepto aquellos ya conocidas y clasificadas como amenazas.
 - El elemento se incorpora al listado **Programas permitidos por el administrador**.
 - El elemento deja de generar incidentes en los paneles **Actividad de malware / PUP / Exploits**

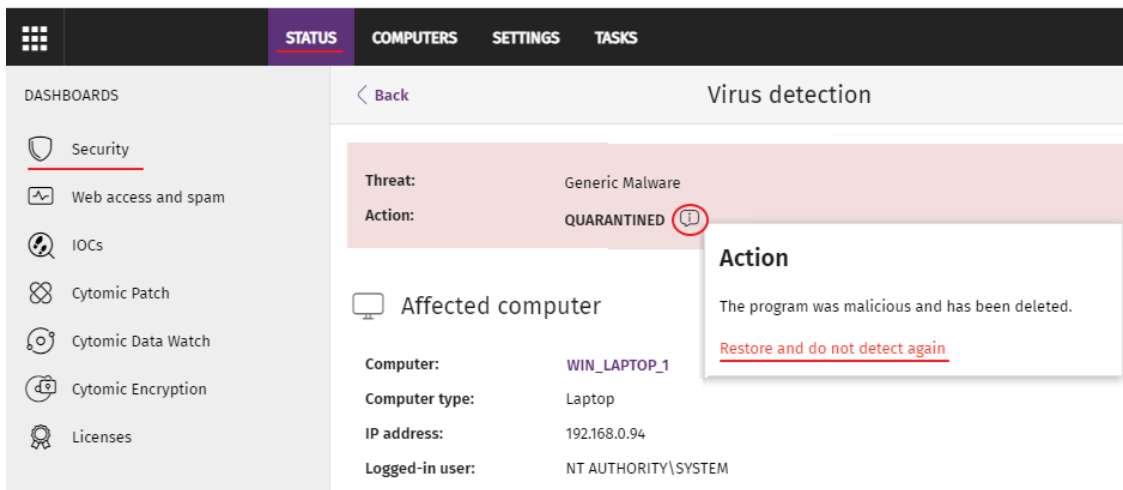


Figura 22.5: Restaurar y no volver a detectar una amenaza

No volver a detectar la llegada de tráfico de red sospechoso

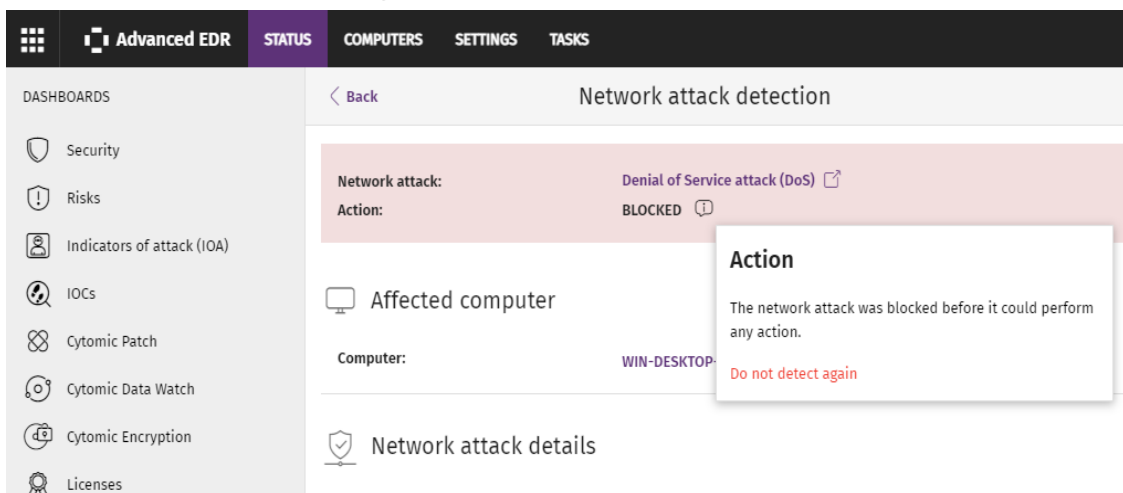


Figura 22.6: No volver a detectar un ataque de red

Si el administrador considera que el tráfico bloqueado no es peligroso, puede permitirlo añadiendo las IPs de origen y los tipos de ataque que considere no dañinos para su infraestructura.



Una vez definida una exclusión, ésta aplica a todos los equipos gestionados por Advanced EDR.

Para evitar el bloqueo de tráfico marcado como peligroso por Protección contra ataques de red:

- Selecciona en el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en el panel **Actividad de ataques de red** y selecciona el tipo de ataque de red que quieres permitir .

- Haz clic en el icono del campo **Acción**. Se mostrará una ventana explicando la acción que ejecutará Advanced EDR.
- Haz clic en el enlace **No volver a detectar**. Se mostrará la ventana **No volver a detectar**, indicando la IP origen del ataque y su tipo en el campo **Ataque de red**.
- Escribe en **Permitir este tipo de ataque de red sólo desde las siguientes IPs** las direcciones IP de origen desde las cuales se permitirá la llegada de tráfico con el tipo de ataque indicado en **Ataque de red**. Escribe las IPs individuales separadas por comas y rangos de IPs separados por guión. Para que cualquier IP pueda enviar tráfico de red del tipo del ataque elegido deja la caja de texto vacía.
- Haz clic en el botón **No volver a detectar**. Advanced EDR ejecuta las siguientes acciones:
 - Permite en todo el parque administrado el tráfico del tipo de ataque indicado en el campo **Ataque de red** si tiene como origen una IP de la lista indicada.
 - El tráfico de red no genera detecciones.
 - El tipo de ataque se incorpora al listado **Listado Elementos permitidos por el administrador**.

Dejar de permitir la ejecución de elementos previamente permitidos

Para volver a bloquear un elemento previamente permitido por el administrador:

- Selecciona en el menú superior **Estado**, panel lateral **Seguridad**.
- En el listado **Elementos detectados permitidos por el administrador** haz clic en el icono  situado a la derecha del elemento cuya ejecución quieres dejar de permitir.

Al hacer clic en el icono  asociado al elemento, Advanced EDR ejecuta las acciones siguientes:

- El elemento se retira del listado **Elementos detectados permitidos por el administrador**
- Se añade una entrada al listado **Historial de elementos permitidos por el administrador** indicando como **Acción** el valor **Exclusión eliminada por el usuario**.
- El elemento vuelve a aparecer en su listado correspondiente:
 - **Actividad de malware**
 - **Actividad de PUP**
 - **Actividad de exploits**
 - **Amenazas detectadas por el antivirus.**
 - **Actividad de ataques de red**
- El elemento vuelve a generar incidentes.
- Si es un elemento desconocido en proceso de clasificación, vuelve a aparecer en el listado **Programas actualmente bloqueados en clasificación**.

Información de elementos bloqueados en clasificación

El administrador de la red dispone de varios paneles y listados para obtener información sobre los programas bloqueados en clasificación:

- El panel **Programas actualmente bloqueados en clasificación**.
- El listado **Programas actualmente bloqueados en clasificación**.
- El listado **Historial de programas bloqueados**.

Además, el administrador puede realizar acciones de mantenimiento sobre el listado **Programas actualmente bloqueados en clasificación**, eliminando aquellos programas que Advanced EDR no puede analizar por diversas razones. Consulta [Eliminar procesos desconocidos de los listados](#).

Panel Programas actualmente bloqueados en clasificación

CURRENTLY BLOCKED PROGRAMS BEING CLASSIFIED

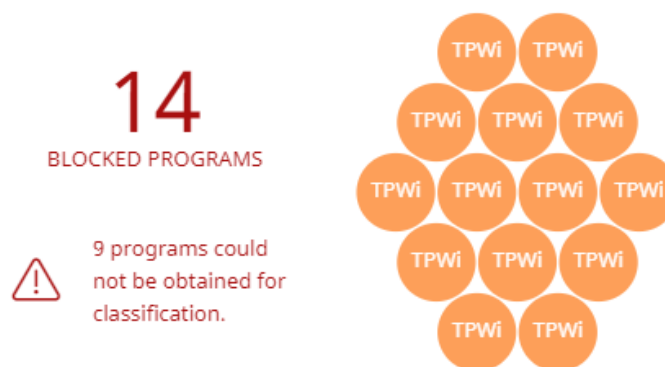


Figura 22.7: Panel de Programas actualmente bloqueados en clasificación,

Advanced EDR muestra incidencias en el panel **Programas actualmente bloqueados en clasificación** cuando registra la ejecución de un programa que todavía no ha sido clasificado. Este panel muestra todos los elementos bloqueados que aún no han sido clasificados desde la puesta en marcha del servicio de protección en el cliente hasta el momento actual.

Cuando en alguno de los equipos sobre los que el administrador tiene visibilidad se detecta la llegada de un fichero infectado, se muestran la IP origen de la infección y el número de veces entre paréntesis que esta IP ha sido origen de alguna detección. Haz clic en el enlace de la IP para acceder al listado **Actividad del Malware**. Consulta [Actividad de malware / PUP](#) en la página 628.

Para evitar la aparición de muchas repeticiones de un mismo programa, Advanced EDR muestra como máximo 1 incidencia cada 24 horas por cada hash encontrado en cada equipo.



*Este widget no se ve afectado por la selección del intervalo de tiempo establecida por el administrador en el menú superior **Estado**, panel lateral **Seguridad**.*

Cada programa diferente bloqueado en clasificación se representa mediante un círculo con las características siguientes:

- Cada círculo se corresponde con un elemento bloqueado en clasificación con un hash diferente.
- El color representa el grado de peligrosidad asignado temporalmente al elemento.
- El tamaño representa el número de equipos diferentes donde se intentó ejecutar el programa desconocido bloqueado. El tamaño **no** representa la cantidad de intentos de ejecución en los equipos de la red.

Además, se indican los programas que no han podido enviarse a la nube de Cytomic para su análisis.

Descripción de las series

Las aplicaciones bloqueadas se muestran con el código de colores indicado a continuación:

Serie	Descripción
Naranja	Aplicaciones con probabilidad media de ser malware.
Naranja oscuro	Aplicaciones con probabilidad alta de ser malware.
Rojo	Aplicaciones con probabilidad muy alta de ser malware.
Programas bloqueados	Número total de aplicaciones diferentes bloqueadas.
Programas que no se han podido obtener para su clasificación	Número total de programas bloqueados que han experimentado algún tipo de error al intentar obtener su clasificación.
Amenazas copiadas desde equipos de la red	Dirección IP origen de la amenaza y número de veces que esta dirección ha sido origen de detección.

Tabla 22.1: Descripción de la serie Programas actualmente bloqueados en clasificación

Al pasar el ratón por encima de cada círculo, éste se amplía, mostrando su nombre completo y iconos que representan acciones clave:

- **Carpeta:** el programa ha leído datos del disco duro del usuario.
- **Bola del mundo:** el programa estableció una conexión con otro equipo.



Figura 22.8: Representación gráfica de un programa en clasificación

Filtros preestablecidos desde el panel

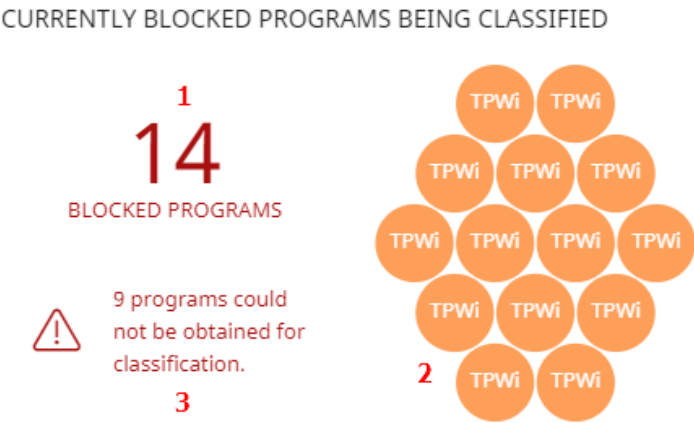


Figura 22.9: Zonas activas del panel Programas actualmente bloqueados en clasificación

Haz clic en las zonas indicadas en **Zonas activas del panel Programas actualmente bloqueados en clasificación** para abrir el listado **Programas actualmente bloqueados en clasificación** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.
(2)	Buscar = Hash.
(3)	Estado = No se ha podido obtener

Tabla 22.2: Definición de los filtros del listado Programas actualmente bloqueados en clasificación

Listado de Programas actualmente bloqueados en clasificación

Muestra una tabla con los todos ficheros bloqueados por no haberse completado su clasificación.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario.	Cadena de caracteres
Ha accedido a datos 	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Booleano
Se ha comunicado con equipos externos 	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano
Modo de protección	Modo en el que se encontraba la protección avanzada en el momento del descubrimiento del fichero desconocido.	• Audit • Hardening • Lock
Probabilidad de que sea malicioso	Posibilidad de que finalmente el fichero desconocido sea una amenaza.	• Media • Alta • Muy Alta
Estado	Estado del proceso de clasificación: • Obteniendo el programa: el programa se está enviando a la nube de Cytomic para su análisis. • Clasificando: el programa ha sido enviado con éxito a la nube de Cytomic y se está analizando. • No se ha podido obtener: se ha producido un error y el programa no llegó a la nube de Cytomic.	Numeración
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha

Tabla 22.3: Campos del listado Programas actualmente bloqueados

Campos mostrados en fichero exportado



En el menú de contexto de **Programas actualmente bloqueados en clasificación** se muestra un desplegable con dos entradas: **Exportar** y **Exportar listado y detalles**. En este apartado se muestra el contenido de **Exportar**. Para obtener información sobre **Exportar listado y detalles**, consulta **Ficheros exportados Excel** en la página 764.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Amenaza	Nombre del fichero desconocido.	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario.	Cadena de caracteres
Modo de protección	Modo en el que se encontraba la protección en el momento del descubrimiento del fichero desconocido.	• Audit • Hardening • Lock
Acceso a datos	El fichero desconocido ha accedido a ficheros que residen en el equipo del usuario.	Booleano
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano
Probabilidad de que sea malicioso	Posibilidad de que el fichero desconocido sea una amenaza cuando se complete su clasificación.	• Media • Alta • Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha
Tiempo de exposición	Tiempo que la amenaza ha permanecido en el parque del cliente sin clasificar.	Fecha

Campo	Comentario	Valores
Usuario	Cuenta de usuario bajo la cual el programa se ha ejecutado.	Cadena de caracteres
MD5	Código MD5 del archivo.	Cadena de caracteres
SHA-256	Código SHA-256 del archivo.	Cadena de caracteres
Equipo origen de la amenaza	Nombre del equipo si el programa bloqueado viene de un equipo de la red del cliente.	Cadena de caracteres
IP origen de la amenaza	Dirección IP del equipo si el programa bloqueado viene de un equipo de la red del cliente.	Cadena de caracteres
Usuario origen de la amenaza	Usuario registrado en el equipo origen del programa bloqueado.	Cadena de caracteres
Estado	Estado del proceso de clasificación: • Obteniendo el programa: el programa se está enviando a la nube de Cytomic para su análisis. • Clasificando: el programa ha sido enviado con éxito a la nube de Cytomic y se está analizando. • No se ha podido obtener: se ha producido un error y el programa no llegó a la nube de Cytomic.	Enumeración

Tabla 22.4: Campos del fichero exportado Programas actualmente bloqueados

Herramienta de filtrado

Campo	Comentario	Valores
Fechas	Establece un intervalo de fechas desde el momento actual hacia el pasado.	• Últimas 24 horas • Últimos 7 días • Último mes
Buscar	• Equipo: dispositivo donde reside el elemento desconocido.	Enumeración

Campo	Comentario	Valores
	• Amenaza: nombre del archivo. • Hash: Cadena resumen de identificación del archivo. • Origen de la amenaza: permite buscar por el usuario, la IP o el nombre del equipo origen del elemento bloqueado.	
Modos de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	• Hardening • Lock
Acceso a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Booleano
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano
Estado	Estado del proceso de clasificación: • Todos • Obteniendo el programa: el programa se está enviando a la nube de Cytomic para su análisis. • Clasificando: el programa ha sido enviado con éxito a la nube de Cytomic y se está analizando. • No se ha podido obtener: se ha producido un error y el programa no llegó a la nube de Cytomic.	Enumeración

Tabla 22.5: Campos de filtrado para el listado Programas actualmente bloqueados

Ventana de detalle

Muestra información detallada del programa bloqueado. Consulta [Bloqueo de programas desconocidos en clasificación e Historial de programas bloqueados](#) en la página 750.

Listado Historial de programas bloqueados

Muestra un histórico de todos los eventos que se han producido a lo largo del tiempo relativos a los procesos que han sido bloqueados por ser desconocidos.

Este listado no tiene un panel asociado, y es accesible únicamente mediante el enlace **Ver historial de bloqueos** del listado **Programas actualmente bloqueados en clasificación**, situado en la esquina superior derecha.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario.	Cadena de caracteres
Acción	Acción ejecutada por Advanced EDR.	• Bloqueado • Reclasificado a GW • Reclasificado a MW • Reclasificado a PUP
Tiempo de reclasificación	Tiempo que Advanced EDR tardó en clasificar el elemento. Consulta Cálculo del tiempo de reclasificación de ficheros desconocidos	Fecha
Ha accedido a datos 	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Booleano
Se ha comunicado con equipos externos 	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano
Modo de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	• Audit • Hardening • Lock
Excluido	El fichero desconocido ha sido desbloqueado / excluido por el administrador para permitir su ejecución.	Booleano
Probabilidad de que sea malicioso	Posibilidad de que el fichero desconocido sea una amenaza cuando se complete su clasificación.	• Media • Alta • Muy Alta

Campo	Comentario	Valores
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha

Tabla 22.6: Campos del listado Historial de programas bloqueados

Campos mostrados en fichero exportado



En el menú de contexto de **Historial de programas bloqueados** se muestra un desplegable con dos entradas diferentes: **Exportar** y **Exportar listado y detalles**. En este apartado se muestra el contenido de **Exportar**. Para obtener información sobre **Exportar listado y detalles** consulta **Ficheros exportados Excel** en la página **764**

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Amenaza	Nombre del fichero desconocido.	Cadena de caracteres
Ruta	Ruta en el equipo del usuario del fichero desconocido.	Cadena de caracteres
Modo de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	• Audit • Hardening • Lock
Acción	Acción ejecutada por Advanced EDR.	• Bloqueado • Reclasificado a GW • Reclasificado a MW • Reclasificado a PUP
Acceso a datos	El fichero desconocido ha accedido a datos que	Booleano

Campo	Comentario	Valores
	residen en el equipo del usuario.	
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano
Excluido	El fichero desconocido ha sido desbloqueado por el administrador para permitir su ejecución.	Booleano
Probabilidad de que sea malicioso	Posibilidad de que el fichero desconocido sea una amenaza cuando se complete su clasificación.	• Media • Alta • Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha
Fecha de inicio de la reclasificación	Fecha en la que se recibió el elemento en la nube de Cytomic.	Fecha
Reclasificación completada	Fecha en la que se completó la clasificación del elemento.	Fecha
Tiempo de reclasificación	Tiempo que Advanced EDR tardó en clasificar el elemento. Consulta Cálculo del tiempo de reclasificación de ficheros desconocidos	Fecha
Técnica de clasificación	• Clasificado por técnicos del laboratorio de WatchGuard: el elemento fue clasificado manualmente por los técnicos de Cytomic. • Clasificado automáticamente por la inteligencia colectiva de WatchGuard: el elemento fue clasificado por los procesos automáticos de machine learning de Cytomic.	Enumeración
Tiempo de exposición	Tiempo que el fichero desconocido ha permanecido en el parque del cliente sin clasificar.	Fecha
Usuario	Cuenta de usuario bajo la cual el programa se ha ejecutado.	Cadena de caracteres

Campo	Comentario	Valores
MD5	Código MD5 del archivo.	Cadena de caracteres
SHA-256	Código SHA-256 del archivo.	Cadena de caracteres
Equipo origen de la amenaza	Equipo origen del programa bloqueado.	Cadena de caracteres
IP origen de la amenaza	IP origen del programa bloqueado.	Cadena de caracteres
Usuario origen de la amenaza	Usuario origen del programa bloqueado.	Cadena de caracteres

Tabla 22.7: Campos del fichero exportado Historial de programas bloqueados

Herramienta de filtrado

Campo	Comentario	Valores
Buscar	• Equipo: dispositivo donde reside el fichero desconocido. • Amenaza: nombre de la amenaza. • Hash: cadena resumen de identificación del archivo. • Origen de la amenaza: permite buscar por el usuario, la IP o el nombre del equipo origen de la amenaza.	Enumeración
Fechas	Establece un intervalo de fechas desde el momento actual hacia atrás.	• Últimas 24 horas • Últimos 7 días • Último mes
Acción	Acción desencadenada por Advanced EDR.	• Bloqueado • Reclasificado a Goodware • Reclasificado a

Campo	Comentario	Valores
		Malware • Reclasificado a PUP • PUP bloqueado debido a un fallo de conectividad • Malware bloqueado debido a un fallo de conectividad • Goodware bloqueado debido a un fallo de conectividad • Eliminado del listado
Excluido	El fichero desconocido ha sido desbloqueado por el administrador para permitir su ejecución.	Booleano
Modos de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	• Hardening • Lock
Acceso a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Booleano
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano

Tabla 22.8: Campos del fichero exportado Historial de programas bloqueados

Ventana de detalle

Muestra información detallada del programa bloqueado. Consulta [Bloqueo por política avanzada de seguridad](#) en la página **748** para más información.

Eliminar procesos desconocidos de los listados

Los procesos desconocidos se muestran en el widget [Panel Programas actualmente bloqueados en clasificación](#) hasta que Advanced EDR completa su análisis. En ocasiones, no es posible completar este proceso debido a fallos en el envío del fichero por su tamaño, o por no estar ya disponible en el equipo del usuario. En estos casos, los ficheros desconocidos se acumulan de forma indefinida en el widget Programas actualmente bloqueados en clasificación.

Para eliminar estos ficheros del widget y de los listados:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad**, y haz clic en el widget **Programas actualmente bloqueados en clasificación**. Se abrirá el listado **Programas actualmente bloqueados en clasificación**.

o

- Haz clic en el menú superior **Estado**, y en el enlace **Añadir** del panel lateral **Mis listados**. Se mostrará un desplegable con los listados disponibles.
- Haz clic en el listado **Programas actualmente bloqueados en clasificación**.
- Haz clic en las casillas de selección de los ficheros a eliminar y haz clic en el icono eliminar del menú de herramientas. Se mostrará una ventana de advertencia.
- Haz clic en el botón eliminar de la ventana de advertencia. Los elementos así eliminados pasarán al listado **Historial de bloqueos** con el campo **Acción** a **Eliminado del listado**. Estos ficheros no se podrán desbloquear.



*La finalidad de eliminar un programa bloqueado en clasificación mediante este procedimiento es la de simplificar el contenido del listado, retirando aquellos elementos que no se han podido analizar. Internamente, Advanced EDR sigue considerando estos elementos como desconocidos, de modo que, en cada intento de ejecución volverán a aparecer en el panel **Programas actualmente bloqueados en clasificación** y en el listado **Programas actualmente bloqueados en clasificación**.*

Cálculo del tiempo de reclasificación de ficheros desconocidos

Cuando el software de seguridad bloquea la ejecución de un fichero desconocido, Advanced EDR calcula el tiempo que tarda en emitir una categoría y desbloquearlo. Muchos ficheros desconocidos se analizan de forma casi inmediata, y la gran mayoría de los ficheros más complejos requieren un tiempo de análisis inferior a las 4 horas.

La consola de Advanced EDR muestra el tiempo de clasificación de los elementos desconocidos en los campos siguientes:

- **Reclasificación completada:** fecha y hora del momento en el que la reclasificación finalizó.
- **Tiempo de reclasificación:** tiempo que Advanced EDR tarda en clasificar el fichero. Consulta [Inicio del tiempo de clasificación](#).
- **Fecha de inicio de la reclasificación:** fecha y hora en la que el la nube de Cytomic recibe el fichero para su análisis.

Inicio del tiempo de clasificación

Para marcar el inicio del proceso de clasificación, Advanced EDR utiliza la fecha más próxima entre las dos disponibles:

- La fecha en la que se recibió el elemento en los servidores de Cytomic
- La fecha en la que el elemento se bloqueó en el equipo del usuario.

En la mayor parte de los casos, Advanced EDR comienza a contar el tiempo de clasificación desde que se recibe el fichero bloqueado en la nube de Cytomic, indicado en el campo **Fecha de inicio de la reclasificación**. Sin embargo existen varios casos en los que esta regla no se aplica:

- Si el equipo del usuario no puede enviar el fichero bloqueado (por un fallo de red transitorio, porque el fichero ya no existe en el sistema de ficheros o porque no se cumplen los requisitos de tamaño de fichero) pero el fichero se consigue clasificar por otros medios, **Tiempo de reclasificación** comprenderá desde el momento en que Advanced EDR bloqueó el fichero en el equipo del usuario hasta el momento en que obtiene una clasificación, y el campo **Fecha de inicio de la reclasificación** estará vacío.
- Si el fichero bloqueado ya fue enviado previamente por otro usuario a la nube de Cytomic pero Advanced EDR lo bloquea en el equipo del usuario por no tener todavía disponible la clasificación calculada cuando el usuario intenta ejecutarlo, **Tiempo de reclasificación** comprenderá desde el momento en que Advanced EDR bloquea el fichero en el equipo del usuario hasta que completa la clasificación.

Listado de amenazas y programas desconocidos permitidos

El administrador dispone de varios paneles y listados para obtener información sobre los programas que inicialmente fueron bloqueados por Advanced EDR y cuya ejecución ha sido permitida:

- El panel **Elementos detectados permitidos por el administrador**.
- El listado **Elementos detectados permitidos por el administrador**.
- El listado **Historial de elementos permitidos por el administrador**.

Elementos detectados permitidos por el administrador

Muestra los elementos que Advanced EDR bloqueó inicialmente, pero cuya ejecución fue permitida por el administrador con posterioridad. Estos elementos fueron considerados como una amenaza o son ficheros desconocidos en proceso de clasificación.

DETECTED ITEMS ALLOWED BY THE ADMINISTRATOR

14

6 malware
 3 PUPs
 1 being classified
 2 exploits and drivers
 2 network attacks

Figura 22.10: Panel Elementos detectados permitidos por el administrador

Descripción de las series

El panel representa el número total de elementos que el administrador excluyó del bloqueo, desagregados por su tipo:

- Malware
- PUP
- En clasificación
- Exploits y drivers
- Ataque de red

Filtros preestablecidos desde el panel

DETECTED ITEMS ALLOWED BY THE ADMINISTRATOR

1

14

2 6 malware
 3 3 PUPs
 4 1 being classified
 5 2 exploits and drivers
 6 2 network attacks

Figura 22.11: Zonas activas del panel Elementos detectados permitidos por el administrador

Haz clic en las zonas indicadas en **Zonas activas del panel Elementos detectados permitidos por el administrador** para abrir el listado **Listado Elementos permitidos por el administrador** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.
(2)	Clasificación = malware.
(3)	Clasificación = PUP.

Zona activa	Filtro
(4)	Clasificación = En clasificación (bloqueados y sospechosos).
(5)	Clasificación = Exploits y drivers
(6)	Clasificación = Ataque de red.

Tabla 22.9: Definición de los filtros del listado Programas permitidos por el administrador

Listado Elementos permitidos por el administrador

Muestra todos los elementos considerados amenazas que el administrador ha permitido.

Campo	Descripción	Valores
Clasificación	Tipo de la amenaza a la que se permite la ejecución.	- Malware - PUP - Goodware - Exploits y drivers - En clasificación - Ataque de red
Amenaza	Nombre del elemento cuya ejecución se permite. - Si es un elemento desconocido el campo está vacío. - Si es un exploit se indica la técnica de explotación utilizada. - Si es un ataque de red se indica su tipo.	Cadena de caracteres
Detalles	Nombre del fichero que contiene la amenaza. - Si es un elemento desconocido se indica el nombre del fichero en clasificación. - Si es un exploit se indica el nombre del fichero que fue explotado. - Si es un ataque de red se indican las direcciones IP desde las cuales se permite el tipo de ataque de red.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de

Campo	Descripción	Valores
	Vacío si es un exploit o un ataque de red.	caracteres
Nombre de usuario	Cuenta de usuario de la consola que añadió la exclusión del elemento.	Cadena de caracteres
Permitido el	Fecha en la que se produjo el evento.	Fecha
Borrar	Elimina la exclusión del elemento.	

Tabla 22.10: Campos del listado Elementos detectados permitidos por el administrador

Campos incluidos en fichero exportado

Campo	Descripción	Valores
Detalles	Nombre del fichero que contiene la amenaza. • Si es un elemento desconocido se indica el nombre del fichero en clasificación. • Si es un exploit se indica el nombre del fichero que fue explotado. • Si es un ataque de red se indican las direcciones IP desde las cuales se permite el tipo de ataque de red.	Cadena de caracteres
Tipo actual	Clasificación en el momento actual de la amenaza cuya ejecución se permitió.	• Malware • PUP • Goodware • Exploits y drivers • En clasificación • Ataque de red
Tipo original	Clasificación de la amenaza cuya ejecución se permitió en el momento en que se detectó por primera vez.	• Malware • PUP • Goodware • Exploit • En clasificación

Campo	Descripción	Valores
		Ataque de red
Amenaza	Nombre del elemento cuya ejecución se permite. - Si es un elemento desconocido el campo está vacío. - Si es un exploit se indica la técnica de explotación utilizada. - Si es un ataque de red se indica su tipo.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo. Vacío si es un exploit o un ataque de red.	Cadena de caracteres
Nombre de usuario	Cuenta de usuario de la consola que inicio el cambio en el fichero permitido.	Cadena de caracteres
Permitido el	Fecha en la que se registró el evento.	Fecha

Tabla 22.11: Campos del fichero exportado Programas permitidos por el administrador

Herramienta de filtrado

Campo	Descripción	Valores
Buscar	Detalles: detalles de la amenaza. Amenaza: nombre de la amenaza detectada. Nombre de usuario: cuenta de usuario de la consola que añadió la exclusión del elemento. Hash: cadena resumen de identificación del archivo.	Enumeración
Clasificación	Tipo del fichero en el momento en el que se clasificó por última vez.	- Todos - Malware - PUP - Goodware - Exploit - Ataque de red - En clasificación

Campo	Descripción	Valores
		(Bloqueados y sospechoso)
Clasificación original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo.	• Todos • Malware • PUP • En clasificación (Bloqueado) • En clasificación (Sospechoso) • Exploit • Ataque de red

Tabla 22.12: Campos de filtrado para el listado Programas permitidos por el administrador

Listado Historial de elementos permitidos por el administrador

Muestra un histórico de todos eventos que se han producido a lo largo del tiempo relativos a las amenazas y ficheros desconocidos en clasificación cuya ejecución permitió el administrador. El listado muestra el ciclo de estados completo de un elemento, desde que entra en el listado de **Elementos detectados permitidos por el administrador** hasta que lo abandona, pasando por todos los cambios de estado intermedios que Advanced EDR o el administrador provoque.

Este listado no tiene un panel asociado, y es accesible únicamente mediante el botón **Historial**, situado en la esquina superior derecha del listado **Elementos detectados permitidos por el administrador**.

Campo	Descripción	Valores
Clasificación	Tipo de la amenaza cuya ejecución se permitió.	• Malware • PUP • Goodware • Exploit • En clasificación • Ataque de red
Amenaza	Nombre del elemento cuya ejecución se permite. • Si es un elemento desconocido el campo está vacío.	Cadena de caracteres

Campo	Descripción	Valores
	- Si es un exploit se indica la técnica de explotación utilizada. - Si es un ataque de red se indica su tipo.	
Detalles	Nombre del fichero que contiene la amenaza. - Si es un elemento desconocido se indica el nombre del fichero en clasificación. - Si es un exploit se indica el nombre del fichero que fue explotado. - Si es un ataque de red se indican las direcciones IP desde las cuales se permite el tipo de ataque de red.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo. Vacío si es un exploit o un ataque de red.	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido. Exclusión eliminada por el usuario: el administrador permitió bloquear de nuevo el elemento. Exclusión eliminada por reclasificación: Advanced EDR aplica la acción asociada a la categoría obtenida de la reclasificación. Exclusión añadida por el usuario: el administrador permitió ejecutar el elemento. Exclusión mantenida por reclasificación: Advanced EDR no bloqueó el elemento al reclasificarlo.	Enumeración
Nombre de usuario	Cuenta de usuario de la consola que inicio el cambio en el fichero permitido.	Cadena de caracteres
Permitido el	Fecha en la que se registró el evento.	Fecha

Tabla 22.13: Campos del listado Historial de Programas permitidos por el administrador

Campos incluidos en fichero exportado

Campo	Descripción	Valores
Detalles	Nombre del fichero que contiene la amenaza. • Si es un elemento desconocido se indica el nombre del fichero en clasificación. • Si es un exploit se indica el nombre del fichero que fue explotado. • Si es un ataque de red se indican las direcciones IP desde las cuales se permite el tipo de ataque de red.	Cadena de caracteres
Tipo actual	Clasificación en el momento actual de la amenaza cuya ejecución se permitió.	• Malware • PUP • Exploit • Bloqueado • Sospechoso • Ataque de red
Tipo original	Clasificación de la amenaza cuya ejecución se permitió en el momento en que se detectó por primera vez.	• Malware • PUP • Exploit • Bloqueado • Sospechoso • Ataque de red
Amenaza	Nombre del malware o PUP cuya ejecución se permite. Si es un elemento desconocido, se indica el nombre del fichero en su lugar. Si se trata de un exploit o de un ataque de red, se indica la técnica de explotación utilizada.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo. Si se trata de un exploit o de un ataque de red este campo estará vacío.	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido. • Exclusión eliminada por el usuario: el administrador	Enumeración

Campo	Descripción	Valores
	permitió bloquear de nuevo el elemento. • Exclusión eliminada por reclasificación: Advanced EDR aplica la acción asociada a la categoría obtenida de la reclasificación. • Exclusión añadida por el usuario: el administrador permitió ejecutar el elemento. • Exclusión mantenida por reclasificación: Advanced EDR no bloqueó el elemento al reclasificarlo.	
Nombre de usuario	Cuenta de usuario de la consola que añadió la exclusión del elemento.	Cadena de caracteres
Permitido el	Fecha en la que se produjo el evento.	Fecha

Tabla 22.14: Campos del fichero exportado Historial de elementos permitidos por el administrador

Herramienta de filtrado

Campo	Descripción	Valores
Buscar	• Detalles: detalles de la amenaza. • Usuario: cuenta de usuario de la consola que añadió la exclusión del elemento. • Hash: cadena resumen de identificación del archivo.	Enumeración
Clasificación	Tipo del fichero en el momento en el que se clasificó por última vez.	• Todos • Malware • PUP • Goodware • Exploit • Ataque de red • En clasificación (Bloqueados y sospechoso)
Clasificación original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo.	• Todos

Campo	Descripción	Valores
		• Malware • PUP • En clasificación (Bloqueado) • En clasificación (Sospechoso) • Exploit • Ataque de red
Acción	Acción aplicada sobre el elemento permitido. • Exclusión eliminada por el usuario: el administrador permitió bloquear de nuevo el elemento. • Exclusión eliminada por reclasificación: Advanced EDR aplica la acción asociada a la categoría obtenida de la reclasificación. • Exclusión añadida por el usuario: el administrador permitió ejecutar el elemento. • Exclusión mantenida por reclasificación: Advanced EDR no bloqueó el elemento al reclasificarlo.	Enumeración

Tabla 22.15: Campos de filtrado para el listado Historial de elementos permitidos por el administrador

Política de reclasificación

La política de reclasificación establece el comportamiento de Advanced EDR cuando cambia la clasificación de un elemento desbloqueado por el administrador:

- Advanced EDR clasifica el elemento como goodware: permite su ejecución.
- Advanced EDR clasifica el elemento como malware: aplica la política de reclasificación, que permite al administrador definir el comportamiento de Advanced EDR a seguir.

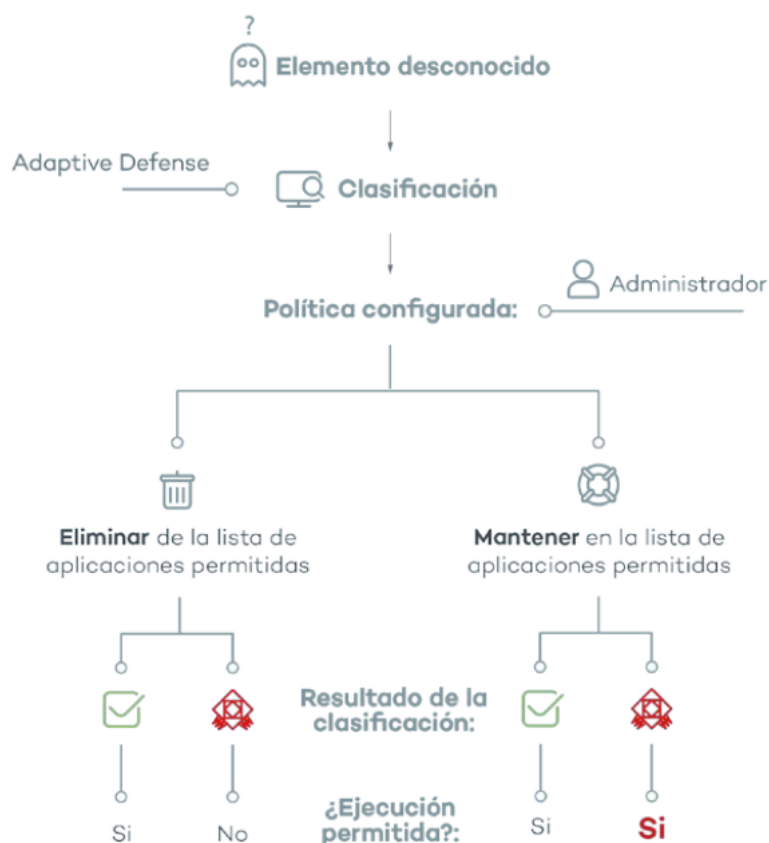


Figura 22.12: Comportamiento de Advanced EDR ante la política de reclasificación elegida y el resultado de la clasificación

Cambiar la política de reclasificación

La política de reclasificación es general para todos los equipos de la red e independiente de la configuración de seguridad.

Para cambiar la acción que ejecuta Advanced EDR cuando se produce una reclasificación de archivos:

- Haz clic en el menú superior **Estado** y en el panel lateral **Seguridad**.
- Haz clic en el tipo de elemento en el panel **Programas permitidos por el administrador**:
 - Malware
 - PUPs
 - En clasificación
 - Exploits
- Haz clic en el enlace **Cambiar comportamiento**. Se mostrará una ventana emergente con la política de reclasificación a aplicar.
 - **Eliminar de la lista de programas permitidos por el administrador**: si Advanced EDR clasifica el fichero desconocido como goodware, se sigue ejecutando de forma normal. Si el fichero es malware, la exclusión se elimina de forma automática y el fichero queda

bloqueado, a no ser que el administrador genere una nueva exclusión manual para ese fichero.

- **Mantener en la lista de Programas permitidos por el administrador:** se muestra en el listado **Programas permitidos por el administrador** una franja de color rojo que indica que esta elección puede dar lugar a situaciones potencialmente peligrosas. Tanto si Advanced EDR clasifica el fichero desconocido como goodwill o malware, la exclusión se mantiene y el fichero se sigue ejecutando.



Cytopic desaconseja el uso de esta configuración por el riesgo de permitir ejecutar malware en los equipos protegidos.

Trazabilidad de las reclasificaciones

El administrador puede conocer si un elemento desconocido ha sido reclasificado como malware cuando elige la política **Mantener en la lista de Programas permitidos por el administrador**.

Trazabilidad mediante el Historial de Programas bloqueados

Para visualizar el histórico de reclasificaciones y eventos de un fichero desbloqueado:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en el panel **Programas actualmente bloqueados en clasificación**
- Haz clic en el enlace **Ver historial de bloqueos**. Se mostrará el listado **Historial de programas bloqueados**.
- Utiliza el buscador para indicar el nombre de la amenaza. En el campo **Acción** se detalla el tipo de evento producido. Consulta [Listado Historial de programas bloqueados](#) para más información.

Trazabilidad mediante alertas



Para obtener el detalle de las alertas recibidas consulta [Alertas](#) en la página [775](#) para más información.

El administrador puede recibir notificaciones por correo en el momento en que se producen los bloqueos por ficheros desconocidos. También se envía información de las reclasificaciones de los ficheros que previamente ha desbloqueado.

Para habilitar las notificaciones por correo en bloqueos de ficheros desconocidos:

- Haz clic en el menú superior **Configuración** y en el panel lateral **Mis alertas**.
- Habilita los siguientes tipos de alertas:

- Programas bloqueados en proceso de clasificación.
- Clasificaciones de archivos que han sido permitidos por el administrador.

Estrategias para supervisar la clasificación de ficheros

Muchos departamentos de IT controlan la instalación de programas en los equipos que gestionan. En estos casos, el administrador puede querer minimizar los bloqueos del software desconocido, pero sin relajar la seguridad de la red.

Para preparar de antemano la ejecución del software nuevo antes de su instalación y uso masivo:

- Configura el PC de pruebas.
- Instala el software.
- Reclasifica los programas bloqueados.
- Envía el programa directamente a la nube de Cytomic.

Configurar el equipo de pruebas

El objetivo es determinar si el software a utilizar en la red ya es conocido como malware, o es desconocido para Cytomic. Para ello, utiliza el equipo de un usuario de la red o un equipo dedicado en exclusiva a este objetivo. Este equipo debe tener asignada inicialmente una configuración de seguridad avanzada **Hardening**

Instalar el software

Instala el software y ejecútalo de forma normal. Si Advanced EDR encuentra algún módulo o programa desconocido, lo bloqueará y mostrará una ventana emergente en el equipo. Además, se añadirá un nuevo elemento en el panel **Programas actualmente bloqueados en clasificación**. Internamente, Advanced EDR registrará los eventos generados por el uso del programa y enviará los binarios a la nube para poder estudiarlos.

Si no se han presentado bloqueos en el modo Hardening, cambia la configuración a modo Lock y vuelve a ejecutar el programa recién instalado. Si aparecen nuevos bloqueos, el panel **Programas actualmente bloqueados en clasificación** los mostrará.

Reclasificar los programas bloqueados

En el momento en que Advanced EDR emite una clasificación de los programas bloqueados, envía una notificación por correo al administrador avisando del desbloqueo si la clasificación es **goodware**, o su bloqueo por considerarse una amenaza. Cuando todos los procesos han sido reclasificados como **goodware**, el software instalado será apto para su ejecución en el parque informático.

Enviar el programa directamente a la nube de Cytomic

Debido a que Advanced EDR está preparado para no impactar en el rendimiento de la red en el caso de tener que enviar ficheros a la nube de Cytomic, su envío puede demorarse en el tiempo. Si quieres acelerar el proceso, ponte el contacto con el departamento de soporte de Cytomic.

Gestión de la zona de backup / cuarentena

La cuarentena en Advanced EDR es el área de backup donde se copian los elementos clasificados como amenaza que han sido eliminados.

La cuarentena se almacena en el propio equipo del usuario, en el directorio `Quarantine` dentro de la carpeta donde se instaló el software de seguridad. Se trata de un área cifrada e inaccesible al resto de procesos del equipo, para impedir el acceso ni la ejecución de los programas allí contenidos de forma directa.



La cuarentena es compatible con las plataformas Windows, macOS y Linux.

Cytomic establece la acción a ejecutar en función de la clasificación y tipo de elemento detectado:

- **Elementos maliciosos no desinfectables:** se mantienen en cuarentena permanentemente.
- **Elementos maliciosos desinfectables:** el malware de tipo virus se desinfecta y el fichero se restaura a su ubicación original, manteniendo una copia en backup durante 30 días.
- **Elementos no maliciosos restaurados:** si se clasificó de forma errónea un elemento que es *goodware* (falso positivo), se restaura desde la cuarentena a su ubicación original, manteniendo una copia en backup durante 7 días.
- **Elementos sospechosos:** se almacenan en la cuarentena durante 30 días. Si finalmente resultan ser *goodware*, se restauran automáticamente.



Advanced EDR no borra ningún fichero del equipo del usuario. Todos los elementos eliminados son enviados al área de backup.

Visualizar los elementos en cuarentena

Para obtener un listado de los elementos introducidos en la cuarentena:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en el panel apropiado según el tipo de elemento a restaurar de la cuarentena:

- Actividad de malware.
 - Actividad de PUP.
 - Actividad de exploits.
- En los filtros del listado haz clic en las casillas de selección **Movido a cuarentena** y **Eliminado** del campo **Acción** y haz clic en el botón **Filtrar**.

Restaurar elementos de cuarentena

- Haz clic en el menú superior **Estado** y en el panel lateral **Seguridad**.
- Haz clic en el panel apropiado según el tipo de elemento a restaurar de la cuarentena:
 - Actividad de malware
 - Actividad de PUPs
 - Actividad de Exploits
- En el listado, selecciona la amenaza cuyo campo **Acción** muestre **Movido a Cuarentena** o **desinfectado**.
- Haz clic en el icono  del campo **Acción**. Se mostrará una ventana que explica el motivo del movimiento del elemento a cuarentena.
- Haz clic en el enlace **Restaurar y no volver a detectar**. El elemento se moverá a su ubicación original. Se restaurarán también los permisos, propietario, entradas del registro referidas al fichero y otra información.

Análisis forense

Advanced EDR detecta y bloquea la ejecución de malware desconocido o especialmente diseñado para pasar inadvertido por los antivirus tradicionales basados en ficheros de firmas. Esta característica se basa en la monitorización de las acciones ejecutadas por los procesos en los equipos del cliente, que se envían a la nube de Cytomic como parte del flujo de telemetría. La monitorización de procesos permite clasificar cada uno de los programas ejecutados en el equipo del usuario y determinar hasta qué punto ha sido comprometida la red del cliente. El detalle de qué acciones ejecutaron los programas maliciosos ayuda al administrador de la red a tomar las medidas de contención y resolución apropiadas en cada caso.

La consola Web pone a disposición del administrador toda esta información a través de varios recursos, dependiendo del grado de detalle que se necesite:

- Páginas de detalle extendido.
- Tablas de acciones.
- Diagramas de grafos.
- Ficheros Excel.

Contenido del capítulo

Detalle de los programas bloqueados	740
Bloqueo por política avanzada de seguridad	748
Tablas de acciones	754
Grafos de ejecución	759
Ficheros exportados Excel	764
Interpretación de las tablas de acciones y grafos	768

Detalle de los programas bloqueados

Advanced EDR muestra el detalle extendido de los programas cuando son bloqueados por alguna de las tecnologías de detección avanzada soportadas:

- **Detección del malware y PUP**
- **Detección exploit**
- **Detalles del driver**
- **Bloqueo por política avanzada de seguridad**
- **Bloqueo de programas desconocidos en clasificación e Historial de programas bloqueados**

Detección del malware y PUP

Acceso a la ventana Detalle del malware y Detalle de PUP

- Selecciona el menú superior **Estado** y haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana con los listados disponibles.
- Haz clic en el listado **Actividad del malware o PUPs**
- Configura los filtros y haz clic en el botón **Buscar**. Se mostrará un listado de elementos clasificados como malware o PUP.
- Haz clic en un elemento. Se mostrará la ventana **Detección de malware o Detección de PUP**.

O bien:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad**. Se mostrarán los widgets asociados a los módulos de seguridad.
- Haz clic en los widgets **Actividad de malware o Actividad de PUP**.
- Configura los filtros y haz clic en el botón **Buscar**. Se mostrará un listado de elementos clasificados como malware o PUP.
- Haz clic en un elemento. Se mostrará la ventana **Detección de malware o Detección de PUP**.

La ventana de detalle se divide en varias secciones:

- Información general.
- Equipo afectado.
- Impacto de la amenaza en el equipo.
- Origen de la infección.
- Apariciones en otros equipos.

Información general

Campo	Descripción	Valores
Amenaza	Nombre de la amenaza y hash que la identifica.	- Tipo y nombre de la amenaza - Hash (MD5 y/o SHA-256)
Acción	Tipo de acción que Advanced EDR ha ejecutado sobre el elemento. Movido a Cuarentena: el fichero que se ha movido a cuarentena. Bloqueado: el proceso fue bloqueado antes de su ejecución. Eliminado: el fichero se ha eliminado. Detectado: el proceso fue detectado pero no bloqueado por estar la protección avanzada configurada en modo Audit. Permitido (modo auditoría): se informó al usuario de que el malware había realizado acciones sospechosas. Al estar el modo auditoría activado, las amenazas se detectan pero no se bloquean ni eliminan. Consulta Modo auditoría en la página 306	Enumeración Consulta Permitir y volver a impedir la ejecución de elementos en la página 705 para obtener información de como gestionar los bloqueos de la amenazas detectadas. Consulta Restaurar elementos de cuarentena en la página 737.

Tabla 23.1: Campos de la sección Información general en Detección de malware

Equipo afectado



Consulta [Gestión de amenazas, elementos en clasificación y cuarentena](#) en la página 701 para obtener información sobre las acciones que el administrador puede ejecutar sobre los elementos encontrados.

Campo	Descripción
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
Visualizar parches	Si el módulo Cytomic Patch está activado muestra los parches y

Campo	Descripción
disponibles	actualizaciones pendientes de instalar en el equipo.
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza.

Tabla 23.2: Campos de la sección Equipo afectado en Detección de malware, PUP y programas bloqueados en clasificación

Impacto de la amenaza en el equipo

Campo	Descripción
Amenaza	Nombre de la amenaza detectada y cadena resumen de identificación del archivo (hash). Haz clic en los dos botones para ampliar información en Internet mediante el buscador Google y la web de Virustotal. Si la amenaza es de reciente aparición se mostrará la leyenda Nueva amenaza .
Actividad	Resumen de las acciones más importantes ejecutadas por el malware: • Se ha ejecutado  • Ha accedido a datos  • Ha intercambiado datos con otros equipos  • Ver detalle de actividad completo: al hacer clic se muestra la pestaña Actividad tratada en Tablas de acciones. • Ver gráfica de actividad: al hacer clic se muestra la gráfica de Actividad tratada en Grafos de ejecución.
Fecha de detección	Fecha en la que Advanced EDR detectó la amenaza en la red del cliente.
Tiempo de exposición	Tiempo que la amenaza ha permanecido sin clasificar en la red del cliente.

Tabla 23.3: Campos de la sección Impacto de la amenaza en el equipo en Detección de malware, PUP y programas bloqueados en clasificación

Origen de la infección

Campo	Descripción
Equipo origen de la amenaza	Si el intento de infección viene de un equipo de la red del cliente, indica el nombre del equipo.
IP origen de la amenaza	Si el intento de infección viene de un equipo de la red del cliente, indica la dirección IP del equipo.
Usuario origen de la amenaza	Usuario conectado en la máquina origen de la infección.

Tabla 23.4: Campos de la sección Origen de la infección en Detección de malware, PUP y programas bloqueados en clasificación

Apariciones en otros equipos

Muestra todos los equipos de la red donde fue visto el malware detectado.

Campos	Descripción
Equipo	Nombre del equipo.
Ruta del archivo	Ruta y nombre del fichero que contiene el malware.
Fecha primera aparición	Fecha en la que la amenaza fue detectada por primera vez en ese equipo.

Tabla 23.5: Campos de la sección Apariciones en otros equipos en Detección de malware, PUP y programas bloqueados en clasificación

Detección exploit

Acceso a la ventana Detalle del exploit

- Selecciona el menú superior **Estado** y haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana con los listados accesibles.
- Haz clic en el listado **Actividad de exploits**.
- Configura los filtros y haz clic en el botón **Buscar**. Se mostrará un listado de elementos clasificados como exploits.
- Haz clic en un elemento. Se mostrará la ventana **Detección de exploit**.

O bien:

- Selecciona el menú superior **Estado**, panel lateral **Seguridad**. Se mostrarán los widgets asociados a los módulos de seguridad.
- Haz clic en el widget **Actividad de exploits**.
- Configura los filtros y haz clic en el botón **Buscar**. Se mostrará un listado de elementos clasificados como exploits.
- Haz clic en un elemento. Se mostrará la ventana **Detalle de exploit**.

La ventana de detalle se divide en varias secciones:

- Información general.
- Equipo afectado.
- Impacto del exploit en el equipo.

Información general

Campo	Descripción	Valores
Programa comprometido	Nombre del programa que recibió el intento de explotación de una vulnerabilidad y hash que lo identifica.	• Ruta: ruta del programa afectado por el exploit. • Versión: versión del programa afectado por el exploit. • Hash: hash del programa afectado por el exploit (MD5 y/o SHA-256).
Técnica	Identificador de la técnica utilizada para explotar las vulnerabilidades de los programas.	Enlace a la descripción de la técnica utilizada por el exploit.
Acción	Muestra el tipo de acción que Advanced EDR ha ejecutado sobre el programa afectado por el exploit. • Permitido: la protección anti-exploit está configurada en modo Audit. El exploit se ejecutó. • Bloqueado: el exploit fue bloqueado antes de su ejecución. • Permitido por el usuario: se preguntó al usuario del equipo si finalizar el proceso	Enumeración Consulta Permitir y volver a impedir la ejecución de elementos en la página 705 para obtener información de como gestionar los bloqueos de las amenazas detectadas.

Campo	Descripción	Valores
	comprometido y el usuario decidió permitir que el exploit continúe ejecutándose. • Proceso finalizado: el exploit fue eliminado, pero se llegó a ejecutar parcialmente. • Pendiente de reinicio: se informó al usuario del equipo de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto el exploit se seguirá ejecutando. • Permitido (modo auditoría): se informó al usuario de que el exploit ha realizado acciones sospechosas. Al estar el modo auditoría activado, las amenazas se detectan pero no se bloquean ni eliminan. Consulta Modo auditoría en la página 306	

Tabla 23.6: Campos de la sección Información general en Detección exploit

Equipo afectado

Campo	Descripción
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.
Ruta del programa comprometido	Ruta del programa que recibió el intento de explotación de una vulnerabilidad.

Tabla 23.7: Campos de la sección Equipo afectado en Detección exploit

Impacto del exploit en el equipo

Campo	Descripción
Programa comprometido	Ruta y nombre del programa que recibió el intento de explotación. Si Advanced EDR detectó que el programa no está actualizado a la última versión publicada

Campo	Descripción
	por el proveedor, mostrará el aviso  Programa vulnerable.
Actividad	• Se ha ejecutado : el exploit se llegó a ejecutar antes de ser detectado por Advanced EDR. • Ver detalle de actividad completo: al hacer clic se muestra la pestaña Actividad tratada en Tablas de acciones. • Ver gráfica de actividad: al hacer clic se muestra la gráfica de Actividad tratada en Grafos de ejecución
Fecha de detección	Fecha en la que Advanced EDR detectó el exploit en la red del cliente.
Posible origen del exploit	Ruta y nombre del programa que posiblemente inició el exploit.

Tabla 23.8: Campos de la sección Impacto del exploit en el equipo en Detección exploit

Detalles del driver

Acceso a la ventana Detalles del driver

Para acceder a la ventana **Detalles del driver**, sigue los pasos indicados en **Detección exploit** y selecciona en el listado **Actividad de exploit** un elemento cuya técnica de exploit sea **Driver vulnerable**.

La ventana de detalle se divide en varias secciones:

- Información general.
- Equipo afectado.
- Driver vulnerable

Información general

Campo	Descripción	Valores
Driver vulnerable	Nombre del driver cuya carga fue bloqueada.	• Nombre del programa comprometido. • Ruta: driver cuya carga fue bloqueada por la protección. • MD5: código MD5 del driver.

Campo	Descripción	Valores
		• SHA-256: código SHA-256 del driver.
Técnica	Identificador de la técnica utilizada para explotar las vulnerabilidades de los programas.	Driver vulnerables
Acción	Muestra el tipo de acción que Advanced EDR ha ejecutado sobre el exploit: • Bloqueado: el exploit fue bloqueado antes de su ejecución. • Permitido por el usuario: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continúe ejecutándose. • Permitido (modo auditoría): se informó al usuario de que el exploit ha realizado acciones sospechosas. Al estar el modo auditoría activado, las amenazas se detectan pero no se bloquean ni eliminan. Consulta Modo auditoría en la página 306	Enumeración. Consulta Permitir y volver a impedir la ejecución de elementos en la página 705 para obtener información de como gestionar los bloqueos de las amenazas detectadas.

Tabla 23.9: Campos de la sección Información general en Detalles del driver

Equipo afectado

Campo	Descripción
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.
Ruta del driver	Ruta del driver cuya carga fue bloqueada por la protección.

Tabla 23.10: Campos de la sección Equipo afectado en Detalles del driver

Driver vulnerable

Campo	Descripción
Nombre	Nombre del driver cuya carga fue bloqueada por la protección.
Actividad	• Se ha ejecutado : el exploit se llegó a ejecutar antes de ser detectado por Advanced EDR. • Ver detalle de actividad completo: al hacer clic se muestra la pestaña Actividad tratada en Tablas de acciones. • Ver gráfica de actividad: al hacer clic se muestra la gráfica de Actividad tratada en Grafos de ejecución
Fecha de detección	Fecha en la que Advanced EDR detectó el exploit en la red del cliente.
MD5	Código MD5 del driver bloqueado.
SHA-256	Código SHA-256 del driver bloqueado.

Tabla 23.11: Campos de la sección Driver vulnerable

Bloqueo por política avanzada de seguridad

Acceso a la ventana Bloqueo por política avanzada de seguridad

- Selecciona el menú superior **Estado** y haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana con los listados accesibles.
- Haz clic en el listado **Bloqueos por políticas avanzadas de seguridad**.
- Configura los filtros y haz clic en el botón **Buscar**. Se mostrará un listado de elementos bloqueados por política avanzada de seguridad.
- Haz clic en un elemento. Se mostrará la ventana **Bloqueo por política avanzada de seguridad**.

O bien:

- Selecciona el menú superior **Estado** y haz clic en el panel lateral **Seguridad**. Se mostrarán los widgets asociados a los módulos de seguridad.
- Haz clic en el widget **Detecciones mediante políticas avanzadas de seguridad**.

- Configura los filtros y haz clic en el botón **Buscar**. Se mostrará un listado de elementos bloqueados por política avanzada de seguridad.
- Haz clic en un elemento. Se mostrará la ventana **Bloqueo por política avanzada de seguridad**.

La ventana de detalle se divide en varias secciones:

- Información general.
- Equipo.
- Programa bloqueado.

Información general

Campo	Descripción
Programa bloqueado	Nombre del programa bloqueado por el administrador.
Política aplicada	Nombre de la política avanzada de seguridad que bloqueó el programa. Consulta Políticas avanzadas de seguridad en la página 299.
Acción	• Bloqueado: el proceso fue bloqueado antes de su ejecución. • Detectado: el proceso fue detectado pero no bloqueado por estar configurada la política de seguridad en modo Audit. • Permitido (modo auditoría): se informó al usuario de que el proceso ha realizado acciones sospechosas. Al estar el modo auditoría activado, las amenazas se detectan pero no se bloquean ni eliminan. Consulta Modo auditoría en la página 306

Tabla 23.12: Campos de la sección Información general en Bloqueo por política avanzada de seguridad

Equipo

Campo	Descripción
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos. Al hacer clic en el nombre el equipo, se accede a la ventana de información del equipo. Consulta Información de equipo en la página 218.

Campo	Descripción
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.

Tabla 23.13: Campos de la sección Equipo en Bloqueo por política avanzada de seguridad

Programa bloqueado

Campo	Descripción
Nombre	Nombre del programa bloqueado.
MD5	Hash del fichero bloqueado.
SHA-256	Si la detección lo incluye, se muestra el código SHA-256 del programa bloqueado.
Ruta	Dispositivo y carpeta donde se almacena el fichero bloqueado en el equipo del usuario.
Actividad	• Ver detalle de actividad completo: al hacer clic se muestra la pestaña Actividad tratada en Tablas de acciones. • Ver gráfica de actividad: al hacer clic se muestra la gráfica de Actividad tratada en Grafos de ejecución.
Fecha de detección	Fecha en la que Advanced EDR bloqueó la ejecución del programa.

Tabla 23.14: Campos de la sección Programa bloqueado en Bloqueo por política avanzada de seguridad

Bloqueo de programas desconocidos en clasificación e Historial de programas bloqueados

Acceso a la ventana Detalles del programa bloqueado

- Selecciona el menú superior **Estado** y haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana con los listados accesibles.
- Haz clic en el listado **Programas actualmente bloqueados en clasificación**.
- Configura los filtros y haz clic en el botón **Buscar**. Se mostrará un listado de elementos desconocidos en clasificación.

- Haz clic en un elemento. Se mostrará la ventana **Detalles del programa bloqueado**.
- Para abrir el histórico de programas bloqueados por ser desconocidos haz clic en el enlace **Ver historial de bloqueos**.

O bien:

- Selecciona el menú superior **Estado** y haz clic en el panel lateral **Seguridad**. Se mostrarán los widgets asociados a los módulos de seguridad.
- Haz clic en el widget **Programas actualmente bloqueados en clasificación**.
- Configura los filtros y haz clic en el botón **Buscar**. Se mostrará un listado de elementos desconocidos en clasificación.
- Haz clic en un elemento. Se mostrará la ventana **Detalles del programa bloqueado**.

La ventana de detalle se divide en varias secciones:

- Información general.
- Equipo.
- Actividad del programa en el equipo.
- Origen.

Información general

Campo	Descripción
Programa	Nombre del programa bloqueado. Al situar el cursor en el icono  se muestra información sobre el código MD5 y/o SHA-256 del programa bloqueado.
Acción	• Bloqueado • Reclasificado a Goodware • Reclasificado a Malware • Reclasificado a PUP • Eliminado del listado
Probabilidad de que sea malicioso	Solo se muestra si el elemento todavía no se ha clasificado. • Baja • Media • Alta • Muy Alta

Campo	Descripción
Técnica de clasificación	• Clasificado por técnicos del laboratorio de WatchGuard: el elemento fue clasificado manualmente por los técnicos de Cytomic. • Clasificado automáticamente por la inteligencia colectiva de WatchGuard: el elemento fue clasificado por los procesos automáticos de machine learning de Cytomic.
Reclasificación completada	Fecha en la que se completó la clasificación del elemento.
Tiempo de reclasificación	Tiempo que Advanced EDR tardó en clasificar el elemento. Al situar el cursor en el icono  se muestra el campo Inicio de la reclasificación. Consulta Cálculo del tiempo de reclasificación de ficheros desconocidos en la página 722
Estado	Estado del proceso de clasificación y origen del error si no se ha podido iniciar el proceso de investigación.
Desbloquear	Permite la ejecución del programa antes de que sea clasificado. Consulta Permitir y volver a impedir la ejecución de elementos en la página 705 para obtener información de como gestionar los bloqueos de las amenazas detectadas.

Tabla 23.15: Campos de la sección Información general en Detalle del programa bloqueado

Equipo

Campo	Descripción
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.
Modo de protección	Configuración de la protección avanzada en el momento de producirse el bloqueo (Audit, Hardening, Lock).

Campo	Descripción
Ruta de detección	Ruta del programa bloqueado dentro del equipo del usuario o servidor.

Tabla 23.16: Campos de la sección Equipo en Detalle del programa bloqueado

Actividad del programa en el equipo



Campo	Descripción
Programa	Nombre del programa bloqueado.
Actividad	Resumen de las acciones más importantes ejecutadas por el malware: • Se ha ejecutado • Ha accedido a datos • Ha intercambiado datos con otros equipos • Ver detalle de actividad completo: al hacer clic se muestra la pestaña Actividad tratada en Tablas de acciones. • Ver gráfica de actividad: al hacer clic se muestra la gráfica de Actividad tratada en Grafos de ejecución.
Fecha de detección	Fecha en la que Advanced EDR bloqueó la ejecución del programa.
Tiempo de exposición	Tiempo que la amenaza ha permanecido sin clasificar en la red del cliente.

Tabla 23.17: Campos de la sección Actividad del programa en el equipo en Detalle del programa bloqueado

Origen



Campo	Descripción
Equipo origen	Si el fichero viene de un equipo de la red del cliente, indica el nombre del equipo.
IP origen	Si el fichero viene de un equipo de la red del cliente, indica la dirección IP del equipo.

Campo	Descripción
Usuario origen	Usuario conectado en el equipo origen del fichero.

Tabla 23.18: Campos de la sección Origen en Detalle del programa bloqueado

Tablas de acciones

Advanced EDR muestra 15 días de telemetría asociada a cada detección realizada por la protección avanzada, donde se indican las acciones de los programas envueltos en el ataque.

Para acceder a la tabla de acciones de las amenazas abre la ventana de detalle (consulta [Detalle de los programas bloqueados](#)) y haz clic en la pestaña **Actividad**.

La información de la amenaza se muestra en una tabla de acciones, que incluye los eventos producidos más relevantes.



La cantidad de acciones ejecutadas por un proceso es muy alta, visualizarlas todas dificultaría la extracción de información útil para realizar un análisis forense.

El contenido de la tabla se presenta inicialmente ordenado por fecha, de esta forma es más fácil seguir el curso de la amenaza.

La tabla de acciones contiene los campos mostrados a continuación:

Campo	Comentario	Valores
Fecha	Fecha de la acción registrada.	Fecha
Nº veces	Número de veces que se ejecutó la acción. Una misma acción ejecutada varias veces de forma consecutiva solo aparece una vez en el listado de acciones con el campo Nº veces actualizado.	Numérico
Acción	Tipo de acción registrada en el sistema y línea de comandos asociada a la ejecución de la acción.	• Descargado de • Comunica con • Accede a datos • Accede • Es accedido por

Campo	Comentario	Valores
		• LSASS.EXE abre • LSASS.EXE es abierto por • Es ejecutado por • Ejecuta • Es creado por • Crea • Es modificado por • Modifica • Es cargado por • Carga • Es borrado por • Borra • Es renombrado por • Renombra • Es matado por • Mata proceso • Proceso suspendido • Crea hilo remoto • Hilo inyectado por • Es abierto por • Abre • Crea clave apuntando a Exe • Modifica clave apuntando a Exe.

Campo	Comentario	Valores
		• Intenta detener • Finalizado por
Ruta/URL/Clave de registro /IP:Puerto	• Entidad de la acción. Según el tipo de acción contiene diferentes valores. • Clave del registro: acciones que impliquen modificación del registro de Windows. • IP:Puerto: acciones que implican una comunicación con un equipo local o remoto. • Ruta: acciones que implican acceso al disco duro del equipo. Para obtener más información consulta Formato de la ruta. • URL: acciones que implican el acceso a una URL.	
Hash del archivo/Valor del registro /Protocolo-Dirección/Descripción	Campo que complementa a la entidad: • Hash del archivo: para todas las acciones que implican acceder a un fichero. En el caso de incluir código SHA-256, éste se muestra junto al código MD5 separado mediante el carácter . Ejemplo: d131dd02c5e6eec4 4d70210e28716ccaa7cd4ddb79 • Valor del Registro: para todas las acciones que implican acceder al registro. • Protocolo-Dirección: para todas las acciones que implican comunicarse con un equipo local o remoto. Los valores posibles son:	

Campo	Comentario	Valores
	- TCP - UDP - Bidirectional - Unknown - Descripción	
Confiable	El fichero está firmado digitalmente.	Binario

Tabla 23.19: Campos de la tabla de acciones de una amenaza

Formato de la ruta

Se utilizan números y el carácter “|” para indicar la unidad de almacenamiento y las carpetas de sistema respectivamente:

Código	Tipo de unidad de almacenamiento
0	Unidad desconocida.
1	Ruta inválida. Por ejemplo, una unidad que no tiene un volumen montado.
2	Unidad extraíble. Por ejemplo, un disquete, una memoria USB o un lector de tarjetas.
3	Unidad interna. Por ejemplo, un disco duro o un disco SSD.
4	Unidad remota. Por ejemplo, una unidad de red.
5	Unidad de CD-ROM / DVD.
6	Unidad disco RAM.

Tabla 23.20: Códigos utilizados para indicar el tipo de unidad

A continuación se muestran las partes de una ruta a modo de ejemplo:

```
3|TEMP|\app\a_470.exe
```

- **3**: Unidad interna. El fichero está almacenado en el disco duro del equipo.
- **[TEMP]**: el fichero reside en la carpeta de sistema \windows\temp\ del equipo.

- **\app**: nombre de la carpeta donde está almacenado el fichero.
- **a_470.exe**: nombre del fichero.

Sujeto y predicado de las acciones

El formato utilizado para presentar la información en el listado de acciones mantiene cierto paralelismo con el lenguaje natural:

- Todas las acciones tienen como sujeto el fichero clasificado como amenaza. Este dato no se indica en cada línea de la tabla de acciones porque es común para todas las líneas.
- Todas las acciones tienen un verbo que relaciona el sujeto (la amenaza clasificada) con un complemento, llamado entidad. La entidad se corresponde con el campo **Ruta/URL/Clave de registro /IP:Puerto** de la tabla.
- La entidad se complementa con un segundo campo que añade información a la acción, indicado en el campo **Hash del archivo/Valor del registro /Protocolo-Dirección/Descripción**.

En **Listado de acciones de una amenaza de ejemplo** se muestran dos acciones de ejemplo de un mismo malware hipotético:

Fecha	Nº veces	Acción	Ruta/URL/Clave de registro /IP:Puerto	Hash del archivo/Valor del registro /Protocolo-Dirección/Descripción	Confiable
3/30/2015 4:38:40 PM	1	Comunica con	54.69.32.99:80	TCP-Bidirectional	NO
3/30/2015 4:38:45 PM	1	Carga	PROGRAM_FILES \MOVIES TOOLBAR\SAFETYNTN	9994BF035813FE8EB6BC98ECCBD5B0E1	NO

Tabla 23.21: Listado de acciones de una amenaza de ejemplo

La primera acción indica que el malware (sujeto) se conecta (Acción **Comunica con**) con la dirección IP 54.69.32.99:80 (entidad) mediante el protocolo TCP-Bidireccional.

La segunda acción indica que el malware (sujeto) carga (Acción **Carga**) la librería PROGRAM_FILES | \MOVIES TOOLBAR\SAFETYNTN\SAFETYCRT.DLL con hash 9994BF035813FE8EB6BC98ECCBD5B0E1.

Al igual que en el lenguaje natural, en Advanced EDR se implementan dos tipos de oraciones:

- **Activa:** son acciones predicativas (con un sujeto y un predicado) relacionados por un verbo en forma activa. En estas acciones, el verbo de la acción relaciona el sujeto, que siempre es el proceso clasificado como amenaza y un complemento directo, la entidad, que puede ser de múltiples tipos según la acción. Ejemplos de acciones activas son:
 - Comunica con
 - Carga
 - Crea
- **Pasiva:** son acciones donde el sujeto (el proceso clasificado como amenaza) pasa a ser sujeto paciente (que recibe la acción, no la ejecuta) y el verbo aparece en forma pasiva (ser + participio). En este caso el verbo pasivo relaciona el sujeto pasivo que recibe la acción con la entidad, que es la que ejecuta la acción. Ejemplos de acciones pasivas son:
 - Es creado por
 - Descargado de

Ejemplo de acción pasiva muestra una acción pasiva de ejemplo para un malware hipotético:

Fecha	Nº veces	Acción	Ruta/URL/Cla ve de registro /IP:Puerto	Hash del archivo/Valor del registro /Protocolo- Dirección/Descripción	Con- fiable
3/30/201 5 4:51:46 PM	1	Es ejecutad o por	WINDOWS \ explorer.e xe	7522F548A84ABAD8F A516D E5AB3931EF	NO

Tabla 23.22: Ejemplo de acción pasiva

En esta acción el malware (sujeto pasivo) es ejecutado (acción pasiva **Es ejecutado por**) por el programa WINDOWS | \explorer.exe (entidad) de hash 7522F548A84ABAD8FA516DE5AB3931EF.



Las acciones de tipo activa permiten inspeccionar en detalle los pasos que ha ejecutado la amenaza. Por el contrario, las acciones de tipo pasivo suelen reflejar el vector de infección utilizado por el malware (qué proceso lo ejecutó, qué proceso lo copió al equipo del usuario etc.).

Grafos de ejecución

Advanced EDR visualiza en un grafo el período de 15 días con la telemetría asociada a cada detección realizada por la protección avanzada. En este grafo se muestra de forma gráfica las acciones de los programas que envueltos en el ataque.

Para acceder al grafo de ejecución abre la ventana de detalle (consulta **Detalle de los programas bloqueados**), haz clic en la pestaña **Actividad** y en el botón **Ver gráfica de actividad**.

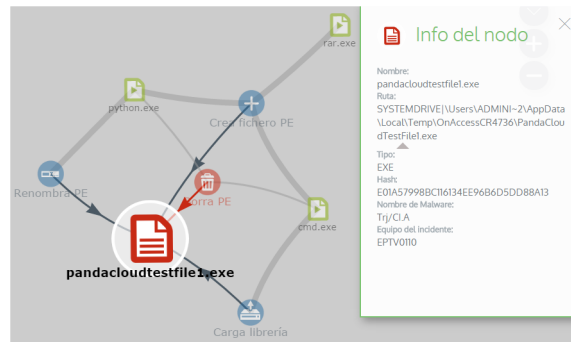


Figura 23.1: Amenaza representada mediante grafos

- **Actividad de Malware y PUPs** para abrir la ventana **Detección del malware**.
- **Actividad de Exploits** para abrir la ventana **Detección de exploit**.
- **Programas actualmente bloqueados en clasificación** para abrir la ventana **Detalles del programa bloqueado**.
- **Bloqueos por políticas avanzadas de seguridad** para abrir la ventana **Bloqueo por política avanzada de seguridad**.

Haz clic en la pestaña **Actividad** y **Ver gráfica de actividad** para mostrar el grafo de ejecución de la amenaza.

Los grafos de ejecución representan de forma visual la información mostrada en las tablas de acciones, poniendo énfasis en el enfoque temporal. Los grafos se utilizan inicialmente para tener, de un solo vistazo, una idea general de las acciones desencadenadas por la amenaza.

Diagramas

La cadena de acciones en la vista de grafos de ejecución se representa mediante dos elementos:

- **Nodos:** en su mayoría acciones o elementos informativos.
- **Líneas y flechas:** unen los nodos de acción e informativos para establecer un orden temporal y asignar a cada nodo el rol de “sujeto” o “predicado”.

Nodos

Muestran la información mediante su icono asociado, color y un panel descriptivo que se muestra a la derecha de la pantalla cuando se seleccionan con el ratón.

El código de colores utilizado es:

- **Rojo:** elemento no confiable, malware, amenaza.
- **Naranja:** elemento desconocido, no catalogado.
- **Verde:** elemento confiable, goodware.

Representación gráfica de acciones en el diagrama de grafos lista los nodos de tipo acción junto con una breve descripción:

Símbolo	Descripción	Símbolo	Descripción
	Fichero descargado. Fichero comprimido creado.		Fichero ejecutable borrado.
	Socket / comunicación usada.		Librería cargada.
	La monitorización comenzó.		Servicio instalado.
	Proceso creado.		Fichero ejecutable renombrado.
	Fichero ejecutable creado. Librería creada. Clave en el registro creada.		Proceso detenido o cerrado.
	Fichero ejecutable modificado. Clave de registro modificada.		Hilo creado remotamente.
	Fichero ejecutable mapeado para escritura.		Fichero comprimido abierto.

Tabla 23.23: Representación gráfica de acciones en el diagrama de grafos

Tipos de nodo en el diagrama de grafos lista los nodos de tipo descriptivo junto con una breve descripción:

Símbolo	Descripción
	Nombre de fichero y extensión. Verde: goodwill.

Símbolo	Descripción
	• Naranja: no catalogado. • Rojo: malware/PUP.
	Equipo interno (está en la red corporativa). • Verde: confiable. • Naranja: desconocido. • Rojo: no confiable.
	Equipos externos. • Verde: confiable. • Naranja: desconocido. • Rojo: no confiable.
	País asociado a la IP de un equipo externo.
	Fichero y extensión.
	Clave del registro.

Tabla 23.24: Tipos de nodo en el diagrama de grafos

Líneas y flechas

Las líneas del diagrama de grafos relacionan los diferentes nodos y ayudan a establecer visualmente el orden de ejecución de las acciones.

Los dos atributos de una línea son:

- **Grosor de la línea**: número de veces que ha aparecido la relación en el diagrama. A mayor número de veces mayor tamaño de la línea.
- **Flecha**: dirección de la relación entre los dos nodos.

La línea temporal (Timeline)

Controla la visualización de la cadena de acciones ejecutadas por la amenaza a lo largo del tiempo. Mediante los botones situados en la parte inferior de la pantalla visualiza el momento preciso donde la amenaza ejecutó cierta acción, y recupera información extendida para ayudar en los procesos de análisis forense.

Es posible seleccionar un intervalo concreto de la línea temporal arrastrando los selectores de intervalo hacia la izquierda o derecha para abarcar la franja más interesante.

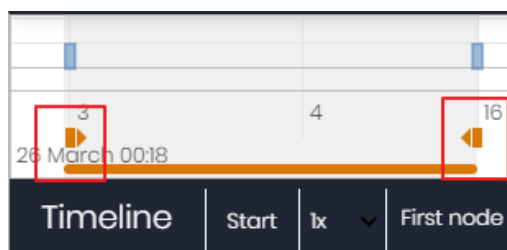


Figura 23.2: Selectores del intervalo temporal a presentar

Una vez seleccionado el intervalo, el grafo mostrará únicamente las acciones y nodos que caigan en dentro de él. El resto de acciones y nodos quedará difuminado en el diagrama.

Las acciones de la amenaza se representan en la línea temporal como barras verticales acompañadas del time stamp, que marca la hora y minuto donde ocurrieron.

Para poder ver la ejecución completa de la amenaza y la cadena de acciones que ejecutó, se utilizan los siguientes controles:

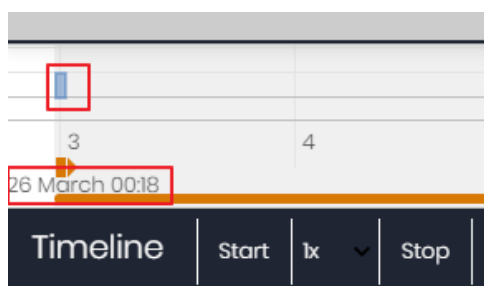


Figura 23.3: Timestamp, fecha y acciones de la amenaza

- **Iniciar:** comienza la ejecución de la Timeline a velocidad 1x. Los grafos y las líneas de acciones irán apareciendo según se vaya recorriendo la línea temporal.
- **1x:** establece la velocidad de recorrido de la línea temporal.
- **Detener:** detiene la ejecución de la línea temporal.
- **+ y -:** zoom in y zoom out de la línea temporal.
- **< y >:** mueve la selección del nodo al inmediatamente anterior o posterior.
- **Zoom inicial:** recupera el nivel de zoom inicial si se modificó con los botones + y -.
- **Seleccionar todos los nodos:** mueve los selectores temporales para abarcar toda la línea temporal.

- **Primer nodo:** establece el intervalo temporal en el inicio, paso necesario para iniciar la visualización de la TimeLine completa.



Para poder visualizar el recorrido completo de la Timeline primero selecciona “Primer nodo” y después “Iniciar”. Para ajustar la velocidad de recorrido selecciona el botón 1x.

Filtros

En la parte superior del diagrama de grafos se encuentran los controles para filtrar la información que se mostrará.

- **Acción:** desplegable que selecciona un tipo de acción de entre todas las ejecutadas por la amenaza. El diagrama solo mostrará los nodos que coincidan con el tipo de acción seleccionada y aquellos nodos adyacentes relacionados con esta acción.
- **Entidad:** desplegable que selecciona una entidad (contenido del campo Path/URL/Entrada de registro /IP:Puerto).

Recolocar los nodos y zoom general del grafo

Para mover el grafo en las cuatro direcciones y hacer zoom in o zoom out utiliza los controles situados en la parte superior derecha del grafo.



Para hacer zoom in y zoom out más fácilmente utiliza la rueda central del ratón.

- El símbolo  abandona la vista de grafos.
- Para ocultar la zona de botones Timeline a fin de ganar espacio de la pantalla haz clic en el icono  situado en la parte inferior derecha del grafo.
- El comportamiento del grafo representando en pantalla es configurable mediante el panel accesible al seleccionar el botón  situado en la zona superior izquierda del grafo.

Ficheros exportados Excel

Advanced EDR permite exportar a un fichero Excel la telemetría del contexto asociada al proceso en el momento en que se detecta el ataque por parte de alguna de las tecnologías avanzadas. Para descargar el fichero Excel consulta el apartado **Detalle de los programas bloqueados** y haz clic en el icono situado en la parte superior derecha del listado. Al elegir la opción **Exportar listado y detalles** se descargará un fichero Excel con los detalles extendidos de todas las amenazas mostradas en el listado.

Campo	Descripción	Valores
Fecha	Fecha de la acción registrada.	Fecha
MD5	Código MD5 del fichero bloqueado.	Cadena de caracteres
SHA-256	Código SHA-256 del fichero bloqueado.	Cadena de caracteres
Política	Nombre de la política que bloqueó el fichero. Disponible en el listado Detecciones mediante políticas avanzadas de seguridad .	Cadena de caracteres
Amenaza	Nombre de la amenaza. Disponible en los listados: - Actividad del malware - Actividad de PUPs - Programas actualmente bloqueados en clasificación - Historial de programas bloqueados	Cadena de caracteres
Usuario	Cuenta de usuario bajo la cual se ejecutó la amenaza.	Cadena de caracteres
Equipo	Nombre del equipo donde se encontró la amenaza.	Cadena de caracteres
Ruta	Nombre de la amenaza, dispositivo y carpeta donde se almacena dentro del equipo del usuario.	Cadena de caracteres
Acceso a datos	La amenaza ha accedido a ficheros que residen en el equipo del usuario. Disponible en los listados: - Actividad del malware - Actividad de PUPs - Programas actualmente bloqueados en clasificación	Binario

Campo	Descripción	Valores
	• Historial de programas bloqueados	
Acción	Tipo de acción registrada en el sistema.	• Descargado de • Comunica con • Accede a datos • Accede • Es accedido por • LSASS.EXE abre • LSASS.EXE es abierto por • Es ejecutado por • Ejecuta • Es creado por • Crea • Es modificado por • Modifica • Es cargado por • Carga • Es borrado por • Borra • Es renombrado por • Renombra • Es matado por • Mata proceso • Proceso suspendido • Crea hilo remoto • Hilo inyectado por • Es abierto por • Abre • Crea • Es creado por

Campo	Descripción	Valores
		• Crea clave apuntando a Exe • Modifica clave apuntando a Exe • Intenta detener • Finalizado por
Línea de comandos	Línea de comandos asociada a la ejecución de la acción.	Cadena de caracteres
Fecha del evento	Fecha y hora en la que el evento se registró en el equipo del cliente.	Cadena de caracteres
Nº veces	Número de veces que se ejecutó la acción. Una misma acción ejecutada varias veces de forma consecutiva solo aparece una vez en el listado de acciones con el campo Nº veces actualizado.	Numérico
Ruta/URL/Clave de registro/IP:Puerto	Entidad de la acción. Según sea el tipo de acción podrá contener diferentes valores.	• Clave del registro: acciones que implican modificación del registro de Windows. • IP:Puerto: acciones que implican una comunicación con un equipo local o remoto. • Ruta: acciones que implican acceso al disco duro del equipo. • URL: acciones que implican el acceso a una URL.
Hash del archivo/Valor del registro/Protocolo-Dirección/Descripción	Campo que complementa a la entidad.	• Hash del archivo: acciones que implican acceso a un archivo.

Campo	Descripción	Valores
		• Valor del registro acciones que implican un acceso al registro. • Protocolo-Dirección: acciones que implican una comunicación con un equipo local o remoto. Los valores posibles son: • TCP • UDP • Bidirectional • UnKnown • Descripción
Confiable	El fichero bloqueado está firmado digitalmente.	Binario

Tabla 23.25: Campos del fichero exportado Listado y detalles

Interpretación de las tablas de acciones y grafos

Las tablas de acciones y grafos de actividad muestran 15 días de telemetría asociada a cada detección realizada por la protección avanzada, donde se indican las acciones de los programas envueltos en el ataque. Por esta razón se requieren ciertos conocimientos técnicos para poder extraer pautas e información clave en cada situación.

A continuación, se ofrecen unas directrices básicas para interpretar las tablas de acciones mediante varios ejemplos de amenazas reales.



El nombre de las amenazas aquí indicadas puede variar entre diferentes proveedores de seguridad. Para identificar un malware concreto se recomienda utilizar su hash.

Ejemplo 1: actividad del malware Trj/OCJ.A

En la pestaña **Detalles** se muestra la información fundamental del malware encontrado. En este caso los datos relevantes son los siguientes:

- **Amenaza:** Trj/OCJ.A
- **Equipo:** XP-BARCELONA1
- **Ruta de detección:** TEMP|\Rar\$EXa0.946\appnee.com.patch.exe

Actividad

La pestaña **Actividad** contiene acciones ya que el modo de Advanced EDR configurado era Hardening y el malware ya residía en el equipo en el momento en que Advanced EDR se instaló, siendo desconocido en el momento de su ejecución.

Hash

Con la cadena de hash se podrá obtener más información de recursos web como Virus total para tener una idea general de la amenaza y funcionamiento.

Ruta de detección

La ruta donde se detectó el malware por primera vez en el equipo pertenece a un directorio temporal y contiene la cadena RAR: la amenaza procede de un fichero empaquetado que el programa WinRAR descomprimió temporalmente en el directorio, y dió como resultado el ejecutable appnee.com.patch.exe.

Pestaña Actividad

Paso	Fecha	Acción	Ruta
1	3:17:00	Es creado por	PROGRAM_FILES \WinRAR\WinRAR.exe
2	3:17:01	>Es ejecutado por	PROGRAM_FILES \WinRAR\WinRAR.exe
3	3:17:13	Crea	TEMP \bassmod.dll
4	3:17:34	Crea	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK
5	3:17:40	Modifica	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\amtlib.dll
6	3:17:40	Borra	PROGRAM_FILES \ADOBE\ACROBAT 11.0\ACROBAT\AMTLIB.DLL.BAK
7	3:17:41	Crea	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\ACROBAT.DLL.BAK
8	3:17:42	Modifica	PROGRAM_FILES \Adobe\ACROBAT

Paso	Fecha	Acción	Ruta
			11.0\Acrobat\Acrobat.dll
9	3:17:59	Ejecuta	PROGRAM_FILES \Google\ Chrome\Application\chrome.exe

Tabla 23.26: Listado de acciones Trj/OCJ.A

Los pasos 1 y 2 indican que el malware fue descomprimido por el WinRar.Exe y ejecutado desde el mismo programa: el usuario abrió el fichero comprimido e hizo clic en el binario que contiene.

Una vez en ejecución, en el paso 3 el malware crea una dll (bassmod.dll) en una carpeta temporal y otra (paso 4) en el directorio de instalación del programa Adobe Acrobat 11. En el paso 5 también modifica una dll de Adobe, quizá para aprovechar algún tipo de exploit del programa.

Después de modificar otras dlls lanza una instancia de Chrome y en ese momento termina la Timeline; Advanced EDR catalogó el programa como amenaza después de esa cadena de acciones sospechosas y detuvo su ejecución.

En la Timeline no aparecen acciones sobre el registro, de modo que es muy probable que el malware no sea persistente o no haya podido ejecutarse hasta el punto de sobrevivir a un reinicio del equipo.

El programa Adobe Acrobat 11 ha resultado comprometido, de modo que se recomienda su reinstalación. Gracias a que Advanced EDR monitoriza ejecutables tanto si son goodware como malware, la ejecución de un programa comprometido será detectada en el momento en que desencadene acciones peligrosas, terminando en su bloqueo.

Ejemplo 2: comunicación con equipos externos en BetterSurf

BetterSurf es un programa potencialmente no deseado que modifica el navegador instalado en el equipo del usuario e inyecta anuncios en las páginas Web que visite.

En la pestaña **Detalles** se muestra la información fundamental del malware encontrado. En este caso se cuenta con los siguientes datos:

- **Nombre:** PUP/BetterSurf
- **Equipo:** MARTA-CAL
- **Ruta de detección:** PROGRAM_FILES|\VER0BLOCKANDSURF\N4CD190.EXE
- **Tiempo de permanencia:** 11 días 22 horas 9 minutos 46 segundos

Tiempo de exposición

En este caso el tiempo de exposición ha sido muy largo: durante casi 12 días el malware ha estado latente en la red del cliente. Este comportamiento es cada vez más usual, y puede deberse a varios motivos: que el malware no haya realizado ninguna acción sospechosa hasta muy tarde, o que simplemente el usuario descargó el fichero, pero tardó en ejecutarlo. En ambos casos la amenaza no era conocida anteriormente, con lo cual no se disponía de una firma con la que el sistema antivirus pueda compararla.

Pestaña Actividad

Paso	Fecha	Acción	Ruta
1	08/03/2015 11:16	Es creado por	TEMP \08c3b650-e9e14f.exe
2	18/03/2015 11:16	Es creado por	SYSTEM \services.exe
3	18/03/2015 11:16	Carga	PROGRAM_ FILES \VER0BLOF\N4Cd190.dll
4	18/03/2015 11:16	Carga	SYSTEM \BDL.dll
5	18/03/2015 11:16	Comunica con	127.0.0.1:13879
6	18/03/2015 11:16	Comunica con	37.58.101.205:80
7	18/03/2015 11:17	Comunica con	5.153.39.133:80
8	18/03/2015 11:17	Comunica con	50.97.62.154:80
9	18/03/2015 11:17	Comunica con	50.19.102.217:80

Tabla 23.27: Listado de acciones PUP/BetterSurf

Se puede apreciar como el malware establece comunicación con varias IPs. La primera de ellas (paso 5) es el propio equipo y el resto son IPs del exterior a las que se conecta por el puerto 80, de las cuales probablemente se descarguen los contenidos de publicidad.

La principal medida de prevención en este caso será bloquear las IPs en el cortafuegos corporativo.



Antes de añadir reglas para el bloqueo de IPs en el cortafuegos corporativo se recomienda consultar las IPs a bloquear en el RIR asociado (RIPE, ARIN, APNIC etc.) para comprobar la red del proveedor al que pertenecen. En muchos casos la infraestructura remota utilizada por el malware es compartida con servicios legítimos alojados en proveedores, tales como Amazon y otros, de modo que bloquear IPs equivaldría a bloquear también el acceso a páginas Web legítimas.

Ejemplo 3: acceso al registro con PasswordStealer.BT

PasswordStealer.BT es un troyano que registra la actividad del usuario en el equipo y envía la información obtenida al exterior. Entre otras cosas, es capaz de capturar la pantalla del usuario, registrar las teclas pulsadas y enviar ficheros a un servidor C&C (Command & Control).

En la pestaña **Detalles** se muestra la información fundamental de la amenaza encontrada. En este caso se cuenta con los siguientes datos relevantes:

Ruta de la detección: `APPDATA\microsoftupdates\micupdate.exe`

Por el nombre y la localización del ejecutable, el malware se hace pasar por una actualización de Microsoft. Este malware en concreto no tiene capacidad para contagiar equipos por sí mismo, requiere que el usuario ejecute de forma manual la amenaza.

Pestaña Actividad

El modo de Advanced EDR configurado era Hardening: el malware ya residía en el equipo en el momento en que Advanced EDR se instaló y era desconocido en el momento de su ejecución.

Tabla de acciones

Paso	Fecha	Acción	Ruta
1	31/03/2015 23:29	Es ejecutado por	PROGRAM_FILESX86\internet explorer\iexplore.exe
2	31/03/2015 23:29	Es creado por	INTERNET_CACHE\Content.IE5\QGV8PV80\index[1].php
3	31/03/2015 23:30	Crea clave apuntando a Exe	\REGISTRY\USER\S-1-5[...]9-5659\Software\Microsoft\Windows\CurrentVersion\Run?MicUpdate
4	31/03/2015 23:30	Ejecuta	SYSTEMX86\notepad.exe
5	31/03/2015	Hilo inyectado	SYSTEMX86\notepad.exe

Paso	Fecha	Acción	Ruta
	23:30	por	

Tabla 23.28: Listado de acciones PasswordStealer.BT

En este caso, el malware fue generado en el paso 2 por una página web y ejecutado por Internet Explorer.



El orden de las acciones tiene una granularidad de 1 microsegundo. Por esta razón, las acciones ejecutadas dentro del mismo microsegundo pueden aparecer desordenadas en la Timeline, como sucede en el paso 1 y paso 2.

Una vez ejecutado, el malware se hace persistente en el equipo del usuario en el paso 3, añadiendo una rama en el registro que lanzará el programa en el inicio del sistema. Después comienza a ejecutar acciones propias del malware, tales como arrancar un `notepad` e inyectar código en uno de sus hilos.

Como acción de resolución en este caso, y en ausencia de un método de desinfección conocido, se puede minimizar el impacto de este malware borrando la entrada del registro. Es muy posible que en un equipo infectado el malware impida modificar dicha entrada; dependiendo del caso sería necesario arrancar el equipo en modo seguro o con un CD de arranque para borrar dicha entrada.

Ejemplo 4: acceso a datos confidenciales en Trj/Chgt.F

Trj/Chgt.F fue publicado por wikileaks a finales de 2014 como herramienta utilizada por las agencias gubernamentales de algunos países para realizar espionaje selectivo.

En este ejemplo se muestra directamente a la pestaña **Actividad** para observar el comportamiento de esta amenaza avanzada.

Tabla de acciones

Paso	Fecha	Acción	Ruta
1	4/21/2015 2:17:47	Es ejecutado por	SYSTEMDRIVE \Python27\pythonw.exe
2	4/21/2015 2:18:01	Accede a datos	#.XLS
3	4/21/2015 2:18:01	Accede a datos	#.DOC
4	4/21/2015 2:18:03	Crea	TEMP \doc.scr

Paso	Fecha	Acción	Ruta
5	4/21/2015 2:18:06	Ejecuta	TEMP \doc.scr
6	4/21/2015 2:18:37	Ejecuta	PROGRAM_FILES\Microsoft Office\Office12\WINWORD.EXE
7	4/21/2015 8:58:02	Comunica con	192.168.0.1:2042

Tabla 23.29: Listado de acciones Trj/Chgt.F

Inicialmente el malware es ejecutado por el intérprete de Python (paso 1) para luego acceder a un documento de tipo Excel y otro de tipo Word (paso 2 y 3). En el paso 4 se ejecuta un fichero de extensión `scr`, probablemente un salvapantallas con algún tipo de fallo o error que provoque una situación anómala en el equipo aprovechada por el malware.

En el paso 7 se produce una conexión de tipo TCP. La dirección IP es privada de modo que se estaría conectando a la red del propio cliente.

En este caso se deberá comprobar el contenido de los ficheros accedidos para evaluar la pérdida de información, aunque viendo la Timeline la información accedida no parece haber sido extraída de la red del cliente.

Advanced EDR desinfectará por sí mismo la amenaza y bloqueará de forma automática posteriores ejecuciones del malware en este y en otros clientes.

Capítulo 24

Alertas

El sistema de alertas es un recurso utilizado por Advanced EDR para comunicar de forma rápida al administrador situaciones que afectan al buen funcionamiento del servicio de seguridad.

En conjunto, las alertas informan al administrador de las situaciones mostradas a continuación:

- Detección de malware, PUP o exploits.
- Detecciones de ataques de red
- Detección de indicadores de ataque (IOA)
- Reclasificación de elementos desconocidos, malware o PUP.
- Bloqueo de procesos desconocidos para Advanced EDR y en proceso de clasificación.
- Cambios en el estado de las licencias.
- Errores de instalación y desprotegidos.

Contenido del capítulo

Alertas por correo	775

Alertas por correo

Son mensajes generados por Advanced EDR cuando se producen determinados eventos y enviados a las cuentas de correo configuradas como destinatarios, generalmente mantenidas por los administradores de la red.

Acceso a la configuración de alertas

Desde el menú superior **Configuración**, en el panel de la izquierda **Mis alertas** se accede al menú de **Alertas** por correo en el que se establecen las opciones de las alertas por correo.

Configuración de alertas

La configuración de las alertas se divide en tres partes:

- **Enviar alertas en los siguientes casos:** selecciona que eventos generan una alerta. Consulta [Tipos de alertas](#) para más información.
- **Enviar alertas a la siguiente dirección:** introduce las direcciones de correo que recibirán la alerta.
- **Enviar las alertas en el siguiente idioma:** elige el idioma del mensaje de alerta entre los soportados por la consola:
 - Alemán
 - Español
 - Francés
 - Inglés
 - Italiano
 - Japonés
 - Magiar
 - Portugués
 - Sueco

Exportación de alertas

Si el usuario de la consola posee permiso de control total, puede exportar la configuración **Mis alertas** de todos los usuarios de una cuenta que hayan especificado direcciones de correo destinatarias de las alertas. Consulta [Configuración de alertas](#)

Para exportar las configuraciones, haz clic en el icono , situado en la esquina superior derecha de la ventana **Alertas por correo**.

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente.	Cadena de caracteres
Usuario	Usuario de la consola de Advanced EDR que ha configurado Mis alertas .	Cadena de caracteres
Email de Acceso	Dirección de correo con la que el usuario accede a la consola de Advanced EDR	Cadena de caracteres

Campo	Descripción	Valores
Bloqueado	Indica si el usuario tiene denegado el acceso a la consola de Advanced EDR. Consulta Borrar o bloquear cuentas de usuarios en la página 64.	• Sí • No
Alertas seleccionadas para envío	Indica si hay casos activados en la configuración Mis alertas . Consulta Configuración de alertas .	• Si • No
Dirección del destinatario	Direcciones de correo especificadas por el usuario como receptoras de las alertas.	Cadena de caracteres

Tabla 24.1: Campos del fichero exportado Destinatarios de las alertas

Nivel de acceso del administrador y envío de alertas

Las alertas se definen de forma independiente por cada usuario de la consola. El contenido de una alerta queda limitado por la visibilidad de los equipos administrados que tiene asignado el rol de la cuenta de usuario.

Tipos de alertas

Tipo	Frecuencia	Condición	Información contenida
Detecciones de exploits	Máximo de 10 alertas al día por equipo y exploit	• Por cada detección de exploit que se produzca. • Solo en equipos Windows.	• Nombre, ruta y hash del programa que recibió el intento de explotación. • Nombre del equipo. • Grupo. • Fecha y hora UTC. • Acción ejecutada. • Nivel de riesgo del equipo. • Valoración de la seguridad del programa atacado. • Tabla con la telemetría del contexto asociada al proceso atacante en el momento en que se detecta. • Posible origen del exploit.

Tipo	Frecuencia	Condición	Información contenida
Detecciones de PUP	Máximo 2 mensajes por equipo - PUP - día.	• Por cada PUP detectado en tiempo real en el equipo. • Solo en equipos Windows.	• Primer o segundo mensaje. • Nombre del programa malicioso. • Nombre del equipo. • Grupo. • Fecha y hora UTC. • Ruta del programa malicioso. • Hash. • Tabla con la telemetría del contexto asociada al proceso atacante en el momento en que se detecta. • Listado de equipos donde fue previamente visto el malware.
Detecciones de ataques de red	Cada 1 hora.	• Por cada tipo de ataque de red detectado e IP de origen que coincidan. • Solo en equipos Windows.	• Equipo. • Grupo. • Ataque de red. • Dirección IP local. • Dirección IP remota. • Puerto local. • Puerto remoto. • Número de ocurrencias.
Programas bloqueados en proceso de clasificación	Por cada programa desconocido detectado en el sistema de ficheros en tiempo real.	Solo en equipos Windows.	• Nombre del programa desconocido. • Nombre del equipo. • Grupo. • Fecha y hora UTC. • Ruta del programa desconocido. • Hash.

Tipo	Frecuencia	Condición	Información contenida
			• Tabla con la telemetría del contexto asociada al proceso atacante en el momento en que se detecta. • Listado de equipos donde fue previamente visto el programa desconocido.
Programas bloqueados o detectados por política avanzada de seguridad	• Si la acción es Bloquear se envía un único correo por cada equipo y día. • Si la acción no es Bloquear se envían los 50 primeros correos generados entre todos los equipos del cliente y día.	Solo en equipos Windows.	• Detalles de la detección: • Nombre de la política aplicada • Nombre del equipo • Grupo • Usuario Logeado • Nombre del fichero • MD5 del fichero. • Ruta y nombre del programa. • Fecha y hora UTC. • Ciclo de vida del elemento detectado: • Fecha y hora UTC. • Acción. • Ruta/Url/Registro/Clave • Archivo/MD5/Valor del registro • Confiable • Apariciones en otros equipos: • Nombre del equipo • Fecha de la primera vez que fue visto • Ruta y nombre del

Tipo	Frecuencia	Condición	Información contenida
			programa.
Programas bloqueados por el administrador	Por cada programa bloqueado.	Solo en equipos Windows.	• Nombre del programa • Hash • Ruta del programa • Nombre del equipo • Grupo al que pertenece el equipo • Usuario que lanzó el programa • Fecha del bloqueo
Clasificaciones de archivos que han sido permitidos por el administrador	Los archivos permitidos por el administrador son aquellos que han sido bloqueados por ser desconocidos para Advanced EDR o por haber sido clasificados como amenazas, pero el administrador permite su ejecución. El sistema genera un correo de alerta cada vez que una clasificación se completa, ya que es posible que la acción emprendida por el sistema puede cambiar después de la clasificación, según se indica en la política de reclasificación configurada por el administrador. Consulta Política de reclasificación en la página 732 para obtener más información sobre las políticas de reclasificación.		
Indicadores de ataque (IOA)	Cada vez que se detecte el hecho relevante	Por cada equipo de la red con la configuración Indicadores de ataque (IOA) asignada	• Equipo afectado • Dirección IP • Grupo • Cliente • Tipo de indicador de ataque • Riesgo • Acción
Equipos con error en la protección	Cada vez que se detecte el hecho relevante	• Por cada equipo desprotegido de la red. • Equipos con la protección en estado de error o	• Nombre del equipo. • Grupo. • Descripción. • Sistema operativo. • Dirección IP.

Tipo	Frecuencia	Condición	Información contenida
		fallo en la instalación de la protección	- Ruta del directorio activo. - Dominio. - Fecha y hora UTC. Motivo de la desprotección: Protección con error o Error instalando.
Equipos sin licencia	Cada vez que se detecte el hecho relevante	Por cada equipo que intenta licenciarse, pero no lo consigue por falta de licencias libres.	- Nombre del equipo. - Descripción. - Sistema operativo - Dirección IP - Grupo - Ruta del directorio activo - Dominio. - Fecha y hora UTC. - Motivo de la desprotección: equipo sin licencia.
Errores durante la instalación	Cada vez que se detecte el hecho relevante	- Por cada uno de los equipos de la red, cada vez que se crea una nueva situación que derive en el cambio de estado (1) de protegido a desprotegido. - Si en un mismo momento se detectan varios motivos que derivan en el cambio de estado en un mismo equipo, solo se	- Nombre del equipo. - Estado de la protección. - Razón del cambio del estado de la protección.

Tipo	Frecuencia	Condición	Información contenida
		genera una alerta con todos los motivos.	
Equipos no administrados descubiertos	Cada vez que se detecte el hecho relevante	• Cada vez que un equipo descubridor termina un descubrimiento. • El descubrimiento ha encontrado equipos no vistos anteriormente en la red.	• Nombre del equipo descubridor. • Número de equipos descubiertos. • Enlace al listado de los equipos descubiertos en la consola.

Tabla 24.2: Tabla de alertas

Cambios de estado (1)

Las razones de cambio de estado que generan una alerta son:

- **Protección con error:** sólo se contempla el estado de la protección avanzada.
- **Error instalando:** se enviará alerta cuando se haya producido un error en la instalación que requiera de la intervención del usuario (e.g., no hay espacio en disco), y no ante errores transitorios que podrían solucionarse autónomamente tras varios reintentos.
- **Sin licencia:** cuando el equipo no ha recibido una licencia tras registrarse, por no haber libres en ese momento.

Las razones de cambio de estado que no generan una alerta son:

- **Sin licencia:** cuando el administrador ha quitado la licencia al dispositivo o cuando Advanced EDR haya retirado la licencia automáticamente al equipo por haberse reducido el número de licencias contratadas.
- **Instalando:** por no resultar útil recibir una alerta cada vez que se instala un equipo.
- **Protección desactivada:** este estado es consecuencia de un cambio de configuración voluntario.
- **Protección desactualizada:** no implica necesariamente que el equipo este desprotegido, pese a estar desactualizado.
- **Pendiente de reinicio:** no implica necesariamente que el equipo este desprotegido.
- **Desactualizado el conocimiento:** no implica necesariamente que el equipo este desprotegido.

Dejar de recibir alertas por correo

Si el destinatario de las alertas por correo quiere dejar de recibirlas pero no tiene acceso a la consola de Advanced EDR o no tiene permisos suficientes para modificar la configuración, puede darse de baja del servicio si sigue los pasos mostrados a continuación:

- Haz clic en el enlace del pie de mensaje **“Si no deseas recibir más mensajes de este tipo, pincha aquí.”**. Se mostrará una ventana pidiendo la dirección de correo del usuario. El enlace tiene una caducidad de 15 días.
- Si se ha introducido una dirección de correo que pertenece a alguna configuración de Advanced EDR se envía un correo al usuario para confirmar la baja de notificaciones para esa cuenta.
- Haz clic en el enlace del nuevo correo para retirar la cuenta de correo de todas la configuraciones en las que aparezca. El enlace tiene una caducidad de 24 horas.

Capítulo 25

Envío programado de informes y listados

Advanced EDR envía por correo electrónico toda la información de seguridad que se produce en los equipos que protege. Este método de entrega facilita la compartición de información entre los distintos departamentos de la empresa, así como permite guardar un histórico de todos los eventos producidos por la plataforma, más allá de los límites de capacidad de la consola Web. De esta forma, es posible realizar un seguimiento completo del estado de la seguridad sin necesidad de que el administrador tenga que acudir a la consola web, ahorrando tiempo de gestión.

El envío automático de informes por correo electrónico permite entregar a las personas interesadas toda la información de los eventos de seguridad generados, sin dejar espacio a manipulaciones para poder evaluar de forma precisa el estado de la seguridad de la red.

Contenido del capítulo

Características de los informes	785
Tipos de informes	786
Requisitos para generar informes	787
Acceso al envío de informes y listados	787
Gestión de informes	788
Configuración de los informes y listados	789
Contenido de los informes y listados	792

Características de los informes

Según el intervalo de tiempo abarcado

Dependiendo del momento en el que se produce la información incluida en el informe se distinguen dos tipos:

- **Informes consolidados:** reúnen en un solo documento toda la información generada en un intervalo de fechas.
- **Informes instantáneos:** contienen información que refleja el estado de la seguridad de la red en un momento concreto.

Según la forma de envío

Advanced EDR genera y envía informes de forma automática según la configuración establecida en el programador de tareas o de forma manual bajo demanda.

Con el envío de informes automáticos, los destinatarios obtendrán de forma automática y sin necesidad de acudir a la consola Web la información producida en el parque de equipos gestionado.

Según el formato de salida

Dependiendo del tipo de informe Advanced EDR entrega informes en formato pdf y /o csv.

Según su contenido

Dependiendo del tipo de informe su contenido será configurable, permitiendo abarcar más o menos módulos soportados por Advanced EDR o estableciendo filtros para limitar la información a equipos que cumplan con determinadas características.

Tipos de informes

Advanced EDR permite generar 3 tipos de documentos, cada uno de ellos con sus características asociadas:

- Vistas de listados
- Informes ejecutivos
- Listados de dispositivos

A continuación se resumen las características de cada tipo de informe:

Tipo	Intervalo	Envío	Contenido	Salida
Vistas de listados	Instantáneo	Automático	Configurable mediante búsquedas	csv
Informes ejecutivos	Consolidado	Automático y bajo demanda	Configurable por categorías y por grupos	pdf, csv, excel, word
Listados de dispositivos	Instantáneo	Automático	Configurable mediante filtros	csv

Tabla 25.1: Resumen de tipos de informes y sus características

Requisitos para generar informes



Los usuarios con el rol de solo lectura podrán previsualizar los informes ejecutivos pero no podrán programar el envío de nuevos informes.

A continuación se detallan las tareas previas que el administrador deberá realizar antes de poder utilizar la funcionalidad de envío de informes y listados programados.

Vistas de listados

El administrador deberá de crear previamente una vista y configurar las herramientas de búsqueda hasta que el listado muestre la información que considere relevante. Una vez hecho esto podrá crear un informe programado. Consulta [Crear un listado personalizado](#) en la página **54** para obtener información de cómo crear vistas de listados con búsquedas asociadas.

Informes ejecutivos

No es necesaria la ejecución de ninguna tarea previa: su contenido se determina en el momento de configurar el informe programado.

Listado de dispositivos filtrado

El administrador deberá crear un filtro o utilizar uno de los filtros ya creados en Advanced EDR. Consulta [Árbol de filtros](#) en la página **180** para obtener más información acerca del manejo y configuración de los filtros.

Acceso al envío de informes y listados

Desde la sección Informes programados

Para acceder al listado de tareas que envían informes y listados haz clic en el menú superior **Estado**, panel lateral **Informes programados**. Se mostrará una pantalla con las herramientas necesarias para buscar tareas de envío ya creadas, editarlas, borrarlas o crear nuevas.

Desde una vista de listado

Las vistas de listados se almacenan en el panel lateral izquierda del menú superior **Estado**, y cada una de ellas puede enviarse de forma programada siguiendo los pasos mostrados a continuación:

- **Desde el menú de contexto:** haz clic en el menú de contexto de la vista de listado y en la opción **Programar informe** . Se mostrará la ventana de información requerida explicada en [Configuración de los informes y listados](#).
- **Desde la propia vista del listado:** haz clic en el icono  situado en la esquina superior derecha de

la ventana. Se mostrará la ventana de información requerida explicada en [Configuración de los informes y listados](#).

Al completarse la creación del informe programado se mostrará un mensaje emergente en la esquina superior derecha de la pantalla indicado la generación de una nueva tarea de envío.

Desde un filtro

- En el menú superior **Equipos** haz clic en la pestaña  para mostrar el árbol de filtros.
- Al hacer clic en un filtro, el listado de dispositivos se actualizará para mostrar los dispositivos cuyos atributos satisfagan las condiciones impuestas por el filtro seleccionado.
- Haz clic en el icono del menú de contexto : asociado al filtro y selecciona la opción **Programar Informe**. Se mostrará la ventana de información requerida explicada en [Configuración de los informes y listados](#).

Al completarse la creación del informe programado se mostrará un mensaje emergente en la esquina superior o inferior derecha de la pantalla indicado la generación de una nueva tarea de envío y un enlace para ver el listado de informes programados. Consulta [Configuración de los informes y listados](#).

Gestión de informes

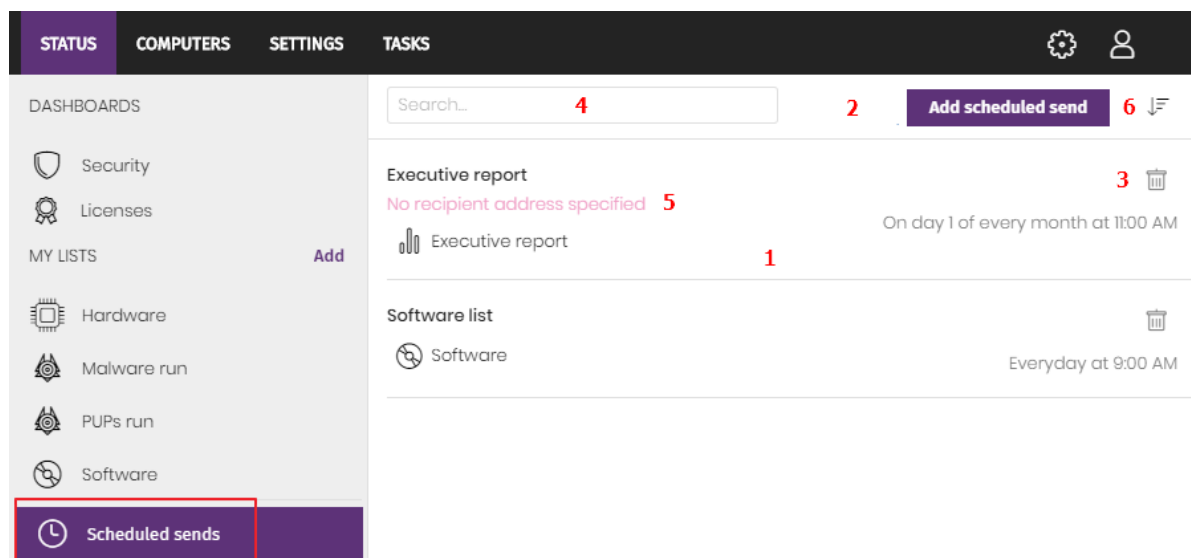


Figura 25.1: Ventana para gestionar los informes programados

Para crear, borrar, editar y listar informes programados haz clic en el menú superior **Estado** y en el menú lateral **Informes programados**.

Listado de Informes programados

En el panel de la derecha se muestran los informes programados ya creados).

Todas las tareas de envío incluye un nombre y debajo una serie de mensajes que indican si faltan datos por indicar en la configuración del informe programado (5).

Crear Informes programados

Haz clic sobre el botón **Añadir Informe programado (2)** para mostrar la ventana de configuración.

Consulta [Configuración de los informes y listados](#) para obtener información sobre los datos que el administrador debe aportar al crear un informe programado.

Ordenar Informes programados

Haz clic en el icono  (6) para desplegar un menú de contexto con las opciones de ordenación disponibles:

- Ordenado por fecha de creación
- Ordenado por nombre
- Ascendente
- Descendente

Borrar y editar Informes programados

Para borrar y editar un informe programado sigue los pasos mostrados a continuación:

- Para borrar un informe programado utiliza el icono  (3).
- Haz clic en el nombre del informe programado para editarlo.



Una vista de listado o listado filtrado que tenga configurado un informe programado no podrá borrarse hasta que el informe programado sea eliminado.

Los listados enviados por un informe programado se corresponden a una vista de listado o a un listado filtrado concretos. Si éstos son modificados, el informe programado se actualizará con la nueva configuración.

Configuración de los informes y listados

Campo	Descripción
Nombre	Nombre de la entrada que se mostrará en el listado de informes programados.
Enviar automáticamente	Frecuencia de envío del informe o listado:

Campo	Descripción
	• Todos los días: el envío se producirá todos los días a la hora seleccionada. • Todas la semanas: el envío se producirá todos las semanas a la hora y día de la semana seleccionados. • Todos los meses: el envío se producirá todos los meses en el día del mes y hora seleccionados.
Tipo de informe	Tipo de informe que se enviará: • Informe ejecutivo • Listado • Filtro El contenido del informe varía según su tipo. Para más información, consulta Contenido de los informes y listados.
Previsualizar informe	Este enlace solo se muestra cuando el tipo de informe elegido es Informe ejecutivo. Al hacer clic, se abrirá una nueva pestaña en el navegador con el contenido del informe para previsualizarlo. De esta manera es posible configurar el informe, descargarlo o imprimirlo mediante la barra de herramientas superior. Para los listados y filtros el formato elegido es csv, por lo que la opción de previsualizar no está disponible.
Fechas	Intervalo de tiempo que abarca el informe. Esta configuración de fechas solo está disponible para los informes ejecutivos. • Último mes • Últimos 7 días • Últimas 24 horas En el caso de los listados y filtros el informe obtenido es de tipo instantáneo, por lo que la información que muestra es la correspondiente al estado de la seguridad en el momento en que se genera el informe. Para más información, consulta Características de los informes.
Equipos	De qué equipos se extraen datos para generar el informe ejecutivo: • Todos los equipos. • Los grupos seleccionados: muestra el árbol de grupos para seleccionar

Campo	Descripción
	de forma individual los grupos mediante las casillas de selección. Este campo solo está disponible cuando el tipo de informe es Informe ejecutivo.
Para	Direcciones de correo separadas por comas que recibirán el informe.
CC	Direcciones de correo en copia separadas por comas que recibirán el informe.
CCO	Direcciones de correo en copia oculta separadas por comas que recibirán el informe.
Asunto	Frase resumen que describe el correo.
Formato	• Para vistas de listado: adjunta un fichero en formato csv al correo. • Para informes ejecutivos: adjunta al correo electrónico el informe en formato .PDF, Excel o Word.
Idioma	Idioma en el que se envía el informe.
Contenido	Tipo de información que incluye el informe: • Tabla de contenidos: índice de los distintos apartados dentro del informe. • Estado de licencias: muestra la información de las licencias contratadas, consumidas y su fecha de caducidad. Consulta Licencias en la página 157 para más información. • Estado de seguridad: funcionamiento del software Advanced EDR en los equipos de la red donde ha sido instalado. • Detecciones: muestra las amenazas detectadas en la red. • Riesgos: muestra el estado global del riesgo de seguridad asignado a los equipos. Consulta Paneles/widgets del módulo Evaluación de riesgos en la página 659 • Indicadores de ataque: información sobre los IOAs detectados. Consulta Paneles / widgets del módulo Indicadores de ataque en la página 592. • Gestión de parches: muestra el estado del parcheo de los equipos. Consulta Paneles/widgets en Cytomic Patch en la página 398 para más información.

Campo	Descripción
	• Estado de la evaluación de vulnerabilidades: muestra los equipos de la red que contienen software con vulnerabilidades conocidas, e informa sobre la disponibilidad de parches para evitar su impacto en los equipos. Visible solo si el cliente no tiene contratado Cytomic Patch Para más información, consulta Paneles/widgets de Evaluación de vulnerabilidades en la página 671 • Data Control: información sobre el estado del despliegue de Cytomic Data Watch y los equipos con mayor cantidad de ficheros PII detectados en la red. Consulta Paneles / widgets del módulo Cytomic Data Watch en la página 337. • Cifrado: muestra el estado del cifrado en los equipos de la red. Consulta Paneles / widgets del módulo Cytomic Encryption en la página 499 para más información. • Control de Acceso a Endpoints: muestra las conexiones entrantes detectadas y bloqueadas en los equipos de la red corporativa. Para más información, consulta Paneles/widgets de Control de Acceso a Endpoints en la página 466. Consulta Contenido de los informes y listados.

Tabla 25.2: Información para generar informes bajo demanda

Contenido de los informes y listados

Listados

El contenido de los listados enviados equivale a la opción **Exportar** o **Exportación detallada** de una vista de listado. Si la vista de listado soporta exportación detallada, al configurar el envío se muestran dos opciones:

- **Informe resumido:** se corresponde con la opción **Exportar** del listado.
- **Informe completo:** se corresponde con la opción **Exportación detallada** del listado.

Los listados que admiten exportación detallada son:

- Inventario de Software
- Malware y PUPs
- Exploits

- Programas actualmente bloqueados en clasificación
- Bloqueos por políticas avanzadas de seguridad
- Historial de instalaciones de parches

Consulta [Gestión de listados](#) en la página [47](#) para obtener información sobre los tipos de listados disponibles en Advanced EDR y su contenido.



El listado incluirá información de los equipos visibles por la cuenta de usuario que modificó por última vez el informe programado. Por esta razón, un listado modificado por una cuenta con menor visibilidad que la cuenta que lo creó inicialmente contendrá información de un número de equipos menor que la que mostró en el momento de su creación.

Listados de dispositivos

El contenido del informe enviado se corresponde con la exportación simple del listado de dispositivos filtrados por un criterio. Consulta [Equipos](#) en la página [195](#) para obtener información sobre el contenido del fichero csv enviado y [Árbol de filtros](#) en la página [180](#) para obtener información acerca del manejo y configuración de los filtros.

Informe ejecutivo

Dependiendo de la configuración establecida en el campo **Contenido**, el informe ejecutivo contendrá los datos mostrados a continuación:

Información general

- **Creado el:** fecha de generación del informe.
- **Periodo:** intervalo de tiempo que abarca el informe.
- **Información incluida:** equipos de la red incluidos en el informe.

Tabla de contenidos

Índice con enlaces a las distintas secciones incluidas en el informe ejecutivo.

Estado de las licencias

- **Licencias contratadas:** número de licencias adquiridas por el cliente.
- **Licencias consumidas:** número de licencias asignadas a los equipos de la red.
- **Fecha de caducidad:** fecha en la que caduca el mantenimiento.

Consulta [Licencias](#) en la página [157](#).

Estado de seguridad

Funcionamiento del módulo de protección en los equipos de la red donde ha sido instalado.

- **Estado de protección:** consulta [Estado de protección](#) en la página 608.
- **Equipos conectados:** consulta [Equipos sin conexión](#) en la página 611.
- **Protecciones actualizado:** consulta [Protección desactualizada](#) en la página 612.
- **Conocimiento actualizado:** consulta [Protección desactualizada](#) en la página 612.

Detecciones

Amenazas detectadas en la red.

Riesgos

Estado global del riesgo de seguridad asignado a los equipos. Consulta [Paneles/widgets del módulo Evaluación de riesgos](#) en la página 659

- **Riesgo de la compañía:** número de equipos que se encuentran en alguno de los niveles de riesgo establecidos.
- **Evolución del riesgo:** evolución del número de equipos que se encuentran en algún nivel de riesgo a lo largo de un periodo de tiempo determinado.
- **Riesgos detectados:** lista de los riesgos que más veces se han detectado en los equipos.
- **Equipos en riesgo (Top 10):** lista de los 10 equipos con el nivel de riesgo global más elevado.

Indicadores de ataque

Detalle de los IOAs detectados.

- **Servicio threat hunting:** consulta [Servicio Threat Hunting](#) en la página 593.
- **Evolución de las detecciones:** consulta [Evolución de las detecciones](#) en la página 594.
- **Indicadores de ataque (IOA) detectados (top 10):** consulta [Indicadores de ataque \(IOA\)](#) en la página 569.
- **Indicadores de ataque (IOA) por equipo (top 10):** consulta [Indicadores de ataque \(IOA\)](#) en la página 569.

Gestión de parches

Estado del parcheo de los equipos.

- **Estado de gestión de parches:** consulta [Estado de gestión de parches](#) en la página 399.
- **Equipos con más parches disponibles (top 10):** listado de los 10 equipos de la red que tiene más parches disponibles sin instalar agrupados por su tipo: parches de seguridad, parches no de seguridad y Service Packs. Consulta [Equipos con más parches disponibles](#) en la página 412.

- **Parches más críticos (top 10):** listado de los 10 parches más críticos ordenado por el número de equipos afectados.
- **Evolución de los parches disponibles:** muestra la evolución de los parches pendientes de instalar en los equipos de la red según su criticidad. Consulta [Evolución de los parches disponibles](#) en la página [404](#).

Evaluación de vulnerabilidades

- **Estado de la evaluación de vulnerabilidades:** muestra los equipos donde la evaluación de vulnerabilidades está funcionando correctamente y aquellos con errores o problemas en la instalación o en la ejecución del módulo. Consulta [Estado de la evaluación de vulnerabilidades](#) en la página [671](#).

Tiempo desde la última comprobación: muestra los equipos de la red que no han conectado con la nube de Cytomic en un determinado periodo de tiempo para comprobar su estado de parcheo. Consulta [Tiempo desde la última comprobación](#) en la página [674](#).

- **Parches más críticos (top 10):** listado de los 10 parches más críticos ordenado por el número de equipos afectados.
- **Programas con más parches disponibles (top 10)** listado de los 10 programas con más parches disponibles para su instalación.
- **Evolución de los parches disponibles:** muestra la evolución de los parches pendientes de instalar en los equipos de la red según su criticidad. Consulta [Evolución de los parches disponibles](#) en la página [678](#).

Cytomic Data Watch

Estado del despliegue de Cytomic Data Watch y los equipos con mayor cantidad de ficheros PII detectados en la red.

- **Estado del despliegue:** consulta [Estado del despliegue](#) en la página [338](#).
- **Archivos por tipo de información personal:** [Archivos por tipo de información personal](#) en la página [348](#).
- **Equipos por información personal:** [Equipos con información personal](#) en la página [347](#).
- **Equipos con más archivos con información personal (top 10):** [Equipos con información personal](#) en la página [347](#).

Cifrado

Estado del cifrado de los equipos. Incluye los widgets y listados mostrados a continuación:

- **Estado del cifrado:** consulta [Estado del cifrado](#) en la página [499](#).
- **Equipos compatibles con cifrado:** consulta [Equipos compatibles con cifrado](#) en la página [501](#).
- **Equipos cifrados:** consulta [Equipos cifrados](#) en la página [502](#).

- **Método de autenticación aplicado:** consulta [Métodos de autenticación aplicados](#) en la página [504](#).
- **Últimos equipos cifrados:** listado de los 10 equipos que han sido cifrados recientemente por Cytomic Encryption, ordenados por 'Fecha de cifrado'. Cada línea del listado contiene el nombre del equipo, grupo al que pertenece, sistema operativo instalado, método de autenticación configurado y fecha de cifrado.

Control de Acceso a Endpoints

Conexiones detectadas en los equipos de la red corporativa. Incluye los widgets y listados mostrados a continuación:

- **Conexiones por condición:** evolución de las conexiones en función de la razón por la cual se las categorizó como peligrosas. Para más información, consulta [Conexiones por condición](#) en la página [469](#)
- **Conexiones por protocolo monitorizado:** conexiones detectadas transportadas por los protocolos monitorizados a lo largo del tiempo. Para más información, consulta [Conexiones por protocolo monitorizado](#) en la página [471](#)
- **Equipos con conexiones salientes de alto riesgo (top 10):** las diez direcciones IP o nombres de los equipos que envían más conexiones de alto riesgo a los equipos de la red. Para más información, consulta [Equipos con conexiones salientes de alto riesgo \(top 5\)](#) en la página [467](#)
- **Equipos con conexiones entrantes de alto riesgo (top 10):** los nombres de los diez equipos de la red que reciben más conexiones entrantes de alto riesgo procedentes de equipos administrados. Para más información, consulta [Equipos con conexiones entrantes de alto riesgo \(top 5\)](#) en la página [468](#)

Capítulo 26

Herramientas de resolución

Advanced EDR cuenta con varias herramientas de resolución que permiten al administrador solucionar los problemas encontrados en las fases de Protección, Detección y Monitorización del ciclo de protección adaptativa.

Contenido del capítulo

Análisis y desinfección automática de equipos	798
Análisis y desinfección bajo demanda de equipos	799
Reiniciar equipos	803
Aislar un equipo	804
Control remoto de los equipos	807
Notificar un problema	821
Permitir el acceso externo a la consola Web	822
Eliminar el ransomware y recuperar el estado anterior	822

Herramientas de resolución disponibles en Advanced EDR muestra las herramientas disponibles por plataforma y sus características.

Herramienta de resolución	Tipo	Acción
Análisis y desinfección automática de equipos	Automático	Detecta y desinfecta el malware cuando se registra un movimiento en el sistema de ficheros (copia, movimiento, ejecución) o en un vector de infección soportado.
Análisis y	Automático	Detecta y desinfecta el malware en el sistema de ficheros

Herramienta de resolución	Tipo	Acción
desinfección bajo demanda de equipos	(Programado) / Manual	cuando lo requiera el administrador: en franjas horarias concretas o cuando cree la tarea de resolución.
Reinicio bajo demanda	Manual	Fuerza un reinicio del equipo para aplicar actualizaciones, completar desinfecciones manuales y corregir errores detectados en la protección.
Aislamiento de equipos	Manual	Aísla el equipo de la red, impidiendo la extracción de información confidencial y la propagación de la amenaza a los equipos vecinos.
Control remoto de los equipos	Manual	Permite al administrador establecer desde la consola web una conexión remota con los equipos de la red, para comprobar su estado o para iniciar tareas de resolución de problemas.
Eliminar el ransomware y recuperar el estado anterior	Manual	Permite detectar ataques de tipo ransomware y eliminar las amenazas. En el caso de Windows, es posible restaurar los archivos cifrados a su situación previa al ataque.

Tabla 26.1: Herramientas de resolución disponibles en Advanced EDR

Análisis y desinfección automática de equipos

El módulo de protección avanzada de Advanced EDR detecta y desinfecta de forma automática las amenazas analizadas cuando se ejecuta el software instalado en el equipo.



*La desinfección automática no requiere de la intervención del administrador, si bien es necesario que esté seleccionada la casilla **Protección de archivos** en la configuración de seguridad asignada al equipo. Consulta [Configuración de la seguridad en estaciones y servidores](#) en la página 291 para más información sobre las configuraciones disponibles en el módulo antivirus de Advanced EDR.*

Ante la detección de una amenaza conocida, Advanced EDR desinfecta de forma automática los elementos afectados siempre y cuando exista un método de desinfección conocido. En su defecto, el elemento se moverá a cuarentena.

Análisis y desinfección bajo demanda de equipos

Para analizar y desinfectar los equipos de usuario bajo demanda, Advanced EDR utiliza la infraestructura de tareas.

Permisos necesarios

La cuenta de usuario utilizada para acceder a la consola web tiene que tener asignado el permiso **Lanzar análisis y desinfectar** a su rol. Para obtener más información sobre el sistema de permisos consulta [Gestión de roles y permisos](#) en la página 67.

Tipos de tareas de análisis bajo demanda

Inmediatas (opción Desinfectar)

Tarea de inicio inmediato que analiza y desinfecta el sistema de ficheros local (no analiza las unidades de red).

Advanced EDR crea una tarea con las características siguientes:

- **Tiempo de ejecución máxima de la tarea:** sin límite.
- **Inicio de la tarea:**
 - Si el equipo esta encendido, la tarea se inicia en el momento de su lanzamiento.
 - Si el equipo está apagado, la tarea retrasa su ejecución hasta los siguientes 7 días.
- Los elementos del equipo analizado en busca de malware son los siguientes:
 - Memoria.
 - Dispositivos de almacenamiento interno. Sistema de ficheros completo, todas las extensiones.
 - Dispositivos de almacenamiento conectados físicamente al equipo (discos USB y otros). Sistema de ficheros completo, todas las extensiones.
- La acción predeterminada del proceso de análisis es:
 - **Para ficheros desinfectables:** se reemplazan los ficheros desinfectados por una versión desinfectada.
 - **Para ficheros no desinfectables:** se eliminan y se realiza una copia de seguridad en la cuarentena.

Acceso a las tareas de desinfección bajo demanda

Desde el Árbol de equipos

- Selecciona el menú superior **Equipos** y haz clic en la pestaña **Carpetas** del árbol de equipos situado en el panel izquierdo.
- Para lanzar una tarea de desinfección inmediata sobre un grupo de equipos haz clic en el menú de contexto del grupo y selecciona **Desinfectar** . Se mostrará el mensaje **Nueva tarea de desinfección creada** y la tarea se añadirá a la lista de tareas en la sección **Tareas**.

Desde el listado del árbol de equipos

- Selecciona el menú superior **Equipos** y haz clic en la pestaña **Carpetas** del árbol de equipos situado en el panel izquierdo.
- Selecciona el grupo de equipos y haz clic en las casillas de selección del listado de equipos.
- Para lanzar una tarea de desinfección inmediata, si has seleccionado un solo equipo haz clic en el menú de contexto asociado al equipo y selecciona **Desinfectar** . Si has seleccionado varios, haz clic en **Desinfectar**  en la barra superior de herramientas. Se mostrará el mensaje **Nueva tarea de desinfección creada** y la tarea se añadirá a la lista de tareas en la sección **Tareas**.

Listados generados por tareas de análisis

Las tareas de análisis generan listados con los resultados.

Acceso a los listados

Para acceder a estos listados sigue los pasos a continuación:

- Desde el menú superior **Tareas**, haz clic en la **Ver resultados** en la tarea de análisis para acceder al listado **Resultados de tarea**.
- En el listado de **Resultados de Tarea**, selecciona **Ver Detecciones** para acceder al listado.

Permisos requeridos

Permisos	Acceso a listados
Sin permisos	Listado Resultados de la tarea de análisis .
Ver detecciones y amenazas	Acceso a los listados Ver Detecciones dentro de la tarea.

Tabla 26.2: Permisos requeridos para los listados de tareas de análisis

Listado Resultados tarea de análisis

Este listado muestra las detecciones de malware realizada sobre los equipos de la red:

Campo	Descripción	Valores
Equipo	Nombre del equipo analizado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Detecciones	Número de elementos encontrados en el equipo.	Cadena de caracteres
Estado	Estado de la tarea de análisis en el equipo.	• Todos los estados • Pendiente • En curso • Finalizado • Con error • Cancelada (no pudo iniciar a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)
Fecha de comienzo	Fecha en la que comenzó el análisis del equipo.	Fecha
Fecha de fin	Fecha en la que finalizó el análisis del equipo.	Fecha

Tabla 26.3: Campos del listado de Resultado de tarea de análisis

Herramientas de filtrado

Campo	Comentario	Valores
Estado	Según el estado de la tarea	• Todos los estados • Pendiente • En curso

Campo	Comentario	Valores
		- Finalizado - Con error - Cancelada (no pudo iniciar a la hora programada) - Cancelada - Cancelando - Cancelada (tiempo máximo superado)
Detecciones	Equipos con detecciones de malware o sin ellas	- Todos - Con detecciones - Sin detecciones

Tabla 26.4: Filtros Resultado de tareas de análisis

Listado Ver detecciones

Este listado muestra el detalle de cada una de las detecciones de malware encontradas por la tarea de análisis.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Tipo de amenaza	Función del archivo detectado.	- Virus y ransomware - Spyware - Tracking Cookies - Herramientas de hacking y PUPs - Pishing - Acciones peligrosas

Campo	Descripción	Valores
		bloqueadas • URLs con malware • Otros
Ruta	Ubicación de la amenaza en los equipos.	Cadena de caracteres
Acción	Acción realizada en el equipo.	• Borrado • Desinfectado • En cuarentena • Bloqueado • Proceso terminado
Fecha	Fecha en la que se realizó la acción.	Fecha

Tabla 26.5: Campos del listado Ver detecciones

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Para obtener más información, consulta [Información de equipo](#) en la página 218.

Reiniciar equipos

Para mantener los equipos actualizados a la última versión de la protección, o si se detecta algún error en la protección, el administrador puede reiniciar los equipos involucrados desde la consola web:

- Selecciona el menú superior **Equipos** y localiza el equipo desde el panel de equipos situado a la derecha.
 - **Para reiniciar un único equipo:** selecciona el menú de contexto del equipo en el listado de equipos.
 - **Para reiniciar varios equipos:** mediante las casillas de selección, marca los equipos que quieres reiniciar y haz clic en el icono  de la barra de acciones.



Para los equipos que estén apagados Advanced EDR guardará la orden de reinicio hasta 7 días, momento en el cual si el equipo no se ha iniciado se desechará.

Aislar un equipo

Advanced EDR aísla bajo demanda los equipos de la red para evitar la propagación de las amenazas y la comunicación y extracción de información confidencial.



Esta función es compatible con estaciones y servidores Windows, macOS y Linux. No es compatible con dispositivos Android.

Cuando un equipo está aislado, sus comunicaciones quedan restringidas a los servicios mostrados a continuación:

- El acceso al equipo desde la consola para que el administrador pueda analizar el problema y resolverlo mediante las herramientas suministradas por Advanced EDR.
- El acceso a los dispositivos y su control remoto mediante Panda Systems Management para que el administrador pueda recoger información extendida y resolver los problemas mediante las herramientas de gestión remota (escritorio remoto, línea de comandos remota, visor de sucesos remoto etc.).



Para obtener un listado de las herramientas de gestión remota disponibles en Cytomic consulta la Guía de administración de Panda Systems Management en <https://www.pandasecurity.com/rfiles/enterprise/documentation/pcsm/docswebpage/SYSTEMSMANAGEMENT-Manual-ES.pdf>

El resto de productos y servicios instalados en el equipo de usuario o servidor dejarán de poder comunicarse por red a no ser que el administrador establezca excepciones. Consulta [Opciones avanzadas](#).

Estados de los equipos aislados

Las operaciones **Aislar un equipo** y **Dejar de Aislar un equipo** se ejecutan en tiempo real, pero el proceso puede retrasarse si el equipo no está conectado a Internet. Para reflejar su situación exacta, Advanced EDR distingue los 4 estados a través de los iconos mostrados a continuación:

Icono	Descripción
Aislando	El administrador lanzó una petición para aislar uno o más equipos y se está procesando.
Aislado	El proceso de aislamiento se completó y el equipo tiene restringidas sus

Icono	Descripción
	comunicaciones.
Dejando de aislar 	El administrador lanzó una petición para dejar de aislar uno o más equipos y se está procesando.
No aislado	El proceso para retirar el aislamiento del equipo se completó. Las comunicaciones se permiten acorde la configuración definida en otros módulos, productos, o en el propio sistema operativo.

Tabla 26.6: Estados de los equipos aislados

Estos iconos acompañan a la columna dirección IP en los listados de **Licencias**, **Estado de la protección** y en la zona **Equipos**.

Aislar uno o varios equipos de la red de la organización

Para aislar uno o varios equipos de la red:

- Haz clic en el menú superior **Equipos** o elige uno de los siguientes listados de equipos:
 - Listado **Estado de protección**.
 - Listado **Licencias**.
- Indica los equipos a aislar con las casillas de selección.
- En la barra de acciones selecciona **Aislar un equipo**. Se mostrará una ventana con un link a **Opciones avanzadas**.
- En **Opciones avanzadas** indica los programas que se seguirán comunicando con el resto de la red a pesar del aislamiento del equipo (exclusión de aislamiento).
- Haz clic en el botón **Aceptar**. El equipo cambiará de estado a **Intentando aislar el equipo**.
- Para aislar un grupo de equipos:
 - Haz clic en el menú superior **Equipos**.
 - En el árbol de equipos haz clic en la vista de carpetas y selecciona el grupo a aislar.
 - En el menú de contexto selecciona la entrada **Aislar equipos** y haz clic en el botón **Aceptar**.
 - Para aislar todos los equipos de la red despliega el menú de contexto del nodo **Todos**.

Quitar el aislamiento de un equipo

- Sigue los pasos indicados en el punto **Aislar uno o varios equipos de la red de la organización** para más información.

- En la barra de acciones selecciona **Dejar de aislar un equipo**.
- El equipo cambiará de estado a **Intentando dejar de aislar el equipo**.

Opciones avanzadas

Permitir procesos

Al aislar un equipo, solo se permite la comunicación de los procesos correspondientes a los productos de Cytomic. El resto de procesos, incluyendo a los programas de usuario, no podrán comunicarse con los equipos de la organización.

Para excluir a ciertos programas de este comportamiento:

- Haz clic en el enlace **Opciones avanzadas** de la ventana flotante mostrada al aislar un equipo.
- En la caja de texto **Permitir los siguientes procesos** indica los programas a excluir del aislamiento.

Los programas indicados en **Permitir los siguientes procesos** podrán comunicarse con libertad con el resto de equipos de la organización o con el exterior, según indique la configuración del resto de módulos de Advanced EDR, de otros productos instalados en el equipo, o del cortafuegos del sistema operativo.

Para acelerar la configuración, la consola de administración retiene la última configuración de procesos excluidos del aislamiento introducida por el administrador. De esta manera, en la caja de texto de un equipo excluido no se mostrará su configuración específica de procesos excluidos, sino la última configuración que utilizó el administrador en cualquier otro equipo.

Mostrar mensaje personalizado (Windows)

Introduce un mensaje descriptivo para informar al usuario de que su equipo ha sido aislado de la red. El agente Advanced EDR mostrará una ventana desplegable con el contenido del mensaje. Para configurar un mensaje informativo pero sin que se le muestre al usuario haz clic en el selector **Prefiero no mostrar ningún mensaje en esta ocasión**. Hasta que no desactives el selector los mensajes no se mostrarán.



La opción de mostrar mensaje personalizado solo es compatible con estaciones y servidores Windows.

Comunicaciones permitidas y denegadas de un equipo aislado

Advanced EDR deniega todas las comunicaciones en un equipo aislado excepto las necesarias para poder realizar un análisis forense remoto, y utilizar las herramientas de resolución implantadas en Advanced EDR y en Panda Systems Management. A continuación, se indican las comunicaciones permitidas y denegadas.

Procesos y servicios permitidos en un equipo aislado

- Procesos de sistema:
 - Los servicios necesarios para formar parte de la red corporativa: obtención de IP por DHCP, ARP, nombre de equipo por WINS, DNS etc.
- Procesos de Advanced EDR:
 - Comunicación con el Gateway por defecto.
 - Comunicación con la nube de Cytomic para el funcionamiento de los motores de protección, descarga de ficheros de firmas y administración remota mediante la consola web.
 - Descubrimiento de equipos, en equipos aislados con el rol de descubridor asignado.
 - Servidor de ficheros en un equipo aislado con el rol de caché asignado.
 - Proxy de conexiones en un equipo con el rol de proxy Cytomic asignado.
- Procesos de Panda Systems Management entre el equipo aislado y el equipo del administrador:
 - Herramientas de acceso remoto.
 - Monitorización por SNMP de dispositivos no compatibles con Panda Systems Management con el rol Nodo de conexión asignado.

Comunicaciones bloqueadas en un equipo aislado

Todas las comunicaciones que no estén incluidas en el punto anterior son denegadas, entre ellas:

- Políticas de Windows Update, actualizaciones de sistema operativo macOS y Cytomic Patch de Panda Systems Management.



El módulo Cytomic Patch sí permanece operativo en un equipo aislado.

- Comunicación con la red de scripts y módulos desarrollados por el administrador o integrados desde la ComStore de Panda Systems Management.
- Navegación web, ftp, correo y otros protocolos de Internet.
- Transferencia de ficheros por SMB entre los PCs de la red.
- Instalación remota de equipos con Advanced EDR.

Control remoto de los equipos

Advanced EDR permite al administrador establecer desde la consola web una conexión remota con los equipos de la red para comprobar su estado o para iniciar tareas de resolución de problemas.

Herramientas de acceso remoto incluidas en Advanced EDR

- **Línea de comandos remota:** shell remota con permisos de administrador que permite ejecutar operaciones sobre el sistema de ficheros y lanzar programas en el equipo.
- **Gestor de procesos:** muestra un listado con los procesos en ejecución y permite su parada, pausa o reinicio.
- **Gestor de servicios:** muestra un listado con los servicios instalados en el equipo y permite su arranque y parada.
- **Transferencia de ficheros:** envío y recepción de ficheros entre el equipo del administrador y el equipo del usuario.
- **Herramientas de línea de comandos:** conjunto de programas accesibles desde la línea de comandos remota, orientados a recoger información para profundizar en la investigación del administrador, recuperar datos para realizar análisis forense y resolver las brechas de seguridad:
 - **delete:** borra ficheros en todo el disco duro del equipo.
 - **dump:** vuelca en disco la memoria asignada a procesos.
 - **netinfo:** muestra la información de las interfaces de red.
 - **pcap:** captura paquetes de red y los vuelca al disco duro del equipo.
 - **ports:** muestra los procesos que tienen puertos abiertos en el equipo.
 - **process:** muestra los procesos cargados en memoria y sus módulos.
 - **url:** muestra un listado histórico con todas las URLs accedidas desde el navegador instalado en el equipo.

Permisos requeridos

- Para visualizar y modificar la configuración de control remoto, la cuenta de usuario debe disponer del permiso **Configurar Control Remoto**.
- Para establecer un acceso remoto a los equipos de la red, la cuenta de usuario debe disponer del permiso **Control remoto de equipos**.



Para obtener más información sobre los permisos disponibles, consulta [Descripción de los permisos implementados en la página 70](#)

Requisitos

Control remoto está disponible en equipos con sistema operativo Windows, Linux y macOS.

Para utilizar las herramientas de acceso remoto y de línea de comandos remota, es necesario que tanto el equipo del usuario como el cortafuegos perimetral de la red permitan el tráfico desde y hacia las URLs siguientes:

- dir.rc.pandasecurity.com por el puerto 443.
- eu01.rc.pandasecurity.com por los puertos 8080 y 443.
- eu02.rc.pandasecurity.com por los puertos 8080 y 443.
- eu03.rc.pandasecurity.com por los puertos 8080 y 443.
- eu04.rc.pandasecurity.com por los puertos 8080 y 443.
- eu05.rc.pandasecurity.com por los puertos 8080 y 443.
- eu06.rc.pandasecurity.com por los puertos 8080 y 443.
- ams01.rc.pandasecurity.com por los puertos 8080 y 443.
- ams02.rc.pandasecurity.com por los puertos 8080 y 443.

Configuración de control remoto

Para activar el control remoto en los equipos de la red es necesario asignar una configuración a los equipos que serán accesibles por el administrador:

- Haz clic en el menú superior **Configuración**, panel lateral **Control remoto**. Se abrirá una ventana con el listado de configuraciones de control remoto existentes.
- Haz clic en el botón **Añadir** situado en la esquina superior derecha. Se abrirá la ventana **Añadir configuración**.
- Escribe el nombre de la configuración en el campo **Nombre** y opcionalmente una descripción en el campo **Descripción**.
- Haz clic en el botón **Guardar**.
- Haz clic en el enlace **No se ha asignado a ningún equipo** y elige los equipos o grupos de la red que recibirán la configuración de control remoto.
- Establece la funcionalidad de control remoto que se activará para los equipos afectados por la configuración:
 - **Terminal**: acceso remoto a la terminal de la consola
 - **Monitor de procesos**: monitorización remota de los procesos.
 - **Monitor de servicios**: configuración remota de los servicios.
 - **Transferencia de archivos**: transferencia remota de ficheros desde o hacia el equipo del administrador.
- Haz clic en el botón **Guardar** situado en la esquina superior derecha de la ventana. La configuración

se asignará a los equipos afectados y el administrador de la red podrá establecer sesiones de control remoto con ellos.

Acceso a la funcionalidad de control remoto

Para iniciar una sesión de control remoto desde un listado, haz clic en el menú de contexto asociado al equipo y selecciona la opción  **Control remoto**. Esta opción se encuentra disponible en los listados siguientes:

- Licencias
- Hardware
- Riesgos por equipo
- Estado de protección de los equipos
- Estado de cifrado
- Estado de gestión de parches
- Estado de Data Control
- Listado de equipos



*Para obtener más información acerca de los listados disponibles en Advanced EDR consulta **Plantillas, configuraciones y vistas** en la página 48*

La funcionalidad de control remoto también se encuentra disponible en la pantalla de detalle del equipo, haciendo clic en las filas de los listados indicados.

Descripción de las herramientas de control remoto

Gestión de procesos

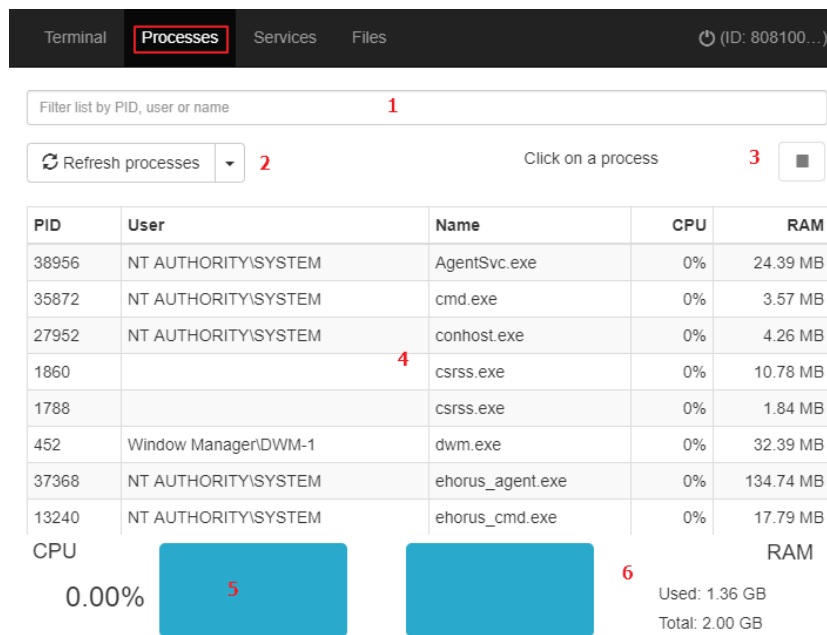


Figura 26.1: Herramienta de gestión de procesos

La herramienta de gestión de procesos muestra todos los procesos cargados en la memoria del equipo, busca procesos concretos y permite parar o arrancarlos remotamente. Además, ofrece información sobre la memoria RAM y CPU consumidas por proceso.

La funcionalidad **Gestión de procesos** incorpora los recursos siguientes:

- **Herramienta de búsqueda (1):** filtra el listado por el PID o por el nombre indicado. Permite búsquedas parciales.
- **Actualización automática del listado (2):** define el intervalo que deberá transcurrir para que Advanced EDR recargue la lista de procesos.
- **Botón de parada (3):** detiene la ejecución del programa seleccionado.
- **Listado de procesos (4):** muestra el listado de procesos cargados en la memoria del equipo.
- **CPU (5):** indica el porcentaje de CPU consumida por todos los procesos cargados en memoria, y muestra un histórico en forma de diagrama de líneas con los consumos desde que se inició la herramienta.
- **Memoria (6):** indica el porcentaje de memoria consumida por todos los procesos cargados, y muestra un histórico en forma de diagrama de líneas con los consumos desde que se inició la herramienta Gestión de procesos

El listado de procesos **(4)** muestra información de cada proceso cargado en la memoria del equipo:

Campo	Descripción
PID	Identificador del proceso.
User	Cuenta de usuario que cargó el proceso.
Name	Nombre del proceso.
CPU	CPU consumida del proceso.
RAM	Memoria consumida por el proceso.

Tabla 26.7: Campos del listado Procesos

Gestión de servicios

The screenshot displays the 'Services' management tool. At the top, there are tabs for 'Terminal', 'Processes', 'Services' (selected), and 'Files'. A user ID '(ID: 808100...)' is shown on the right. Below the tabs is a search bar labeled 'Filter' with a red '1' indicating its function. Under the search bar, there is a 'Refresh services' button with a dropdown arrow and a red '2', and a 'Click on a service' button with a red '3'. A table below lists services with columns 'Name', 'Description', and 'Status'. The 'Application Experience' service is highlighted with a red '4'.

Name	Description	Status
ActiveX Installer (AxInstSV)	Provides User Account Control and if disabled the installation of ActiveX controls will behave according	Not Running
App Readiness	Gets apps ready for use the first	Not Running
Application Experience	Processes application compatib	Not Running
Application Identity	Determines and verifies the ider	Not Running
Background Intelligent Transfer Service	Transfers files in the background programs and other information.	Running
Background	Windows infrastructure service	Running

Figura 26.2: Herramienta de gestión de servicios

La herramienta **Gestión de servicios** muestra todos los servicios configurados en el equipo, busca uno concreto y modifica su estado. Para ello cuenta con los recursos siguientes:

- **Herramienta de búsqueda (1):** filtra el listado por el nombre o descripción indicado. Permite búsquedas parciales mediante subcadenas.
- **Actualización automática del listado (2):** define el intervalo que deberá transcurrir para que Advanced EDR actualice la lista de servicios.

- **Botón de inicio y parada de servicio (3):** detiene o inicia la ejecución del servicio seleccionado.
- **Listado de servicios (4):** muestra el listado de servicios cargados en la memoria del equipo.

El listado de servicios (4) muestra información de cada servicio configurado en el equipo:

Campo	Descripción
Nombre	Identificador del servicio.
Descripción	Descripción del servicio.
Status	Estado del servicio: • Running: servicio en ejecución. • Not running: servicio detenido.

Tabla 26.8: Campos del listado Servicios

Transferencia de ficheros

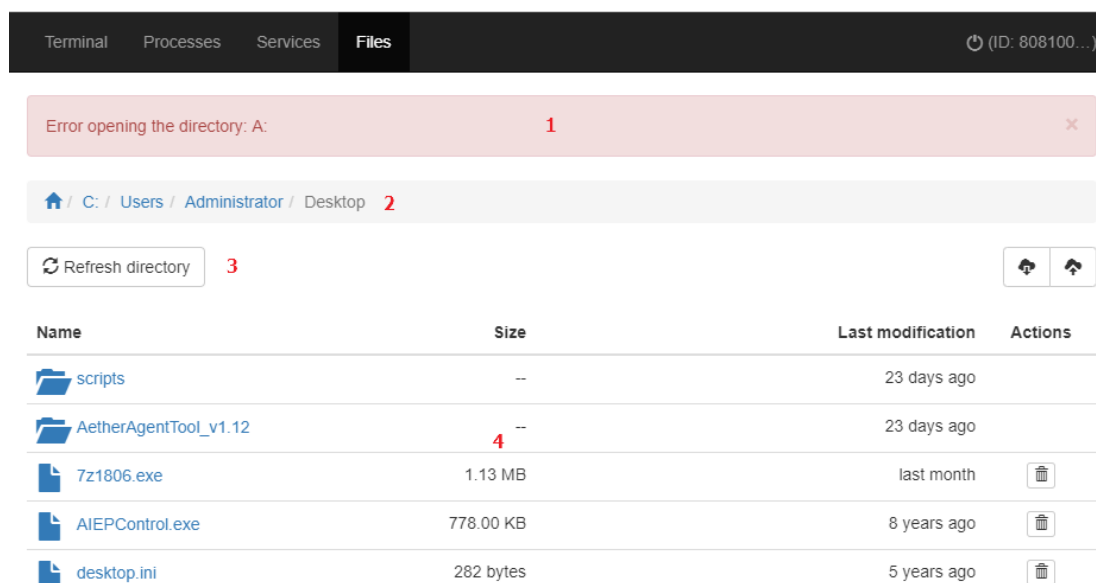


Figura 26.3: Herramienta de gestión de ficheros

La herramienta **Gestión de ficheros** permite transferir ficheros en ambas direcciones desde el equipo del administrador al equipo remoto. Además, permite navegar por el sistema de ficheros del equipo remoto y borrar archivos. Para ello cuenta con los recursos siguientes:

- **Zona de mensajes (1):** muestra los errores que se pueden producir al acceder al sistema de ficheros del equipo remoto.
- **Ruta de navegación (2):** muestra la ruta del sistema de ficheros que se visualiza en la zona de listado.

- Para cambiar de directorio de forma rápida, haz clic en una carpeta.
- Para mostrar el listado de dispositivos conectados al equipo, haz clic en el icono .
- **Actualización automática del listado (3):** permite definir el intervalo que deberá transcurrir para que Advanced EDR actualice la lista de ficheros.
- **Listado de ficheros (4):** muestra el listado de ficheros que contiene la ruta de navegación (2).
- **Carpetas**  : haz clic en una carpeta para mostrar los ficheros que contiene. Se actualizará la ruta de navegación (2) automáticamente.
- **Borrar**  : borra el fichero seleccionado. Los ficheros no pasan por la papelera de reciclaje.

El listado de ficheros (4) muestra la información relativa de cada fichero configurado en el equipo:

Campo	Descripción
Name	Nombre del fichero.
Size	Tamaño del fichero.
Last modification	Fecha en la que se modificó por última vez el fichero.
Actions	Acciones a ejecutar sobre el fichero: •  Borra el fichero

Tabla 26.9: Campos del listado Ficheros

Línea de comandos remota

Windows

Ejecuta en el equipo remoto comandos compatibles con el intérprete de comandos, y permite lanzar programas que tengan salida de texto. Se ejecuta bajo la cuenta LOCAL_SYSTEM del equipo remoto y se encuentra instalada en la siguiente ruta:

```
C:\Program Files (x86)\Panda Security\Panda Aether
Agent\Remote access\
```

Linux/macOS

Abre una shell de tipo bash y permite lanzar comandos compatibles y que tengan salida de texto. Se ejecuta con permisos de root en el equipo remoto.

Programa `rt.exe` para Windows

Advanced EDR incorpora el programa `rt.exe` para dar acceso a un conjunto de utilidades que facilitan la respuesta del administrador ante incidentes de seguridad. Con estas herramientas es posible recuperar información para realizar un análisis forense posterior, así como devolver al estado original el equipo afectado por la brecha de seguridad.

El programa `rt.exe` es accesible desde la línea de comandos remota y sigue la sintaxis indicada:

```
rt.exe [command] [-h|--help]
```

Las consideraciones indicadas a continuación afectan de forma general al comando `rt.exe`:

- `command` indica una acción a realizar. Cada una de ellas soporta distintos parámetros.
- No se soportan los caracteres comodín `"**"`, `"?"`.
- Algunos parámetros permiten búsquedas parciales por subcadenas al comienzo, final y en el interior de la cadena. Por ejemplo, para filtrar la cadena "armario" se admiten las búsquedas por "ar", "mar" e "io".
- Si el comando soporta el volcado de la salida a un fichero, éste se especifica con `-f`.
- Para separar varios elementos del mismo tipo, se usa el carácter `"|"`.
- A continuación se incluyen los parámetros soportados por cada comando.

Comando "delete"

Borra los ficheros indicados con el parámetro `-n`, `-m` o `-s` que se encuentren en la ruta indicada por el parámetro `-p`. Si el fichero está en uso el comando `delete` devolverá un error.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
<code>-h</code>	<code>--help</code>	Ayuda del comando.	
<code>-f</code>	<code>--force</code>	Borra los ficheros definitivamente sin pasar por la papelera de reciclaje.	
<code>-r</code>	<code>--restore</code>	En vez de borrar, recupera de la papelera de reciclaje los ficheros indicados.	Los ficheros se restauran a su localización original.
<code>-p</code>	<code>--path</code>	Ruta absoluta desde el directorio raíz a partir de la cual se buscarán los ficheros a borrar. Solo se borrarán los ficheros que pertenezcan a la ruta	• El carácter separador de carpetas es <code>"\"</code>. • No se soportan

Parámetro corto	Parámetro largo	Descripción	Anotaciones
		indicada.	caracteres comodín.
-n	--name	Nombre de los ficheros a borrar.	- Para indicar varios ficheros se utiliza el carácter “ ” - No se soportan caracteres comodín.
-m	--md5	MD5 de los ficheros a borrar s.	- Para indicar varios MD5 se utiliza el carácter “ ” - No se soportan caracteres comodín.
-s	--sha256	SHA256 de los ficheros a borrar.	- Para indicar varios SHA256 se utiliza el carácter “ ” - No se soportan caracteres comodín.

Tabla 26.10: Parámetros del comando delete

Comando “dump”

Vuelca a disco el espacio de memoria asignado a un proceso de usuario o de sistema.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	--help	Ayuda del comando.	
-p	--pid	PID del proceso a volcar.	Consulta el Comando

Parámetro corto	Parámetro largo	Descripción	Anotaciones
			"process" para obtener el PID del proceso a volcar.
-s	--system	Volcado del kernel.	Valores admitidos: • mini: volcado corto con el contenido de la pila. • kernel: volcado completo. • full: volcado de toda la memoria física del equipo, aunque no esté en uso.
-f	--filename	Nombre del fichero donde se guardará el volcado.	
-z	--zip	El volcado se almacenará en un fichero comprimido en formato zip.	

Tabla 26.11: Parámetros del comando dump

Comando "netinfo"

Muestra la configuración de las interfaces de red instaladas en el equipo con el parámetro **-a**.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	--help	Ayuda del comando.	
-a	--all	Muestra por pantalla la configuración de las interfaces de red instaladas en el equipo.	
-f	--filename	Nombre del fichero donde se guardará la información.	
-z	--zip	El volcado se almacenará en un fichero comprimido en formato zip.	

Tabla 26.12: Parámetros del comando netinfo

Comando “pcap”

Captura el tráfico de red recibido y enviado desde el equipo remoto. El inicio y la finalización de la captura se indican mediante el parámetro `-a start| stop`. La captura de paquetes genera ficheros temporales en el equipo, por lo que es necesario espacio suficiente en el disco duro. El resultado final es un fichero con formato pcap directamente utilizable por el programa Wireshark / Ethereal.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	--help	Ayuda del comando.	
-a	--action	Ejecuta una acción: • start: inicia el proceso de captura. • stop: finaliza el proceso de captura. • queryStatus: muestra el estado del proceso de captura.	
-m	--maxsize	Tamaño máximo del paquete a capturar.	• Especificado en megabytes. • Valor por defecto: 200 Mbytes.
-i	--maxtime	Tiempo máximo de captura.	• Especificado en segundos. • Valor por defecto: 86400 segundos (1 día).
-f	--filename	Nombre del fichero donde se almacenará la información.	
-z	--zip	El volcado se almacenará en un fichero comprimido en formato zip.	

Tabla 26.13: Parámetros del comando pcap

Comando “ports”

Con el parámetro `-a` muestra los sockets abiertos en el equipo y los procesos que los abrieron.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	--help	Ayuda del comando.	
-a	--all	Muestra todos los puertos abiertos y su proceso asociado.	
-p	--pid	Filtra el resultado por el PID de un proceso.	
-n	--name	Filtra el resultado por el nombre de un proceso.	Soporta búsquedas parciales por subcadenas.
-f	--filename	Nombre del fichero donde se almacenará la información.	

Tabla 26.14: Parámetros del comando ports

Comando “process”

Con el parámetro **-a** muestra todos los procesos cargados en la memoria del equipo y sus módulos.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	--help	Ayuda del comando.	
-a	--all	Muestra todos los procesos cargados en la memoria del equipo y sus módulos.	
-p	--pid	Filtra el resultado por el PID de un proceso mostrando sus módulos.	
-u	--user	Muestra los procesos lanzados por un usuario y sus módulos.	
-f	--filename	Nombre del fichero donde se almacenará la información.	

Tabla 26.15: Parámetros del comando process

Comando “url”

Con el parámetro `-a any` muestra todas las URLs accedidas por los usuarios mediante el navegador web instalado en el equipo remoto. Este comando requiere tener activado el control de acceso a páginas web de Advanced EDR.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	--help	Ayuda del comando.	
-a	--action	Filtra el listado de URLs según la acción ejecutada por el control de acceso a páginas web: • allow: muestra las URLs permitidas. • deny: muestra las URLs denegadas. • any: muestra todas las URLs navegadas.	
-c	--count	Número máximo de URLs a mostrar.	Valor por defecto: sin límite
-g	--category	Filtra el listado de URLs según la categoría asignada por el control de acceso a páginas web.	
-b	--begindate	Establece la fecha de inicio desde la que se mostrarán las URLs navegadas.	• Formato de la fecha: “YYYY-MM-DD HH:MM”. • Valor por defecto: 30 días hacia atrás de la fecha de ejecución del comando.
-e	--enddate	Establece la fecha de finalización hasta la que se mostrarán las URLs navegadas.	• Formato de la fecha: “YYYY-MM-DD HH:MM”.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
			• Valor por defecto: fecha de ejecución del comando.
-n	--urlpattern	Filtra las URLs por subcadena.	
-u	--userpattern	Filtra las URLs por usuario.	
-f	--filename	Nombre del fichero donde se guardará la información.	
-z	--zip	El volcado se almacenará en un fichero comprimido en formato zip.	

Tabla 26.16: Parámetros del comando url

Notificar un problema

En algunas ocasiones es posible que el software Advanced EDR instalado en los equipos de la red presente un mal funcionamiento. Algunos de los síntomas pueden ser:

- Fallos en el reporte del estado del equipo.
- Fallos en la descarga de conocimiento o de las actualizaciones del motor.
- Motor de protección en estado de error.

Si Advanced EDR presenta un mal funcionamiento en alguno de los equipos de la red, es posible contactar con el departamento de soporte de Cytomic a través de la consola y enviar de forma automatizada toda la información necesaria para efectuar un diagnóstico. Para ello haz clic en el menú superior **Equipos**, selecciona el equipo que presente errores y haz clic en el menú de contexto. Se desplegará un menú con la opción **Indícanos el problema**.

Si Advanced EDR presenta un mal funcionamiento en alguno de los equipos de la red, es posible contactar con el departamento de soporte de Cytomic a través de la consola y enviar de forma automatizada toda la información necesaria para efectuar un diagnóstico. Para ello haz clic en el menú superior **Equipos**, selecciona el equipo que presente errores y haz clic en el menú de contexto . Se desplegará un menú con la opción **Notificar un problema**.

Permitir el acceso externo a la consola Web

Para aquellos problemas que el administrador de la red no pueda resolver, existe la posibilidad de habilitar el acceso a la consola únicamente para equipo de soporte de Cytomic:

- Haz clic en el menú superior **Configuración**, panel lateral **Usuarios**.
- En la pestaña **Usuarios** haz clic en el control **Permitir al equipo de Cytomic (Panda Security) acceder a mi consola**.

Eliminar el ransomware y recuperar el estado anterior

Las amenazas de tipo ransomware cifran el contenido de los ficheros en los equipos de usuario y servidores, y piden un rescate a la empresa para obtener la clave de recuperación que permite acceder nuevamente a la información cifrada. Este tipo de amenaza es sumamente peligrosa por su potencial impacto en el funcionamiento del negocio. Advanced EDR implementa varias funcionalidades que ayudan tanto en la fase de detección del ataque como en su resolución.

Sigue los pasos mostrados a continuación si detectas un ataque de tipo ransomware:



Dado que Shadow Copies realiza una copia de seguridad diaria de los ficheros y mantiene un máximo de 7 copias, es importante recuperar los archivos encriptados antes del período de 7 días. Si no es así, todas las copias almacenadas estarían cifradas.

- Utiliza la funcionalidad **Aislar equipo** para aislar los equipos afectados. Ten en cuenta que aislar un equipo puede impedir su funcionamiento normal, y en el caso de servidores, también puede impedir el buen funcionamiento del resto de equipos de la red. Si necesitas más información para configurar esta funcionalidad, consulta [Aislar un equipo](#).
- Comprueba que el software de protección está funcionando en todos los equipos:
 - Para ver el estado de la protección, consulta el widget **Estado de protección** en la página [608](#).
 - Reinstala el software de seguridad de aquellos que muestran el estado **Error**.
 - Descubre los equipos sin software de seguridad instalado. Si necesitas más información para configurar esta funcionalidad, consulta [Visualizar equipos descubiertos](#) en la página [121](#).
- Configura la protección avanzada con las opciones mostradas a continuación (si necesitas más información, consulta [Protección avanzada](#) en la página [296](#)).

- Modo de funcionamiento: **Lock**.
- Activar políticas avanzadas en modo **Bloquear**.
- Activar Anti-exploit en modo **Bloquear**.
- Activar **Inyección avanzada de código**.
- Configura la protección anti tamper y establece una contraseña para evitar la desinstalación del software de protección. Si necesitas más información para configurar esta funcionalidad, consulta [Configurar la seguridad frente a manipulaciones no deseadas de las protecciones](#) en la página 285.
- Comprueba que la funcionalidad Shadow Copies está configurada entre el 10 y el 20% para evitar el borrado de copias por falta de espacio. Si necesitas más información para configurar esta funcionalidad, consulta [Configuración de Shadow Copies](#) en la página 289.
- Para eliminar el ransomware sigue los pasos mostrados a continuación:
 - Instala como mínimo los parches que corrigen las vulnerabilidades críticas detectadas. Consulta [Cytomic Patch\(Actualización de programas vulnerables\)](#) en la página 375.
 - Lanza una tarea de análisis bajo demanda. Consulta [Análisis y desinfección bajo demanda de equipos](#).
 - Reinicia los equipos afectados para cerrar cualquier conexión remota en curso. Si necesitas más información para configurar esta funcionalidad, consulta [Reiniciar equipos](#).
 - Si tras el reinicio continúa la actividad del ransomware, contacta con el departamento de soporte de Cytomic.
- Restaura los archivos cifrados en cada equipo con Shadow copies o con el procedimiento de recuperación de datos implantado en tu empresa.
- Restaura las configuraciones de seguridad modificadas al comienzo de este procedimiento a sus valores habituales.

Capítulo 27

Tareas

Una tarea es un recurso implementado en Advanced EDR que permite establecer dos características a la ejecución de un proceso: la repetición y el aplazamiento de su inicio.

- **Repetición:** configura la tarea para su ejecución de forma puntual o repetida a lo largo del tiempo.
- **Aplazamiento:** configura la tarea para ser ejecutada en el momento en que se define (tarea inmediata), o aplazada en el tiempo (tarea programada).

Contenido del capítulo

Introducción al sistema de tareas	825
Crear tareas desde la zona Tareas	827
Publicar tareas	830
Listado de tareas	830
Gestionar tareas	832
Resultados de una tarea	836
Ajuste automático de los destinatarios de una tarea	838

Introducción al sistema de tareas

Accesibilidad del sistema de tareas

Dependiendo de la necesidad o no de configurar todos los parámetros de una tarea, ésta se puede crear desde varios lugares dentro de la consola:

- Menú superior **Tareas**
- Árbol de equipos en el menú superior **Equipos**
- Listados asociados a los distintos módulos soportados.

El árbol de equipos y los listados permiten programar y lanzar tareas de forma ágil, sin necesidad de pasar por todo el proceso de configuración y publicación descrito en [Secuencia completa para lanzar una tarea](#), perdiendo algo de flexibilidad en su definición.

Secuencia completa para lanzar una tarea

El recurso principal para crear una tarea se encuentra en la zona **Tareas**, accesible desde el menú superior de la consola. En esta ventana se definen las tareas desde cero, controlando todos los aspectos del proceso.

El proceso para lanzar una tarea consta de tres pasos:

- **Crear y configurar la tarea:** establece los equipos afectados, las características de la tarea, el momento en que será lanzada, el número de veces que se ejecutará y su comportamiento en caso de error. La configuración de una tarea depende de su tipo. Para obtener información sobre cómo crear y configurar una tarea consulta [Tipos de procesos ejecutados por una tarea](#)
- **Publicar la tarea:** las tareas creadas se introducen en el programador de procesos de Advanced EDR para lanzarse en el momento marcado por su configuración.
- **Ejecutar la tarea:** el programador lanza el proceso en los equipos cuando se alcanzan las condiciones especificadas en la definición de la tarea.

Tipos de procesos ejecutados por una tarea

Advanced EDR ejecuta como tarea los procesos siguientes:

- Análisis y desinfección de ficheros. Consulta [Análisis y desinfección bajo demanda de equipos](#) en la página [799](#) para más información.
- Instalación de parches y actualizaciones del sistema operativo y de los programas instalados en el equipo. Consulta [Descargar e instalar parches](#) en la página [382](#) para más información.
- Búsqueda de IOCs en los equipos de la red. Consulta [Gestión y detección de IOCs](#) en la página [531](#) para más información.

Permisos asociados a la gestión de tareas



Para obtener más información sobre el sistema de permisos implementado en Advanced EDR consulta [Descripción de los permisos implementados](#) en la página [70](#).

Para crear, editar, eliminar o visualizar tareas es necesario utilizar una cuenta de usuario que tenga asignado el permiso apropiado a su rol. Dependiendo del tipo de tarea, los permisos necesarios son:

- **Lanzar análisis y desinfectar:** para crear borrar y modificar tareas de tipo Análisis programado.
- **Buscar y administrar IOCs:** para crear borrar y modificar tareas de tipo Detectar IOCs.

- **Instalar, desinstalar y excluir parches:** para crear borrar y modificar tareas de tipo Instalar parches.
- **Visualizar detecciones:** para visualizar los resultados de las tareas de tipo Análisis programado.

Crear tareas desde la zona Tareas

- Haz clic el menú superior **Tareas**. Se mostrará un listado con todas las tareas y su estado.
- Haz clic en el botón **Añadir tarea** y elige el tipo de tarea en el desplegable: se mostrará una ventana con los datos de la tarea, distribuidos en varias zonas:
 - **Información general (1):** nombre de la tarea y descripción.
 - **Destinatarios (2):** equipos que recibirán la tarea.
 - **Programación (3):** configuración del momento en que se lanzará la tarea.
 - **Configuración (4):** establece las acciones a ejecutar por la tarea. Esta sección varía según el tipo de tarea y se detalla en la documentación asociada al módulo relacionado.

Cancel **New task** **Save**

Name: New scan task **1**

Description: Description

Recipients: No recipients selected yet **2**

Starts: ☐ As soon as possible

7/2/2020 9:00 AM ☒ Computer's local time

3 If the computer is turned off at the scheduled time, run the task as soon as
1 week

Maximum run time: No limit

Repeat: Every week

Scan options

Scan type **4** Critical areas (recommended)
Scans the memory, running processes, cookies, etc.

Detect viruses: ☐

Detect hacking tools and PUPs: ☐

Figura 27. 1: Vista general de la ventana Nueva tarea para una tarea de tipo análisis

Destinatarios de la tarea (2)



Para acceder a la ventana de selección de equipos, es necesario guardar previamente la tarea. Si la tarea no ha sido guardada, se mostrará una ventana de advertencia.

- Haz clic en el enlace **Destinatarios (No se ha asignado a ningún equipo)** para abrir una ventana nueva donde seleccionar los equipos que recibirán la tarea configurada.
- Selecciona el tipo de equipos que recibirán la tarea: **Estación, Portátil, Servidor o Dispositivo móvil**. El tipo de equipo que puede recibir la tarea variará dependiendo de la tarea que se va a ejecutar.
- Haz clic en el botón para agregar equipos individuales o grupos de equipos, y en el botón para eliminarlos.



Si se trata de una tarea de instalación de parches y quieres que se envíe solo a equipos de prueba, desplaza el cursor deslizante **Ejecutar la tarea solo en equipos de prueba**. Esta opción solo es aplicable a proveedores de servicios que tengan contratado CYTOMIC Nexus. Para más información, consulta **Funcionalidades de Cytomic Patch** en la página 376

- En la ventana **Editar tarea**, haz clic en el botón **Ver equipos** para verificar los equipos que recibirán la tarea.

Programación horaria y repetición de la tarea

Se establece mediante tres parámetros:

- **Empieza:** marca el inicio de la tarea.

Valor	Descripción
Lo antes posible (activado)	La tarea se lanza en el momento si el equipo está disponible (encendido y accesible desde la nube), o cuando se encuentre disponible dentro del margen definido en el desplegable Equipo apagado .
Lo antes posible (desactivado)	La tarea se lanza en la fecha seleccionada en el calendario, indicando si se tiene en cuenta la hora del equipo o la hora del servidor Advanced EDR.
Equipo apagado	Si el equipo está apagado o inaccesible, la tarea no se podrá lanzar. El sistema de programación de tareas permite establecer la caducidad de la tarea en

Valor	Descripción
	función del intervalo de tiempo definido por el administrador, desde 0 (la tarea caduca de forma inmediata si el equipo no está disponible) a infinito (la tarea siempre está activa y se espera a que el equipo esté disponible de forma indefinida): • No ejecutar: la tarea se cancela si en el momento del lanzamiento el equipo no está encendido o no es accesible. • Dar un margen de: define un intervalo de tiempo dentro del cual, si el equipo inicialmente no estaba disponible y vuelve a estarlo, la tarea será lanzada. • Ejecutar cuando se encienda: no establece ningún intervalo de tiempo sino que se espera de forma indefinida a que el equipo esté accesible para lanzar la tarea.

Tabla 27.1: Comportamiento del inicio de la tarea si el equipo no está disponible

- **Tiempo máximo de ejecución:** indica el tiempo máximo que la tarea puede tardar en completarse, transcurrido el cual se cancelará con error si no ha terminado.

Valor	Descripción
Sin límite	La duración de la ejecución de la tarea no está definida, pudiéndose extender hasta el infinito.
1, 2, 8 o 24 horas	La duración de la ejecución de la tarea está acotada. Transcurrido el tiempo indicado, la tarea se cancela con error si no ha terminado.

Tabla 27.2: Configuración de la duración de la tarea

- **Frecuencia:** establece un intervalo de repetición cada día, semana, mes o año tomando como referencia la fecha indicada en el campo **Empieza**:

Valor	Descripción
Ejecución única	La tarea se ejecuta de forma puntual a la hora indicada en el campo Empieza .
Diaria	La tarea se ejecuta todos los días a la hora indicada en el campo Empieza .
Semanal	Haz clic en las casillas de selección para establecer la ejecución de la tarea en los días de la semana elegidos, a la hora indicada en el campo Empieza .

Valor	Descripción
Mensual	Elige una de las opciones: • Ejecutar la tarea un día concreto de cada mes. Si se eligen los días 29, 30 o 31 y el mes no tiene esos días, la tarea se ejecuta el último día del mes. • Ejecutar la tarea el primer, segundo, tercer, cuarto o último día de la semana de cada mes.

Tabla 27.3: Configuración de la frecuencia de la tarea

Conversión automática de la frecuencia de ejecución

Si alguno de los equipos del parque informático tiene instalada una versión anterior del software de seguridad, es posible que no sea capaz de interpretar correctamente las configuraciones de frecuencia establecidas por el administrador en la consola web. En este caso, cada equipo establecerá las siguientes correspondencias para la configuración de la frecuencia en las tareas a ejecutar:

- **Tareas diarias:** sin cambios.
- **Tareas semanales:** se omiten los días elegidos por el administrador. La primera ejecución se realiza en la fecha indicada en **Empieza** y, a partir de este punto, se ejecutará nuevamente cada 7 días.
- **Tareas mensuales:** se omiten los días elegidos por el administrador. La primera ejecución se realiza en la fecha indicada en **Empieza** y, a partir de este punto, se ejecutará nuevamente cada 30 días.

Publicar tareas

Una vez creada y configurada, la tarea aparecerá en el listado de tareas configuradas, pero mostrará la etiqueta **Sin publicar**, indicando que no está activa.

Haz clic en el enlace **Publicar** para introducir la tarea en el programador de Advanced EDR, encargado de marcar el momento en que se lanzan las tareas según su configuración.

Listado de tareas

Haz clic en el menú superior **Tareas** para listar tareas creadas, su tipo, estado y otra información relevante.

Campo	Comentario	Valores
Icono	Tipo de la tarea	•  Tarea de tipo instalación o

Campo	Comentario	Valores
		desinstalación de parches  Tarea de tipo desinfección  Tarea de detección de IOCs
Nombre	Nombre de la tarea creada	Cadena de caracteres
Programación	Cuando se ejecuta la tarea.	Cadena de caracteres
Estado	• Sin destinatarios: la tarea no se ejecutará porque no tiene destinatarios asignados. Asigna uno o más equipos a la tarea. • Sin publicar: la tarea no se ejecutará porque no ha entrado en la cola del programador. Publica la tarea para que el programador de procesos planifique su ejecución. • En curso: la tarea se está ejecutando. • Cancelada: la tarea fue cancelada de forma manual. No implica que todos los procesos en ejecución en los diferentes equipos se hayan detenido. • Finalizada: todos los equipos terminaron la ejecución de la tarea asignada, independientemente de que haya finalizado con éxito o con error. Este estado solo se da en las tareas de ejecución puntual o única.	Cadena de caracteres

Tabla 27.4: Campos del listado Tareas creadas

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de tarea	Clase de la tarea	• Análisis • Desinfección • Instalación de parches • Desinstalación de parches • Búsqueda de IOCs
Buscar tarea	Nombre de la tarea	Cadena de caracteres
Programación	Frecuencia de la repetición de la tarea	• Todos • Inmediata • Una vez • Programada
Estado	Estado de la tarea	• Todos • Sin destinatarios • Sin publicar • En curso • Cancelada • Finalizada
Ordenar listado ↓	Criterio de ordenación de las tareas creadas.	• Ordenar por fecha de creación • Ordenar por nombre • Ascendente • Descendente

Tabla 27.5: Campos de filtrado para el listado Tareas creadas

Gestionar tareas

Haz clic en el menú superior **Tareas** para borrar, copiar, cancelar o visualizar los resultados de las tareas creadas.

Seleccionar las tareas a gestionar

- Para gestionar una única tarea, selecciona la casilla situada junto a su nombre.
- Para gestionar todas las tareas visibles en el listado, selecciona la casilla situada junto a la barra de búsqueda en la parte superior del listado. Si quieres seleccionar todas las tareas de todas las páginas del listado, haz clic en el enlace **Seleccionar las X filas del listado**.

Modificar tareas publicadas

Haz clic en el nombre de la tarea creada para mostrar su ventana de configuración, donde es posible modificar algunos de sus parámetros.



Las tareas publicadas solo admiten cambio de nombre y de descripción. Para modificar otros parámetros de una tarea publicada, es necesario copiarla previamente.

Cancelar tareas publicadas

Haz clic en las casillas de selección de las tareas a cancelar y en el icono **Cancelar** de la barra de herramientas. Las tareas se cancelarán, aunque no se borrarán de la ventana de tareas para poder acceder a sus resultados. Únicamente se pueden cancelar las tareas en estado **En curso**.

Borrar tareas

Las tareas ejecutadas no se eliminan automáticamente, para ello es necesario hacer clic en las casillas de selección y después en el icono en la barra de herramientas. Una tarea publicada solo se puede borrar si previamente es cancelada.



Al borrar una tarea se borrarán también sus resultados.

Copiar tareas

Copiar una tarea implica replicar toda su configuración. Con el objeto de reutilizar tareas para asignarlas a distintos grupos de equipos, la copia de los destinatarios de la tarea original es opcional.

- Haz clic en el menú superior **Tareas** y en el icono de la tarea que quieres copiar. Se mostrará un menú para seleccionar el tipo de copia.

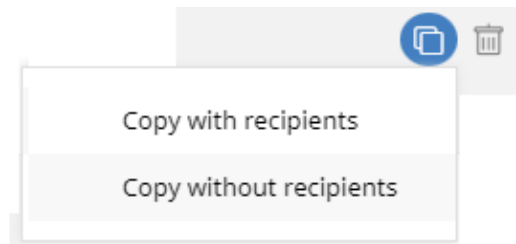


Figura 27.2: Ventana del icono Copiar tarea

- Si has seleccionado **Copia sin destinatarios**, se abrirá la ventana **Copiar tarea**.
 - Para asignar destinatarios haz clic en el enlace **No se ha asignado a ningún equipo**. Se mostrará la ventana **Destinatarios**.
 - Selecciona los destinatarios de la tarea y haz clic en el botón **Guardar** situado en la esquina superior derecha de la ventana.



*Si se trata de una tarea de instalación de parches y quieres que se envíe solo a equipos de prueba, desplaza el cursor deslizante **Ejecutar la tarea solo en equipos de prueba**. Esta opción solo es aplicable a proveedores de servicios que tengan contratado CYTOMIC Nexus. Para más información, consulta [Funcionalidades de Cytomic Patch](#) en la página 376*

Si has seleccionado **Copia con destinatarios**, se abrirá la ventana **Copiar tarea** con los destinatarios de la tarea original.

Exportar tareas



Haz clic en el icono para exportar un listado de las tareas creadas. El archivo csv. se guardará en la carpeta que elija el usuario.

En el archivo descargado se muestran los campos:

Campo	Definición
Nombre de la tarea	Nombre de la tarea
Tipo de la tarea	Tipo de tarea: • Búsqueda de IOCs • Desinstalación de parches • Instalación de parches

Campo	Definición
	Análisis
Programación	Frecuencia de ejecución de la tarea: - Inmediata - Una vez - Programada
Estado	Estado en el que se encuentra la tarea: - Sin destinatarios - Sin publicar - En curso - Cancelada - Finalizada
Grupo destinatario	Grupo destinatario de la tarea.
Estación	Sí: la tarea se asignará a los equipos de tipo Estación del grupo destinatario. No: la tarea no se asignará a los equipos de tipo Estación del grupo destinatario.
Portátil	Sí: la tarea se asignará a los equipos de tipo Portátil del grupo destinatario. No: la tarea no se asignará a los equipos de tipo Portátil del grupo destinatario.
Servidor	Sí: la tarea se asignará a los equipos de tipo Servidor del grupo destinatario. No: la tarea no se asignará a los equipos de tipo Servidor del grupo destinatario.
Dispositivo móvil	Sí: la tarea se asignará a los dispositivos móviles del grupo destinatario. No: la tarea no se asignará a los dispositivos móviles del grupo destinatario.

Campo	Definición
Equipo destinatario	Equipo destinatario de la tarea.
Grupo del equipo destinatario	Tipo de equipo destinatario de la tarea: • Estación • Portátil • Servidor • Dispositivo móvil

Tabla 27.6: Listado de exportación de tareas

Resultados de una tarea

Al hacer clic en el enlace **Ver resultados** de una tarea publicada se mostrarán los resultados obtenidos hasta ese momento y una herramienta de filtrado que permite localizar equipos específicos que recibieron la tarea.

Algunos de los campos incluidos en el listado de resultados son específicos de cada tarea. Estos campos se incluyen en la documentación del módulo correspondiente. A continuación se muestran los campos comunes a todos los listados de resultados.

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se registró un evento de ejecución de tarea.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Advanced EDR a la que pertenece el equipo.	Cadena de caracteres
Estado	Estado del proceso asignado por la tarea para su ejecución en el equipo: • Pendiente: la tarea no ha iniciado la ejecución de su siguiente repetición por estar programada para un momento posterior. • En curso: la tarea se está ejecutando en el equipo. • Finalizada: la tarea terminó con éxito. • Con error: la tarea terminó con error. • Cancelada (no se pudo iniciar a la hora programada): la tarea estaba programada para iniciar su ejecución pero en ese	Cadena de caracteres

Campo	Descripción	Valores
	momento el equipo estaba apagado o en un estado que impedía su ejecución. • Cancelada: el proceso fue cancelado en el equipo. • Cancelando: la tarea se canceló pero el equipo todavía no ha completado la orden de cancelar el proceso. • Cancelada (tiempo máximo superado): la tarea se canceló automáticamente al expirar el tiempo máximo establecido para su ejecución.	
Fecha de comienzo	Fecha de inicio de la tarea.	Fecha
Fecha fin	Fecha de finalización de la tarea.	Fecha

Tabla 27.7: Campos comunes en el resultado de una tarea

Herramienta de filtrado de tareas

Campo	Descripción	Valores
Fecha	Desplegable con las fechas en las que la tarea pasó a estado activo según su programación configurada. Una tarea activa puede iniciarse en el momento o esperar a que el equipo esté disponible. Esta fecha se indica en la columna fecha.	Fecha

Campo	Descripción	Valores
Estado	• Pendiente: la tarea todavía no se ha iniciado por no haber alcanzado la ventana de ejecución configurada. • En progreso: la tarea se está ejecutando en este momento. • Con éxito: la tarea terminó con éxito. • Con error: la tarea terminó con error. • Cancelada (no se pudo iniciar a la hora programada): el equipo no estaba disponible en el momento del inicio de la tarea o en el intervalo definido. • Cancelada: la tarea fue cancelada de forma manual. • Cancelada (tiempo máximo expirado): la tarea duró más tiempo que el indicado en la configuración de la tarea y se canceló.	Enumeración

Tabla 27.8: Filtros de búsqueda en los resultados de una tarea

Ajuste automático de los destinatarios de una tarea

Si el administrador establece un grupo de equipos como destinatario de una tarea, el conjunto final de equipos sobre los que se ejecutará puede variar debido a que los grupos son entidades dinámicas que varían a lo largo del tiempo.

De esta manera, una tarea definida en el momento T1 y asignada a un grupo tendrá como destinatarios los equipos que forman el grupo seleccionado, pero en el momento de ejecución posterior T2, los miembros de ese grupo pueden haber cambiado.

A la hora de resolver qué equipos pertenecen al grupo asignado a la tarea, se distinguen tres casos según su tipo:

- Tareas inmediatas.
- Tareas programadas de ejecución puntual o única.
- Tareas programadas de ejecución repetida.

Tareas inmediatas

Estas tareas se crean, se publican y se lanzan de forma atómica e inmediata una única vez. El grupo destinatario se evalúa en el momento en que el administrador crea la tarea. Los equipos afectados aparecerán en estado **Pendiente** en la tarea.

Añadir equipos al grupo destinatario

No se permite añadir nuevos equipos. Aunque se asignen nuevos equipos al grupo destinatario, éstos no recibirán la tarea.

Quitar equipos del grupo destinatario

Sí se pueden retirar equipos del grupo destinatario. Para cancelar la tarea mueve los equipos a otro grupo.

Tareas programadas de ejecución única

Estas tareas admiten dos estados con respecto a la posibilidad de cambiar a los integrantes del grupo de equipos destinatario:

Tareas cuya ejecución comenzó hace menos de 24 horas

En las primeras 24 horas de la ejecución, el administrador puede añadir o retirar equipos a los grupos destinatarios. Se marca un plazo de 24 horas para abarcar todos los husos horarios en aquellas multinacionales con presencia en varios países.

Tareas cuya ejecución comenzó hace más de 24 horas

Una vez cumplido el plazo de 24 horas no será posible añadir nuevos equipos y, aunque se asignen nuevos equipos al grupo destinatario, éstos no recibirán la tarea. Para cancelar las tareas en curso sobre equipos muévelos fuera del grupo destinatario.

Tareas programadas de ejecución repetida

Estas tareas permiten agregar o eliminar equipos destinatarios en cualquier momento hasta su cancelación o finalización.

Las tareas programadas de ejecución repetida no muestran los equipos destinatarios en estado **Pendiente** de forma automática, sino que éstos se irán mostrando de forma progresiva a medida que la plataforma Cytomic reciba información del estado de la tarea de cada equipo.

Capítulo 28

Funcionalidades del producto y requisitos

Contenido del capítulo

Funcionalidades por plataforma	841

Funcionalidades por plataforma

General

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Consola web	X	X	X
Dashboards	X	X	X
Organización de los equipos por filtros	X	X	X
Organización de los equipos en grupos	X	X	X
Idiomas disponibles en el software de protección	11	11	11

Tabla 28.1: Funcionalidades generales

Listados e informes

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Frecuencia de envío al servidor de la actividad del malware, PUPs, exploits y programas bloqueados	1 min	10 min	10 min
Frecuencia de envío de otras detecciones	15 min	15 min	15 min
Listado de detecciones	X	X	X
Informe ejecutivo	X	X	X
Informe ejecutivo programado	X	X	X

Tabla 28.2: Funcionalidades de listados e informes

Protecciones

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Detecciones contextuales	X	X	
Protección contra ataques de red	X		
Anti-exploit (*)	X		
Zero-Trust Application Service: modos de protección hardening y lock	X		
Indicadores de ataque (IOAs)	X	X	X
Evaluación de riesgos	X	X	X
Shadow Copies	X		
Decoy Files	X		
Indicadores de compromiso (IOCs)	X		

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
compatibles con STIXs y reglas Yara			
Políticas de seguridad avanzada	X		
Indicadores de ataque (IOAs) avanzados	X		

Tabla 28.3: Funcionalidades de protección

Información de hardware y software

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Información y listado de hardware	X	X	X
Información y listado de software	X	X	X
Registro de cambios de software	X	X	X
Información de los parches instalados del sistema operativo	X		
Evaluación de vulnerabilidades	X	X	X

Tabla 28.4: Funcionalidades de información de hardware y software

Configuraciones

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Seguridad para estaciones y servidores	X	X	X
Anti-tamper	X	X	
Verificación en dos pasos	X	X	
Contraseña para desinstalar la protección y tomar acciones en local	X	X	

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Control de acceso a redes VPN	X		X
Control de acceso a redes WiFi	X		X
Asignar listas de proxies	X	X	X
Actuar como Proxy Cytomic	X		
Acceder a la red través de proxy	X	X	X
Actuar como caché de descargas	X		
Utilizar caché de descargas	X		
Descubrir equipos desprotegidos	X		
Alertas por correo ante infecciones	X	X	X
Alertas por correo ante equipos desprotegidos	X	X	X

Tabla 28.5: Funcionalidades de configuración

Acciones remotas desde Consola Web

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Acciones en tiempo real	X	X	X
Análisis bajo demanda	X	X	X
Análisis programados	X	X	X
Instalación remota del agente de Cytomic	X		
Desinstalacion remota del agente de Cytomic	X	X	X

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Posibilidad de reinstalar agente de protección	X		
Reiniciar equipo	X	X	X
Aislar equipos	X	X	X
Autorizar la ejecución de software	X		
Bloquear la ejecución de programas	X		
Reportar una incidencia (PSInfo)	X		
Shell remoto (administrar procesos y servicios, transferencias de archivos, línea de comandos, volcados de memoria, captura de tráfico de red, etc)	X	X	X
Notificar un problema	X	X	X

Tabla 28.6: Acciones remotas disponibles

Actualizaciones del software de seguridad

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Actualizaciones de la protección	X	X	X
Programar la actualización de la protección	X	X	X

Tabla 28.7: Funcionalidades de actualización del software de seguridad

Módulos disponibles

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Cytomic Insights	X	X	X

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Cytomic Patch	X	X	X
Cytomic Data Watch(*)	X		
Cytomic Encryption	X	X	X

Tabla 28.8: Módulos disponibles

(*) Disponible solo en microprocesadores Intel y parcialmente en Windows (ARM)

Funcionalidades del producto y requisitos

Contenido del capítulo

Funcionalidades por plataforma	847
Requisitos de plataformas Windows	852
Requisitos de plataformas macOS	856
Requisitos de plataformas Linux	859
Puertos locales y acceso a URLs	862

Funcionalidades por plataforma

General

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Consola web	X	X	X
Dashboards	X	X	X
Organización de los equipos por filtros	X	X	X
Organización de los equipos en grupos	X	X	X
Idiomas disponibles en el software de protección	11	11	11

Tabla 28.9: Funcionalidades generales

Listados e informes

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Frecuencia de envío al servidor de la actividad del	1 min	10 min	10 min

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
malware, PUPs, exploits y programas bloqueados			
Frecuencia de envío de otras detecciones	15 min	15 min	15 min
Listado de detecciones	X	X	X
Informe ejecutivo	X	X	X
Informe ejecutivo programado	X	X	X

Tabla 28.10: Funcionalidades de listados e informes

Protecciones

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Detecciones contextuales	X	X	
Protección contra ataques de red	X		
Anti-exploit (*)	X		
Zero-Trust Application Service: modos de protección hardening y lock	X		
Indicadores de ataque (IOAs)	X	X	X
Evaluación de riesgos	X	X	X
Shadow Copies	X		
Decoy Files	X		
Indicadores de compromiso (IOCs) compatibles con STIXs y reglas Yara	X		

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Políticas de seguridad avanzada	X		
Indicadores de ataque (IOAs) avanzados	X		

Tabla 28.11: Funcionalidades de protección

Información de hardware y software

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Información y listado de hardware	X	X	X
Información y listado de software	X	X	X
Registro de cambios de software	X	X	X
Información de los parches instalados del sistema operativo	X		
Evaluación de vulnerabilidades	X	X	X

Tabla 28.12: Funcionalidades de información de hardware y software

Configuraciones

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Seguridad para estaciones y servidores	X	X	X
Anti-tamper	X	X	
Verificación en dos pasos	X	X	
Contraseña para desinstalar la protección y tomar acciones en local	X	X	
Control de acceso a redes VPN	X		X

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Control de acceso a redes WiFi	X		X
Asignar listas de proxies	X	X	X
Actuar como Proxy Cytomic	X		
Acceder a la red través de proxy	X	X	X
Actuar como caché de descargas	X		
Utilizar caché de descargas	X		
Descubrir equipos desprotegidos	X		
Alertas por correo ante infecciones	X	X	X
Alertas por correo ante equipos desprotegidos	X	X	X

Tabla 28.13: Funcionalidades de configuración

Acciones remotas desde Consola Web

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Acciones en tiempo real	X	X	X
Análisis bajo demanda	X	X	X
Análisis programados	X	X	X
Instalación remota del agente de Cytomic	X		
Desinstalacion remota del agente de Cytomic	X	X	X
Posibilidad de reinstalar agente de protección	X		

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Reiniciar equipo	X	X	X
Aislar equipos	X	X	X
Autorizar la ejecución de software	X		
Bloquear la ejecución de programas	X		
Reportar una incidencia (PSInfo)	X		
Shell remoto (administrar procesos y servicios, transferencias de archivos, línea de comandos, volcados de memoria, captura de tráfico de red, etc)	X	X	X
Notificar un problema	X	X	X

Tabla 28.14: Acciones remotas disponibles

Actualizaciones del software de seguridad

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Actualizaciones de la protección	X	X	X
Programar la actualización de la protección	X	X	X

Tabla 28.15: Funcionalidades de actualización del software de seguridad

Módulos disponibles

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Cyatomic Insights	X	X	X
Cyatomic Patch	X	X	X

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)
Cytoomic Data Watch(*)	X		
Cytoomic Encryption	X	X	X

Tabla 28.16: Módulos disponibles

(*) Disponible solo en microprocesadores Intel y parcialmente en Windows (ARM)

Requisitos de plataformas Windows

Sistemas operativos soportados



A partir de la fecha 30/09/2024 no será posible añadir a la consola de administración nuevos equipos que utilicen los siguientes sistemas operativos: Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008 (no afecta a Windows Server 2008 R2). Los equipos instalados en una fecha anterior seguirán protegidos. Consulta <https://www.watchguard.com/wgrd-trust-center/end-of-life-policy>

Estaciones de trabajo con microprocesador x86 y x64

- Windows XP SP3 (32 bits)
- Windows Vista (32, 64-bit)
- Windows 7 (32, 64-bit)
- Windows 8 (32, 64-bit)
- Windows 8.1 (32, 64-bit)
- Windows 10 (32, 64-bit)
- Windows 11 (64 bits)

Equipos con microprocesador ARM

- Windows 10 y Pro
- Windows 11 y Pro
- Windows 2025 Standard, Datacenter

Servidores con microprocesador x86 y x64

- Windows 2003 (32, 64-bit) y R2 SP2
- Windows 2008 (32, 64-bit) y R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 y 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 y 2022

IoT y Windows Embedded Industry

- Windows XP Embedded
- Windows Embedded for Point of Service
- Windows Embedded POSReady 2009, 7, 7 (64 bits)
- Windows Embedded Standard 2009, 7, 7 (64 bits), 8, 8 (64 bits),
- Windows Embedded Pro 8, 8 (64 bits)
- Windows Embedded Industry 8, 8 (64 bits), 8.1, 8.1 (64 bits)
- Windows IoT Core 10, 10 (64 bits)
- Windows IoT Enterprise 10, 10 (64 bits), 11
- Windows Server IoT 2019



Los sistemas embedded pueden instalarse de forma personalizada, por lo que el funcionamiento de Advanced EDR y de algunos de sus módulos en dichos sistemas podría variar según la instalación. Para comprobarlo, instala Advanced EDR y verifica que las diferentes protecciones funcionan correctamente.

Requisitos hardware

- **Procesador:** CPU compatible x86 o x64 y con soporte SSE2.
- **Memoria RAM:** 1 Gbyte
- **Espacio libre en el disco duro para la instalación:** el espacio para instalar el software de seguridad

varía dependiendo de la versión del sistema operativo instalada en el equipo. De media se requieren 650 MBytes.

Otros requisitos

Puertos

En su funcionamiento normal, Advanced EDR accede a varios recursos alojados en Internet. De forma general, se requiere acceso a los puertos 80 y 443.

El agente Advanced EDR requiere el puerto 33000 para la comunicación entre los equipos protegidos y con dispositivos Firebox o Access Point (consulta [Configuración de Control de Acceso a Endpoints](#) en la página 458 y [Control de acceso a redes](#) en la página 282).

Actualizar los certificados raíz

Para que el producto funcione correctamente, deben mantenerse actualizados los certificados raíz instalados en cada equipo protegido. Además, se requiere que los equipos puedan acceder a las siguientes URLs:

http://*.globalsign.com

http://*.digicert.com

http://*.sectigo.com

Los equipos Windows actualizan automáticamente los certificados raíz a través de Windows Update. No obstante, pueden darse problemas si las actualizaciones no han sido debidamente instaladas.

Si los certificados raíz no se actualizan, funcionalidades como la comunicación en tiempo real de los agentes con la consola de administración y el módulo Cytomic Patch podrían dejar de funcionar.



Para identificar y actualizar los certificados raíz, utiliza la herramienta que encontrarás en <https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Endpoint-Security/troubleshooting/psinfotool/psinfo-check-cert.html?Highlight=psinfo>

Sincronización horaria de los equipos (NTP)

Aunque no es un requisito indispensable, si es muy recomendable que el reloj de los equipos protegidos con Advanced EDR esté sincronizado. La mayoría de las veces, la sincronización se establece mediante el uso de un servidor NTP.

Si la sincronización no es correcta, la seguridad del equipo puede verse afectada de diferentes maneras:

- Inestabilidad en las comunicaciones entre el equipo y los servidores de Cytomic.
- Fallo en las comprobaciones de certificados, que serán válidos o estarán caducados en función de la fecha del equipo y no de la real.

- Fechas erróneas en las alertas generadas por las diferentes protecciones, que mostrarán como fecha y hora de detección la del equipo, y no la real.
- En el detalle de las tareas de análisis o de instalación de parches se mostrarán fechas no reales.
- La caducidad del instalador no se respetará.
- Algunas acciones programadas, como el reinicio del equipo y la recepción de notificaciones de problemas, podrían no ejecutarse correctamente.

Compatibilidad con firma de drivers SHA-256

Para mantener el software de seguridad actualizado a la última versión publicada por Cytomic, es necesario que el equipo del usuario o servidor sea compatible con la firma de drivers SHA-256. Algunas versiones del sistema operativo Windows no incorporan de fábrica esta funcionalidad y requieren ser actualizadas:

Plataforma Windows	Actualizaciones necesarias	URL
Vistax86 / Vistax64	SP2 + KB4474419	Enlace a KB4474419 Enlace a SP2
Server 2008x86 / Server 2008x64	SP2 + KB4474419	Enlace a KB4474419 Enlace a SP2
W7x86 / W7x64	SP1 + KB4474419	Enlace a KB4474419 Enlace a SP1
2008R2x64	KB4474419	Enlace a KB4474419

Tabla 28.17: Actualizaciones requeridas para compatibilidad con SHA-256

Los equipos no compatibles con la firma de drivers SHA-256 no actualizarán el software de protección más allá de la versión 4.00.00, y tampoco se mostrarán en el widget **Protección desactualizada** en la página 612 como candidatos a actualizarse. Estos equipos se muestran con la alerta **No es posible actualizar la protección de este equipo a la última versión**. Para obtener más información sobre las alertas de equipo y cómo visualizarlas consulta **Información de equipo** en la página 218.

Para localizar los equipos no compatibles con el firmado de drivers SHA-256 crea un filtro en el árbol de filtros con los parámetros mostrados en **Equipos no compatibles con firma de drivers SHA-256** en la página 187. Para obtener más información acerca del árbol de filtros consulta **Árbol de filtros** en la página 180.



Cytomic recomienda actualizar todos los equipos de la red para mantenerlos protegidos con la última versión del software de protección disponible en todo momento.

Cuando el administrador instala los parches indicados, se descargará de forma automática la última versión del software de protección disponible en un plazo máximo de 4 horas, si bien requerirá un reinicio para completar la actualización.

Sistemas operativos Windows XP y Windows 2003

Para que la protección avanzada funcione correctamente en estos sistemas operativos es necesario que esté instalado Internet Explorer 7 o una versión superior.

En el caso de Windows XP, no es posible instalar o actualizar la protección de manera directa, por lo que es necesario utilizar un equipo caché para ello. Para más información, consulta [Configuración de las descargas mediante equipos caché](#) en la página 279

La instalación o actualización de la protección en Windows 2003 solo es posible siempre y cuando el sistema operativo esté debidamente actualizado y con todos los parches necesarios instalados. En caso contrario, será necesario utilizar un equipo caché. Para más información consulta [Cytomic Patch \(Actualización de programas vulnerables\)](#) en la página 375

Requisitos de plataformas macOS



A partir de la fecha 30/09/2024 no será posible añadir a la consola de administración nuevos equipos que utilicen los siguientes sistemas operativos: Yosemite, El Capitan, Sierra, High Sierra y Mojave. Los equipos instalados en una fecha anterior seguirán protegidos. Consulta <https://www.watchguard.com/wgrd-trust-center/end-of-life-policy>.

Sistemas operativos soportados

- 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

Requisitos hardware

- **Procesador:** Intel® Core 2 Duo
- **Memoria RAM:** 2 Gbyte
- **Espacio libre en el disco duro para la instalación:** el espacio para instalar el software de seguridad varía dependiendo de la versión del sistema operativo instalada en el equipo. De media se requieren 400 MBytes.
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento de la detección web de malware. El agente Advanced EDR requiere el puerto 33000 para la comunicación entre equipos protegidos y con dispositivos Firebox y Access Point (consulta [Configuración de Control de Acceso a Endpoints](#) en la página 458 y [Control de acceso a redes](#) en la página 282).

Direcciones IP necesarias para activar el producto

En el proceso de instalación del software de protección, el cortafuegos corporativo debe permitir el tráfico a los siguientes rangos de direcciones IP:

- 17.248.128.0/18
- 17.250.64.0/18
- 17.248.192.0/19

Permisos necesarios

Para el correcto funcionamiento de la protección, es imprescindible que el software de seguridad cuente con los permisos necesarios en el equipo del usuario. Para ello, es necesario activar los siguientes permisos:

- Extensiones de red
- Extensiones de sistema
- Acceso total al disco
- Ejecución en segundo plano.

Según la versión de sistema operativo, los pasos a seguir son diferentes.

Instrucciones para macOS Catalina o superior

Para habilitar el permiso Extensiones del Kernel / Sistema:

- Abre el agente Advanced EDR en el equipo del usuario y haz clic en el botón **Abrir preferencias de seguridad**.
- Haz clic en el icono del candado, situado en la esquina inferior izquierda de la ventana. Se abrirá la ventana **Seguridad y privacidad**.
- Escribe las credenciales del administrador y haz clic en el botón **Desbloquear**.
- Haz clic en el botón **Permitir**. Las extensiones se han habilitado.

Para activar el permiso Acceso total al disco:

- Abre el agente Advanced EDR en el equipo del usuario y haz clic en el botón **Abrir preferencias de acceso a disco**.
- Haz clic en el icono del candado, situado en la esquina inferior izquierda de la ventana. Se abrirá la ventana **Seguridad y privacidad**.
- Escribe las credenciales del administrador y haz clic en el botón **Desbloquear**.
- Selecciona la casilla correspondiente a **Protection Agent**.
- Haz clic en el botón **Salir y abrir**. El acceso al disco se ha activado.

Instrucciones para macOS Mojave 10.14 o inferior

Al iniciarse Advanced EDR, el sistema operativo podría bloquear las extensiones de kernel necesarias para el correcto funcionamiento de la protección.

Esto se debe a que estas versiones de macOS contienen una característica de seguridad que requiere la aprobación del usuario antes de cargar nuevas extensiones de kernel de terceros.



Para mas información, consulta

https://developer.apple.com/library/archive/technotes/tn2459/_index.html#//apple_ref/doc/uid/DTS40017658

Cuando esto sucede, se mostrarán dos mensajes:

- Mensaje de bloqueo de extensiones de sistema.
- Mensaje advirtiendo de que el equipo está desprotegido.

Para resolverlo, sigue los siguientes pasos:

- En el mensaje de bloqueo de extensiones de kernel, haz clic en **OK**. También puedes hacer clic en el botón **Abrir preferencias del sistema** del mensaje de equipo en estado desprotegido. Se abrirá la ventana **Preferencias del sistema**.

- Haz clic en **Seguridad y privacidad**.
- Para desbloquear, haz clic en el icono del candado, situado en la esquina inferior izquierda de la ventana.
- En la ventana **Seguridad y privacidad**, haz clic en el botón **Permitir**. Las extensiones se han habilitado.

Instrucciones para macOS Ventura 13

La protección puede detenerse en los equipos al no permitirse la ejecución en segundo plano del agente. Por ello, es necesario asegurarse de que los equipos cuenten con el permiso de **Ejecución en segundo plano** activo.

Requisitos de plataformas Linux

Advanced EDR se instala tanto en estaciones de trabajo como en servidores Linux. Si no está presente un entorno gráfico en el momento de la instalación las protecciones URL filter y Web filter quedarán deshabilitadas. En equipos sin entorno gráfico utiliza la herramienta `/usr/local/protection-agent/pa_cmd` para controlar la protección.

Distribuciones soportadas

Distribuciones de 64 bits

- **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 y 24.10.
- **Fedora:** 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40 y 41.
- **Debian:** 8, 9, 10, 11 y 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 y 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, y 8.5.
- **CentOS Stream:** 8, 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 y 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 y 9.5.
- **LinuxMint:** 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 y 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 y 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, 8.1, 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 y 9.5.
- **OpenSUSE:** 15.3, 15.4, 15.5 y 15.6.
- **Amazon Linux:** 2

Distribuciones de 32 bits soportadas

- RedHat 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

Versiones del kernel soportadas.

Para más información sobre las distribuciones y kernels soportados en Linux, consulta https://info.cytomicmodel.com/resources/help/EPDR/v16/es/Content/28_hardware_software_network_requirements/linux_kernels.htm

Advanced EDR no es compatible con versiones especiales o modificadas del kernel de Linux.

Gestores de ficheros soportados

- Nautilus
- Pcmmanfm
- Dolphin

Requisitos hardware

- **Procesador:** CPU compatible x86 o x64 y con soporte SSE2.
- **Memoria RAM:** 1.5 Gbytes
- **Espacio libre en el disco duro para la instalación:** el espacio para instalar el software de seguridad varía dependiendo de la versión del sistema operativo instalada en el equipo. De media se requieren 500 MBytes.
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento de la detección web de malware. El agente Advanced EDR requiere el puerto 33000 para la comunicación entre equipos protegidos y con dispositivos Firebox y Access Point (consulta [Configuración de Control de Acceso a Endpoints](#) en la página 458 y [Control de acceso a redes](#) en la página 282).

Comprobaciones del script de instalación

El script de instalación realiza algunas comprobaciones en su inicio que requieren la instalación de uno de los siguientes paquetes / binarios:

- `wget`
- `curl`
- `semanage` (si se requiere integrar el software de seguridad con políticas SELinux)

Si ninguno de los paquetes está instalado, la instalación terminará con error.

Dependencias del paquete de instalación

El agente Linux utiliza el gestor de paquetes de la distribución para descargar todas las dependencias que no estén satisfechas. De forma general, los paquetes necesarios son:

- **Libcurl:** para distribuciones basadas en Debian consulta [Librerías libcurl](#)
- **OpenSSL**
- **Gcc y las utilidades de compilación:** `make` y `makeconfig` solo en Fedora.



El proceso de instalación en Fedora incluye la compilación de los módulos necesarios para el buen funcionamiento del agente Advanced EDR.

Para mostrar las dependencias del agente ejecuta los comandos mostrados a continuación en una terminal según la distribución de destino:

- Para distribuciones basadas en Debian: `dpkg --info paquete.deb`
- Para distribuciones basadas en Fedora: `rpm --qRp paquete.rpm`

Librerías libcurl

El módulo de la protección requiere la instalación de las librerías `libcurl3` o `libcurl4` de 32 bits. Si tienes ya instalada una de estas librerías para 64 bits comprueba que el gestor de paquetes descarga la misma librería (`libcurl3` o `libcurl4`) con la misma versión pero para la arquitectura 32 bits. De no ser así Advanced EDR no se ejecutará correctamente el equipo y será necesario instalar la librería apropiada de forma manual.

Por ejemplo, si en tu equipo tienes instalada la librería `libcurl3 x.y.z` para 64 bits, el gestor de paquetes deberá descargar la librería `libcurl3 x.y.z` para 32 bits y no la `libcurl4 x.y.z` para 32 bits.

Kernels soportados

Fecha de actualización: Tuesday, April 22, 2025

Para más información sobre las distribuciones y kernels soportados en Linux, consulta: [Kernels soportados](#).

Puertos locales y acceso a URLs

Puertos locales

Para poder implementar ciertas funciones, el software de seguridad instalado en los equipos de la red utiliza los puertos de escucha mostrados a continuación:

Windows

- **TCP 18226:** equipos con el rol caché en todas las interfaces de red. Consulta [Rol de caché](#) en la página [274](#).
- **TCP 21226:** equipos con el rol de caché para recoger peticiones de ficheros a enviar en todas las interfaces de red. Consulta [Rol de caché](#) en la página [274](#).
- **TCP 3128:** equipos con el rol de proxy en todas las interfaces de red. Consulta [Rol de Proxy Cytomic](#) en la página [272](#).
- **UDP 21226:** equipos con el rol de descubridor en todas las interfaces de red. Consulta [Rol de descubridor](#) en la página [276](#).
- **TCP 33000:** equipos que inician una conexión VPN con Firebox en todas las interfaces de red, y comunicación entre los equipos. Consulta [Control de acceso a redes](#) en la página [282](#) y [Configuración de Control de Acceso a Endpoints](#) en la página [458](#).
- **UDP 35621:** módulo de protección en la interfaz localhost.

Linux

- **UDP 21226:** equipos con el rol de descubridor en todas las interfaces de red. Consulta [Rol de descubridor](#) en la página [276](#).
- **TCP 4575:** módulo de protección en la interfaz localhost.
- **TCP 8310:** módulo de protección en la interfaz localhost.
- **TCP 5560:** comunicación interna de procesos en la interfaz localhost.
- **TCP 33000:** equipos que inician una conexión VPN con Firebox en todas las interfaces de red, y comunicación entre los equipos. Consulta [Control de acceso a redes](#) en la página [282](#) y [Configuración de Control de Acceso a Endpoints](#) en la página [458](#).

macOS

- **UDP 21226:** equipos con el rol de descubridor en todas las interfaces de red. Consulta [Rol de descubridor](#) en la página [276](#).
- **TCP 33000:** equipos que inician una conexión VPN con Firebox en todas las interfaces de red. Consulta [Control de acceso a redes](#) en la página [282](#).
- **TCP 4575:** módulo de protección en la interfaz localhost.
- **TCP 8310:** módulo de protección en la interfaz localhost.

- **TCP 5560:** comunicación interna de procesos en la interfaz localhost.
- **TCP 33000:** equipos que inician una conexión VPN con Firebox en todas las interfaces de red, y comunicación entre los equipos. Consulta **Control de acceso a redes** en la página **282** y **Configuración de Control de Acceso a Endpoints** en la página **458**.

Acceso a la consola web

La consola de administración es accesible con la última versión de los navegadores compatibles mostrados a continuación:

- Chrome
- Microsoft Edge
- Firefox
- Opera

Acceso a URLs del servicio

Para el correcto funcionamiento de Advanced EDR es necesario que las URL mostradas a continuación sean accesibles desde los equipos protegidos de la red.

Nombre de producto	URLs
Advanced EDR	• https://*.pandasecurity.com • Descarga de instaladores, desinstalador genérico y políticas. • Comunicaciones de agente (registro, configuración, tareas, acciones, estados comunicación en tiempo real). • Comunicaciones de protección con Inteligencia colectiva. • http://*.pandasecurity.com • Descarga de ficheros de firmas. • https://*.windows.net Urls para el envío de ficheros desconocidos: • cmg-fusmb.pandasecurity.com • cmp-fusmb.pandasecurity.com • cpg-fusmb.pandasecurity.com • cpp-fusmb.pandasecurity.com • cpqi-fusmb.pandasecurity.com • cppl-fusmb.pandasecurity.com

Nombre de producto	URLs
	• cppe-fusmb.pandasecurity.com • rpuws.pandasecurity.com
Certificados raiz	• http://*.globalsign.com • http://*.digicert.com • http://*.sectigo.com
Cytomic Data Watch	• https://pandasecurity.devo.com
Cytomic Orion	Para poder ejecutar acciones de resolución desde Cytomic Orion es necesario abrir las siguientes URLs en el cortafuegos local del equipo si es de otro fabricante distinto de Cytomic: • dir.rc.pandasecurity.com por los puertos 8080 y 443. • eu01.rc.pandasecurity.com por los puertos 8080 y 443. • eu02.rc.pandasecurity.com por los puertos 8080 y 443. • eu03.rc.pandasecurity.com por los puertos 8080 y 443. • eu04.rc.pandasecurity.com por los puertos 8080 y 443. • eu05.rc.pandasecurity.com por los puertos 8080 y 443. • eu06.rc.pandasecurity.com por los puertos 8080 y 443. • ams01.rc.pandasecurity.com por los puertos 8080 y 443. • ams02.rc.pandasecurity.com por los puertos 8080 y 443.
Testeo de la actividad	Para versiones de protección Windows superiores a 8.00.16 • http://proinfo.pandasoftware.com/connectiontest.html Para el test de conectividad. • http://*.pandasoftware.com
Protección contra ataques de red	• https://cpg-nap.pandasecurity.com/nap/buffer • https://cpp-nap.pandasecurity.com/nap/buffer
MITRE	• Windows: cpp-fuelg.pandasecurity.com

Nombre de producto	URLs
	• Linux: cppl-fuelg.pandasecurity.com • Mac: cppi-fuelg.pandasecurity.com • cppe-fuelg.pandasecurity.com • cpg-fuelg.pandasecurity.com

Tabla 28.18: URLs de acceso al servicio

Acceso a URLs para la descarga de parches y actualizaciones (Cytomic Patch)

Consulta la página de soporte <https://www.pandasecurity.com/spain/support/card?id=700044> para obtener un listado completo de las urls accesibles desde los equipos de la red que recibirán los parches o desde los equipos con rol de caché .

Capítulo 29

Formato de los eventos recogidos en la telemetría

Advanced EDR monitoriza los procesos ejecutados en los equipos de los clientes y envía a la nube de Cytomic la telemetría que generan. Allí, queda a disposición de un grupo de analistas especializados en tarea de hunting para detectar indicadores de ataque (IOAs) producidos en la infraestructura informática de los clientes.

La telemetría se almacena utilizando un formato estructurado, que recibe el nombre de “evento”, y que está formado por diversos campos. Para interpretar correctamente la información de cada evento, es necesario comprender el significado de cada uno de los campos.

La información del evento que desencadenó el IOA se encuentra en la ventana **Detalle del evento**, y se muestra en formato JSON, así como en las gráficas de ataque. Consulta [Configuración de indicadores de ataque](#) en la página [553](#) para obtener más información acerca del módulo de detección de IOAs.

También es posible acceder a la telemetría completa generada por los equipos en la pestaña **Investigación** de los detalles del equipo. Consulta [Sección Investigación \(5\)](#) en la página [238](#).

Para conocer todos los tipos de eventos, consulta [Campos de los eventos recibidos en Cytomic Orion](#).

Glosario

A

Adaptador de red

Hardware que permite la comunicación entre diferentes equipos conectados a través de una red de datos. Un equipo puede tener más de un adaptador de red instalado y es identificado en el sistema mediante un número de identificación único.

Adware

Programa que una vez instalado o mientras se está instalando, ejecuta, muestra o descarga automáticamente publicidad en el equipo.

Agente Cytomic

Uno de los dos módulos del software de cliente Advanced EDR . Se encarga de las comunicaciones entre los equipos de la red y los servidores en la nube de Cytomic, además de gestionar los procesos locales.

Alerta

Ver Incidencia.

Análisis forense

Conjunto de técnicas y procesos ejecutados por el administrador de la red con herramientas especializadas para seguir la ejecución de un programa malicioso y determinar las consecuencias de la infección.

Análisis heurístico

Análisis estático formado por un conjunto de técnicas que inspeccionan de forma estática los ficheros potencialmente peligrosos. Este tipo de análisis se realiza en base a cientos de características que ayudan a determinar la probabilidad de que el fichero pueda llevar a cabo acciones maliciosas o dañinas cuando se ejecute en el equipo del usuario.

Anti-tamper

Conjunto de tecnologías que evitan la manipulación de los procesos de Advanced EDR por parte de amenazas avanzadas y APT que buscan sortear las capacidades de protección de la herramienta de seguridad instalada.

APT (Advanced Persistent Threat)

Conjunto de estrategias emprendidas por hackers orientadas a infectar la red del cliente, utilizando múltiples vectores de infección de forma simultánea para pasar inadvertidos a los antivirus tradicionales durante largos periodos de tiempo. Su objetivo principal es económico (robo de información confidencial de la empresa para chantaje, robo de propiedad intelectual etc.).

Árbol de carpetas

Estructura jerárquica formada por agrupaciones estáticas, utilizada para organizar el parque de equipos y facilitar la asignación de configuraciones.

Árbol de filtros

Colección de filtros agrupados en carpetas que facilitan la organización del parque de equipos y la asignación de configuraciones.

Archivo de identificadores / fichero de firmas

Fichero que contiene los patrones que el antivirus utiliza para detectar las amenazas.

Asignación automática de configuraciones

Ver Herencia.

Asignación indirecta de configuraciones

Ver Herencia.

Asignación manual de configuraciones

Asignación de una configuración a un grupo de forma directa, en contraposición al establecimiento de configuraciones automático o indirecto, que utiliza el recurso de la herencia para fijar configuraciones sin intervención del administrador.

ASLR (Address Space Layout Randomization)

Técnica implementada por el sistema operativo para mitigar los efectos de ataques de tipo exploit basados en desbordamiento de buffer.

Mediante ASLR el sistema operativo introduce aleatoriedad a la hora de asignar direcciones de memoria para reservar espacio destinado a la pila, el heap y las librerías cargadas por los procesos. De esta forma, se dificulta la utilización ilegítima de llamadas a funciones del sistema por desconocer la dirección física de memoria donde residen.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

Conjunto de recursos desarrollados por la empresa Mitre Corp. para describir y categorizar los comportamientos peligrosos de los ciberdelincuentes, basados en observaciones a lo largo de todo el mundo. ATT&CK es una lista ordenada de comportamientos conocidos

de los atacantes, separados en tácticas y técnicas, y que se expresan a través de una matriz. Ya que esta lista es una representación completa de los comportamientos que los hackers reproducen cuando se infiltran en las redes de las empresas, es un recurso útil para desarrollar mecanismos tanto defensivos como preventivos y resolutivos por parte de las organizaciones. Consulta Mitre corp..

Audit

Modo de configuración de para visualizar la actividad de los procesos ejecutados en los equipos protegidos de la red sin desencadenar ninguna acción de protección (desinfección o bloqueo).

B

Backup

Área de almacenamiento de ficheros maliciosos no desinfectables, así como de spyware y herramientas de hacking detectadas. Todos los programas eliminados del sistema por ser clasificados como amenazas se copian de forma temporal en el área de backup / cuarentena durante un periodo de entre 7 y 30 días según su tipo.

BitLocker

Software instalado en algunas versiones de los equipos Windows 7 y superiores encargado de gestionar el cifrado y descifrado de los datos almacenados en los volúmenes del equipo y utilizado por Cytomic Encryption.

Bloquear

Acción de que impide la ejecución de los programas instalados en el equipo del usuario debido a uno de los motivos siguientes: Programas clasificados como amenaza. Programas desconocidos para y la política

de protección avanzada esta configurada como lock o como hardening y su origen es no confiable. Programas bloqueados por políticas establecidas por el administrador.

C

Caché (rol)

Equipos que descargan y almacenan de forma automática todos los ficheros necesarios para que otros equipos con Advanced EDR instalado puedan actualizar el archivo de identificadores, el agente y el motor de protección sin necesidad de acceder a Internet. De esta manera se produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada.

Cambio de comportamiento

Al clasificar como malware o goodware un programa que el administrador permitió su ejecución cuando todavía era desconocido, se puede comportar de dos maneras: Eliminarlo de la lista de Programas permitidos: si se ha clasificado como goodware seguirá pudiéndose ejecutar, si se ha clasificado como malware, se impedirá su ejecución. Mantener en la lista de Programas permitidos: se seguirá permitiendo su ejecución independientemente de que se trate de malware o goodware.

Ciclo de protección adaptativa

Nuevo enfoque de seguridad basado en la integración de un conjunto de servicios de protección, detección, monitorización, análisis forense y resolución, todos ellos centralizados en una única consola de administración accesible desde cualquier lugar y en cualquier momento.

Ciclo de vida del malware

Detalle de todas las acciones desencadenadas por un programa malicioso, desde que fue visto por primera vez en un equipo del cliente hasta su clasificación como malware y posterior desinfección.

CKC (Cyber Kill Chain)

La empresa Lockheed-Martin describió en 2011 un marco o modelo para defender las redes informáticas, en el que se afirmaba que los ciberataques ocurren en fases y cada una de ellas puede ser interrumpida a través de controles establecidos. Desde entonces, la Cyber Kill Chain ha sido adoptada por organizaciones de seguridad de datos para definir las fases de los ciberataques. Estas fases abarcan desde el reconocimiento remoto de los activos del objetivo hasta la exfiltración de datos.

Clave de recuperación

Cuando se detecta una situación anómala en un equipo protegido con Cytomic Encryption o en el caso de que hayamos olvidado la contraseña de desbloqueo, el sistema pedirá una clave de recuperación de 48 dígitos. Esta clave se gestiona desde la consola de administración y debe ser introducida para completar el inicio del equipo. Cada volumen cifrado tendrá su propia clave de recuperación independiente.

Configuración

Ver Perfil de configuración.

Consola Web

Herramienta de gestión del servicio de seguridad avanzada Advanced EDR, accesible desde cualquier lugar y en cualquier momento mediante un navegador web compatible. Con la consola web el administrador

puede desplegar el software de protección, establecer las configuraciones de seguridad y visualizar el estado de la protección. También permite utilizar herramientas de análisis forense que establecen el alcance de los problemas de seguridad.

Cuarentena

Ver Backup.

Cuenta de usuario

Ver Usuario (consola).

CVE (Common Vulnerabilities and Exposures)

Lista de información definida y mantenida por The MITRE Corporation sobre vulnerabilidades conocidas de seguridad. Cada referencia tiene un número de identificación único, ofreciendo una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

D

DEP

Característica de los sistemas operativos que impide la ejecución de páginas de memoria destinadas a datos y marcadas como no ejecutables. Esta característica se diseñó para prevenir la explotación de fallos por desbordamiento de buffer.

Desbloqueo (programa)

Programas inicialmente bloqueados por no haber obtenido todavía una clasificación, pero que el administrador de la red permite su ejecución de forma selectiva y temporal para minimizar las molestias a los usuarios de la red.

Desbordamiento de buffer

Fallo en la gestión de los buffers de entrada de un proceso. En estos casos, si el volumen de datos recibido es mayor que el tamaño del buffer reservado, los datos sobrantes no se descartan, sino que se escriben en zonas de memoria adyacentes al buffer. Estas zonas de memoria pueden ser interpretadas como código ejecutable en sistemas anteriores a la aparición de la tecnología DEP.

Descubridor (rol)

Equipos capaces descubrir puestos de usuario y servidores no administrados para iniciar una instalación remota del agente Advanced EDR.

Desinfectable

Fichero infectado por malware del cual se conoce el algoritmo necesario para poder revertirlo a su estado original.

DHCP

Servicio que asigna direcciones IP a los nuevos equipos conectados a la red.

Dialer

Programa que marca un número de tarificación adicional (NTA), utilizando para ello el módem. Los NTA son números cuyo coste es superior al de una llamada nacional.

Dirección IP

Número que identifica de manera lógica y jerárquica la interfaz de red de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP.

Dirección MAC

Identificador hexadecimal de 48 bits que corresponde de forma única a una tarjeta o interfaz de red.

Directorio Activo

Implementación propietaria de servicios LDAP (Lightweight Directory Access Protocol, Protocolo Ligero/Simplificado de Acceso a Directorios) para máquinas Microsoft Windows. Permite el acceso a un servicio de directorio para buscar información diversa en entornos de red.

Distribución Linux

Conjunto de paquetes de software y bibliotecas que conforman un sistema operativo basado en el núcleo Linux.

DNS (Domain Name System)

Servicio que traduce nombres de dominio con información de diversos tipos, generalmente direcciones IP.

Dominio

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios está centralizada en un servidor llamado Controlador Principal de Dominio (PDC) o Directorio Activo (AD).

E

Entidad

Predicado o complemento incluido en las tablas de acciones del módulo análisis forense.

Entidad (Cytomic Data Watch)

Conjunto de datos que tomados como una unidad adquieren un significado propio.

EoL (End Of Life)

Término utilizado para indicar el final del ciclo de vida de un producto. A partir de la fecha indicada el producto ya no recibirá actualizaciones ni parches que corrijan sus defectos, convirtiéndose en un objetivo claro para los hackers.

Equipos sin licencia

Equipos cuya licencia ha caducado o no ha sido posible asignar una licencia válida por haberse superado el número máximo permitido de instalaciones de la protección. Estos equipos no están protegidos, pero son visibles en la consola web de administración.

Evento

Acción relevante ejecutada por un proceso en el equipo del usuario y monitorizada por. Los eventos se envían a la nube de en tiempo real como parte del flujo de telemetría. Allí, los analistas, threat hunters y los procesos automáticos de Machine Learning los analizan en su contexto para determinar si son susceptibles de pertenecer a la cadena CKC de un ataque informático. Consulta “CKC (Cyber Kill Chain)”.

Excluido (programa)

Son programas inicialmente bloqueados por haber sido clasificados como malware o PUP, pero que el administrador de la red permite su ejecución de forma selectiva y temporal excluyéndolos del análisis.

Exploit

De forma general un exploit es una secuencia de datos especialmente diseñada para provocar un fallo controlado en la ejecución de un programa vulnerable. Después de provocar el fallo, el proceso comprometido interpretará por error parte de la secuencia de datos como

código ejecutable, desencadenando acciones peligrosas para la seguridad del equipo.

F

Filtro

Contenedor de equipos de tipo dinámico que agrupa de forma automática aquellos elementos que cumplen con todas las condiciones definidas por el administrador. Los filtros simplifican la asignación de configuraciones de seguridad y facilitan la administración de los equipos del parque informático.

FQDN (Fully Qualified Domain Name)

Es un nombre de dominio que especifica la localización de forma precisa y sin ambigüedades dentro del árbol de jerarquía del sistema de nombres DNS. El FQDN especifica todos los niveles del dominio incluyendo el nivel superior y la zona raíz (root).

G

GDPR (General Data Protection Regulation)

Normativa que regula la protección de los datos de los ciudadanos que viven en la Unión Europea. Consulta el enlace <http://www.privacy-regulation.eu/es/index.htm> para acceder al reglamento completo.

Goodware

Fichero clasificado como legítimo y seguro tras su estudio.

Grafo de actividad / grafo de ejecución

Representación visual de las acciones ejecutadas por las amenazas, poniendo énfasis en el enfoque temporal.

Grupo

Contenedor de tipo estático que agrupa a uno o más equipos de la red. La pertenencia de un equipo a un grupo se establece de forma manual. Los grupos se utilizan para simplificar la asignación de configuraciones de seguridad y para facilitar la administración de los equipos del parque informático.

Grupo de trabajo

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios residen en cada uno de los equipos de forma independiente.

H

Hardening

Modo de configuración de que bloquea los programas clasificados como malware y los ficheros desconocidos cuyo origen es una fuente no fiable: Internet. Unidades externas de almacenamiento Otros equipos de la red del cliente.

Heap Spraying

Head Spray es una técnica utilizada para facilitar la explotación de vulnerabilidades por parte de un proceso malicioso independiente. Debido a la constante mejora de los sistemas operativos, la explotación de vulnerabilidades se ha convertido es un proceso muy aleatorio. Debido a que el comienzo de la región de memoria heap de un proceso es predecible, y las posteriores reservas de espacio son secuenciales, Head Spray aporta predictibilidad a los ataques, sobrescribiendo porciones de la región de memoria heap del proceso objetivo. Estas porciones de memoria serán referenciadas más adelante por un proceso

malicioso para ejecutar el ataque. Esta técnica es muy empleada para explotar vulnerabilidades de navegadores y sus plugins correspondientes.

Herencia

Método de asignación automática de configuraciones sobre todos los grupos descendientes de un grupo padre, ahorrando tiempo de gestión. También llamado Asignación automática de configuraciones o Asignación indirecta de configuraciones.

Herramienta de hacking

Programa utilizado por hackers para causar perjuicios a los usuarios de un ordenador, pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.

Hoaxes

Falsos mensajes de alarma sobre amenazas que no existen y que llegan normalmente a través del correo electrónico.

I

Identificador

Palabra clave utilizada en las búsquedas de que permite seleccionar un tipo de entidad.

IDP (Identity Provider)

Servicio centralizado responsable de gestionar las identidades de los usuarios.

IFilter

Librería del sistema operativo que permite el acceso al contenido de ficheros ofimáticos.

Incidencia

Mensaje relativo a la protección avanzada de Advanced EDR, susceptible de requerir la intervención del administrador. Las incidencias se reciben mediante la consola de administración y el correo electrónico (alertas), y el usuario del equipo protegido mediante mensajes generados por el agente que se visualizan en el escritorio de su dispositivo.

Indexar

Proceso que analiza el contenido de los ficheros y lo almacena en una base de datos de rápido acceso para acelerar su búsqueda.

Indicador de ataque (IOA)

Es un indicio con alta probabilidad de pertenecer a un ataque informático. Por lo general, se trata de ataques en fase temprana o en fase de explotación. Estos ataques no suelen utilizar malware, ya que los atacantes suelen utilizar las propias herramientas del sistema operativo para ejecutarlos y así ocultar su actividad.

Indicador de ataque avanzado

Los indicadores de ataque avanzados son aquéllos que realizan un seguimiento detallado de las aplicaciones que se ejecutan en los equipos, para detectar comportamientos sospechosos, analizar los eventos generados por las aplicaciones y determinar si constituyen un ataque.

Indicio

Detección de una cadena de acciones anómala de los procesos que se ejecutan en los equipos del cliente. Son secuencias de acciones poco frecuentes que se analizan en detalle para determinar si pertenecen o no a la secuencia de un ataque informático. Consulta “CKC (Cyber Kill Chain)”.

Informes avanzados

Ver Adware.

Inventario

Base de datos mantenida por con los ficheros clasificados como PII encontrados en el parque informático.

IP (Internet Protocol)

Principal protocolo de comunicación en Internet para el envío y recepción de los datagramas generados en el nivel de enlace subyacente.

J

Joke

Broma con el objetivo de hacer pensar a los usuarios que han sido afectados por un virus.

L

Llave USB

Dispositivo utilizado en equipos con volúmenes cifrados que permite almacenar la clave en una memoria portátil. De esta forma, no se requiere introducir ninguna contraseña en el proceso de inicio del equipo,

aunque es necesario que el dispositivo USB que almacena la contraseña esté conectado en el equipo.

Lock

Modo de configuración de que bloquea los programas desconocidos y los ya clasificados como amenazas.

M

Machine learning

Es una rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas para capaces de generalizar comportamientos a partir de una información no estructurada suministrada en forma de ejemplos.

Malware

Término general utilizado para referirse a programas que contienen código malicioso (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecta a la seguridad e integridad de los sistemas informáticos. El malware se infiltra y daña un ordenador sin el conocimiento de su dueño, con finalidades muy diversas.

Malware freezer

Comportamiento del backup / cuarentena cuyo objetivo es evitar la pérdida de datos por falsos positivos. Todos los ficheros clasificados como malware o sospechosos son enviados a la zona de backup / cuarentena, evitando su borrado completo en previsión de un fallo en la clasificación que derive en pérdida de datos.

MD5 (Message-Digest Algorithm 5)

Algoritmo de reducción criptográfico que obtiene una firma (hash o digest) de 128 bits que representa de forma única una serie o cadena de

entrada. El hash MD5 calculado sobre un fichero sirve para su identificación unívoca o para comprobar que no fue manipulado / cambiado.

Microsoft Filter Pack

Paquete de librerías IFilter que abarca todos los formatos de fichero generados por la suite de ofimática Microsoft Office.

Mitre corp.

Empresa sin ánimo de lucro que opera en múltiples centros de investigación y desarrollo financiados con fondos federales dedicados a abordar problemas relativos a la seguridad. Ofrecen soluciones prácticas en los ámbitos de defensa e inteligencia, aviación, sistemas civiles, seguridad nacional, judicatura, salud y ciberseguridad. Son los creadores del framework ATT&CK. Consulta >ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

MyTerm

N

Normalización

En Cytomic Data Watch, es una tarea que forma parte del proceso de indexación de textos, y que consiste en eliminar todos los caracteres innecesarios (generalmente caracteres separadores o delimitadores) antes de almacenarlos en la base de datos.

Nube (Cloud Computing)

Tecnología que permite ofrecer servicios a través de Internet. En este sentido, la nube es un término que se suele utilizar como una metáfora de

Internet en ámbitos informáticos.

O

OU (Organizational Unit)

Forma jerárquica de clasificar y agrupar objetos almacenados en directorios.

P

Parche

Pequeños programas publicados por los proveedores de software que modifican sus programas corrigiendo fallos y añadiendo nuevas funcionalidades.

Partición de sistema

Zona del disco duro que permanece sin cifrar y que es necesaria para que el equipo complete correctamente el proceso de inicio en los equipos con activado.

Partner

Empresa que ofrece productos y servicios de Cytomic.

Passphrase

También llamado Enhanced PIN (PIN mejorado) o PIN extendido, es una contraseña equivalente al PIN pero que permite añadir caracteres alfanuméricos. Se aceptan letras en mayúscula y minúscula, números, espacios en blanco y símbolos.

Payload

En informática y telecomunicaciones es el conjunto de datos transmitidos útiles, que se obtienen de excluir cabeceras, información de control y

otros datos que son enviados para facilitar la entrega del mensaje. En seguridad informática referida a amenazas de tipo exploit, payload es la parte del código del malware que realiza la acción maliciosa en el sistema, como borrar los ficheros o enviar datos al exterior, frente a la parte del encargado de aprovechar una vulnerabilidad (el exploit) que permite ejecutar el payload.

PDC (Primary Domain Controller)

Es un rol adoptado por servidores en redes Microsoft de tipo Dominio, que gestiona de forma centralizada la asignación y validación de las credenciales de los usuarios para el acceso a los recursos de red. En la actualidad el Directorio Activo cumple esta función.

Perfil de configuración

Un perfil es una configuración específica de la protección o de otro aspecto del equipo administrado. Este perfil es posteriormente asignado a un grupo o grupos y aplicado a todos los equipos que lo forman.

Phishing

Intento de conseguir de forma fraudulenta información confidencial de un usuario mediante el engaño. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.

PII (Personally Identifiable Information)

Ficheros que contienen datos que pueden ser utilizados para identificar o localizar a personas concretas.

PIN (Personal Identification Number, número de identificación personal)

Secuencia de números que actúa como contraseña simple y es requerida en el inicio de un equipo que tenga un volumen cifrado. Sin el PIN la secuencia de arranque no se completa y el acceso al equipo no es posible.

Proceso comprometido

Son aquellos procesos vulnerables que han sido afectados por un exploit y pueden comprometer la seguridad del equipo de usuario.

Proceso vulnerable

Son programas que, debido a fallos de programación, no son capaces de interpretar correctamente los datos recibidos de otros procesos. Al recibir una secuencia de datos especialmente diseñada (exploit), los hackers pueden provocar un mal funcionamiento del proceso, induciendo la ejecución de código que compromete la seguridad del equipo del usuario.

Programas potencialmente no deseados (PUP)

Son programas que se introducen de forma invisible o poco clara en el equipo aprovechando la instalación de otro programa que es el que realmente el usuario desea instalar.

Protección (módulo)

Una de las dos partes que componen el software que se instala en los equipos. Contiene las tecnologías encargadas de proteger el parque informático y las herramientas de resolución para desinfectar los equipos comprometidos y determinar el alcance de los intentos de intrusión en la red del cliente.

Protección avanzada

Tecnología de monitorización continua y recogida de información de los procesos ejecutados en los equipos de la red para su posterior envío de a la nube de . Allí, se analiza mediante técnicas de Machine Learning en entornos Big Data para emitir una clasificación (goodware o malware) precisa.

Protocolo

Conjunto de normas y especificaciones utilizadas para el intercambio de datos entre ordenadores. Uno de los más habituales es el protocolo TCP-IP.

Proxy

Software que hace de intermediario de las comunicaciones establecidas entre dos equipos, un cliente situado en una red interna (por ejemplo, una intranet) y un servidor en una extranet o en internet.

Proxy (rol)

Equipo que hace la función de pasarela, conectando a otros puestos de usuario y servidores sin salida directa a Internet con la nube de Advanced EDR.

Puerto

Identificador numérico asignado a un canal de datos abierto por un proceso en un dispositivo a través del cual tienen lugar las transferencias de información (entradas / salidas) con el exterior.

Q

QR (Quick Response), código

Representación gráfica en forma de matriz de puntos que almacena de forma compacta información.

R

Reclasificación de elementos

Ver Conceptos clave.

Responsive / Adaptable (RWD, Responsive Web Design)

Conjunto de técnicas que permiten desarrollar páginas Web que se adaptan de forma automática al tamaño y resolución del dispositivo utilizado para visualizarlas.

Rol

Configuración específica de permisos que se aplica a una o más cuentas de usuario y autoriza a ver o modificar determinados recursos de la consola.

Rootkits

Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los suyos propios). Este tipo de software es utilizado para esconder evidencias y utilidades en sistemas previamente comprometidos.

ROP

ROP es una técnica de ejecución de exploits que permite a un atacante ejecutar código arbitrario en presencia de defensas como DEP o ASLR. Los ataques tradicionales basados en desbordamiento de pila consistían en sobrescribir regiones de memoria enviando bloques de datos a la

entrada de programas que no controlaban debidamente el tamaño de los datos recibidos. Estos ataques dejaron de funcionar cuando técnicas como DEP fueron implementadas de forma masiva en los sistemas operativos: en esta nueva situación el sistema operativo impide la ejecución del “código desbordado” ya que reside en regiones de memoria marcadas como de no ejecución (datos). ROP sobrescribe la pila de llamadas (call stack) de un proceso para ejecutar zonas de código del propio proceso, conocidas como “gadgets”. Así, el atacante puede “armar” un flujo de ejecución alternativo al del proceso original, formado por partes de código del proceso atacado.

S

Servicio Cytomic Data Watch

Modulo compatible con que descubre ficheros PII en la red de la empresa y monitoriza su acceso para cumplir con las regulaciones de almacenamiento de datos vigentes, tales como la GDPRP.

Servicio Cytomic Encryption

Módulo compatible con que cifra el contenido de los dispositivos de almacenamiento interno del equipo. Su objetivo es minimizar la exposición de los datos de la empresa ante la pérdida o robo, o en caso de sustitución y retirada de los dispositivos de almacenamiento sin formatear.

Servicio Cytomic Insights

Servicio avanzado de explotación del conocimiento generado en tiempo real por los productos y . Facilita el descubrimiento de amenazas desconocidas, ataques dirigidos y APTs, representando los datos de actividad de los procesos ejecutados por los usuarios y poniendo el

énfasis en los eventos relacionados con la seguridad y la extracción de información.

Servicio Cytomic Patch

Módulo compatible con Advanced EDR que parchea y actualiza los programas instalados en los equipos de usuario y servidores para eliminar las vulnerabilidades producidas por fallos de programación, minimizando así su superficie de ataque.

Servicio Cytomic SIEMConnect

Módulo compatible con que envía al servidor SIEM de la empresa toda la telemetría generada por los procesos ejecutados en los equipos de usuario y servidores.

Servidor SMTP

Servidor que utiliza el protocolo SMTP -o protocolo simple de transferencia de correo- para el intercambio de mensajes de correo electrónicos entre los equipos.

Software cliente Advanced EDR

Programa que se instala en los equipos a proteger. Se compone de dos módulos: el agente Cytomic y la protección.

Sospechoso

Programa con alta probabilidad de ser considerado malware y clasificado por el análisis heurístico. Este tipo de tecnología solo se utiliza en los análisis programados o bajo demanda lanzados desde el módulo de tareas, y nunca en el análisis en tiempo real. La razón de su uso es la menor capacidad de detección de las tareas programadas ya que el código de los programas se analiza de forma estática, sin llegar a ejecutar el programa. Consulta Análisis heurístico.

Spyware

Programa que acompaña a otro y se instala automáticamente en un ordenador (generalmente sin permiso de su propietario y sin que éste sea consciente de ello) para recoger información personal y utilizarla posteriormente.

SSL (Secure Sockets Layer)

Protocolo criptográfico diseñado para la transmisión segura de datos por red.

T

Táctica

En terminología ATT&CK, las tácticas representan el motivo u objetivo final de una técnica. Es el objetivo táctico del adversario: la razón para realizar una acción. Consulta ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

Tarea

Conjunto de acciones programadas para ejecutarse con una frecuencia y en un intervalo de tiempo configurables.

TCO (Total Cost of Ownership, Coste total de Propiedad)

Estimación financiera que mide los costes directos e indirectos de un producto o sistema

TCP (Transmission Control Protocol)

Principal protocolo del nivel de transporte dentro de la pila de protocolos de Internet, orientado a la conexión para el envío y recepción de paquetes IP.

Técnica

En terminología ATT&CK, las técnicas representan la forma o la estrategia un adversario logra un objetivo táctico. Es decir, el “cómo”. Por ejemplo, un adversario, para lograr el objetivo de acceder a algunas credenciales (táctica) realiza un volcado de las mismas (técnica). Consulta ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

Threat hunting

Conjunto de tecnologías y recursos humanos especializados que permiten detectar los movimientos laterales y otros indicadores tempranos de las amenazas, antes de que ejecuten acciones nocivas para la empresa.

Tiempo de exposición (dwell time)

Tiempo que una amenaza ha permanecido sin ser detectada en un equipo de la red.

TLS (Transport Layer Security)

Nueva versión del protocolo SSL 3.0.

Topología de red

Mapa físico o lógico de los nodos que conforman una red para comunicarse.

TPM (Trusted Platform Module, módulo de plataforma segura)

Es un chip que se incluye en algunas placas base de equipos de sobremesa, portátiles y servidores. Su principal objetivo es proteger la información sensible de los usuarios, almacenando claves y otra información utilizada en el proceso de autenticación. Además, el TPM es el responsable de detectar los cambios en la cadena de inicio del equipo,

impidiendo por ejemplo el acceso a un disco duro desde un equipo distinto al que se utilizó para su cifrado.

Trojanos

Programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad de los datos del usuario.

U

Usuario (consola)

Recurso formado por un conjunto de información que Advanced EDR utiliza para regular el acceso de los administradores a la consola web y establecer las acciones que éstos podrán realizar sobre los equipos de la red.

Usuario (red)

Personal de la empresa que utiliza equipos informáticos para desarrollar su trabajo.

V

Variable de entorno

Cadena compuesta por información del entorno, como la unidad, la ruta de acceso o el nombre de archivo, asociada a un nombre simbólico que pueda utilizar Windows. La opción Sistema del Panel de control o el comando set del símbolo del sistema permiten definir variables de entorno.

VDI (Virtual Desktop Infrastructure)

Solución de virtualización de escritorio que consiste en alojar máquinas virtuales en un centro de datos al cual los usuarios acceden desde un terminal remoto con el objetivo de centralizar y simplificar la gestión y reducir los costes de mantenimiento. Se distinguen dos grupos de entornos VDI: Persistente: el espacio de almacenamiento asignado a cada usuario se respeta entre reinicios, incluyendo el software instalado, datos y actualizaciones del sistema operativo. No persistente: el espacio de almacenamiento asignado a cada usuario se elimina cuando la instancia VDI se reinicia, restaurándose a su estado inicial y deshaciendo todos los cambios efectuados.

Vector de infección

Puerta de entrada o procedimiento utilizado por el malware para infectar el equipo del usuario. Los vectores de infección más conocidos son la navegación web, el correo electrónico y los pendrives.

Ventana de oportunidad

Tiempo que transcurre desde que el primer equipo fue infectado a nivel mundial por una muestra de malware de reciente aparición hasta su estudio e incorporación a los ficheros de firmas de los antivirus para proteger a los equipos de su infección. Durante este periodo de tiempo el malware puede infectar equipos sin que los antivirus tradicionales sean conscientes de su existencia.

Virus

Programa que se introduce en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

VPN (Virtual Private Network)

Tecnología de red que permite interconectar redes privadas (LAN) utilizando un medio público, como puede ser Internet.

W

Widget (Panel)

Panel que contiene un gráfico configurable y que representa un aspecto concreto de la seguridad de la red del cliente. El conjunto de widgets forma el dashboard o panel de control de Advanced EDR.

Z

Zero-Trust Application Service

Servicio de Advanced EDR incluido en la licencia básica que clasifica el 100% de los procesos ejecutados en los equipos de usuario y servidores para emitir una valoración sin ambigüedades (goodware o malware, sin sospechosos).

