



FICHA DE PRODUCTO

# PROTECT

Plataforma de gestión de seguridad unificada  
que proporciona una visibilidad superior de la red

**Progress. Protected.**

# ¿Qué es una consola de gestión de seguridad para endpoints?

ESET PROTECT es una consola UEM versátil, implementable en la nube o en local, que garantiza visibilidad en tiempo real de los equipos locales y externos, así como la elaboración de informes completos y gestión de la seguridad para todos los sistemas operativos.

Se trata de un panel de control único para todas las soluciones de seguridad ESET implementadas en la red. Controla las capas de prevención, detección y respuesta de endpoints en todas las plataformas, incluyendo equipos de sobremesa, servidores, máquinas virtuales e incluso dispositivos móviles gestionados.



# ESET marca la diferencia

## DE LA PREVENCIÓN A LA RESPUESTA

Una única consola, ESET PROTECT combina la gestión de múltiples soluciones de seguridad de ESET. Desde la prevención de amenazas hasta la detección y respuesta, cubre toda tu empresa de forma multicapa para obtener el mejor nivel de protección.

## SOLUCIÓN DE INCIDENTES CON UN SOLO CLIC

Desde el panel principal, un administrador de IT puede evaluar rápidamente la situación y responder a los problemas. Acciones como crear una exclusión, enviar archivos para su análisis o iniciar un análisis están disponibles con un solo clic. Las exclusiones se pueden hacer por nombre, URL, hash o combinación.

## RBAC AVANZADOS

Comenzando con el acceso protegido por MFA, la consola está equipada con un sistema avanzado de control de acceso basado en roles (RBAC). Asigna a los administradores y usuarios de la consola a subredes, grupos de objetos y define conjuntos de permisos con un gran nivel de granularidad.

## MSP COMPETENTE

Si eres un proveedor de servicios gestionados (MSP) que se ocupa de las redes de sus clientes, apreciarás las capacidades de tenencia múltiple de ESET PROTECT. Las licencias MSP se detectan automáticamente y se sincronizan con el servidor de licencias, y la consola te permite realizar acciones avanzadas como instalar/eliminar cualquier aplicación de terceros, ejecutar scripts, comandos remotos, listar procesos en ejecución, configuraciones HW, etc.

## PROBABLE Y FIABLE

ESET lleva más de 30 años en el sector de la seguridad y seguimos desarrollando nuestra tecnología para estar un paso por delante de las amenazas más recientes. Esto nos ha llevado a contar con la confianza de más de 100 millones de usuarios en todo el mundo. Nuestra tecnología es analizada constantemente y aprobada por terceros que demuestran la eficacia de nuestra propuesta para detener las últimas amenazas.

## INFORMES DINÁMICOS Y PERSONALIZADOS

ESET PROTECT proporciona más de 170 informes integrados y te permite crear informes personalizados a partir de más de 1000 puntos de datos. Esto permite a las empresas crear informes con el aspecto que deseen. Una vez creados, los informes pueden configurarse para ser generados y enviados por correo electrónico a intervalos programados.

## MARCO DE AUTOMATIZACIÓN

Los grupos dinámicos pueden organizar los ordenadores en función del estado actual del dispositivo o de los criterios de inclusión definidos. A continuación, se pueden configurar tareas para desencadenar acciones como análisis, cambios de políticas o instalaciones/desinstalaciones de software.

## SOPORTE VDI TOTALMENTE AUTOMATIZADO

Se utiliza un algoritmo de detección de hardware completo para determinar la identidad de la máquina a partir de su hardware. Esto permite la creación automática de imágenes y la clonación de entornos de hardware no persistentes. Por lo tanto, el soporte VDI de ESET no requiere ninguna interacción manual y está totalmente automatizado.

## SISTEMA DE NOTIFICACIÓN TOTALMENTE PERSONALIZABLE

El sistema de notificaciones cuenta con un editor completo que representa cómo lo verás, con el que podrás configurar las notificaciones para que te avisen con la información exacta que deseas recibir.



# Características técnicas

## UN ÚNICO PANEL DE CONTROL

Todos los productos endpoint de ESET pueden ser gestionados desde una única consola de ESET PROTECT. Esto incluye estaciones de trabajo, móviles, servidores, máquinas virtuales y los siguientes sistemas operativos: Windows, macOS, Linux y Android.

## SOPORTE PARA XDR

Para mejorar aún más el conocimiento de la situación y proporcionar visibilidad a través de tu red, ESET PROTECT trabaja junto con ESET Inspect, el componente de la plataforma ESET PROTECT que permite el uso de XDR. ESET Inspect es multiplataforma (Windows, macOS y Linux), permite la detección y corrección avanzada de amenazas y puede integrarse perfectamente con tu Centro de Operaciones de Seguridad.

## CIFRADO DE DISCO COMPLETO (FDE)

El cifrado de disco completo es propio de ESET PROTECT y gestiona el cifrado de datos en endpoints tanto de Windows como de macOS (FileVault), mejorando la seguridad de los datos y ayudando a las empresas a resolver el problema del cumplimiento de la normativa de datos.

## DEFENSA CONTRA AMENAZAS AVANZADAS

La capacidad de defensa contra amenazas avanzadas mejora en gran medida la detección de amenazas de día cero, como el ransomware, al analizar rápidamente los archivos sospechosos en la potente sandbox en la nube de ESET. Además, ejecuta una serie de análisis de malware muy completos, incluida la detección en la nube.

## INVENTARIO DE HARDWARE Y SOFTWARE

ESET PROTECT no solo informa sobre todos los programas de software instalados de una empresa, sino también sobre el hardware instalado.

## COMPLEMENTAMENTE MULTIUSUARIO

Se pueden crear múltiples usuarios y grupos de permisos para permitir el acceso a una parte limitada de la consola de ESET PROTECT. Permite racionalizar completamente las responsabilidades en los equipos de una gran empresa. Esto hace posible hacer más desde una sola ubicación al agrupar dinámicamente los equipos en función de la marca, modelo, sistema operativo, procesador, memoria RAM, espacio en disco duro y muchos más elementos.



Panel de control ESET PROTECT

## CONTROL DE POLÍTICA GRANULAR

Las empresas pueden asignar políticas múltiples al mismo equipo o grupo y anidarlas para los permisos heredados. Además, las empresas pueden configurar los ajustes de las políticas como configurables por el usuario, por lo que se puede bloquear a los usuarios finales la cantidad de ajustes que se desee.

## SOPORTE TÉCNICO SIEM Y SOC

ESET PROTECT es totalmente compatible con las herramientas SIEM y puede emitir toda la información de registro en los fácilmente reconocibles formatos JSON o LEEF, lo que permite la conexión con los Centros de Operaciones de Seguridad (SOC).

## GESTIÓN DE VULNERABILIDADES Y PARCHES

Rastrea activamente las vulnerabilidades de los sistemas operativos y las aplicaciones más utilizadas, y permite la aplicación automatizada de parches en todos los endpoints gestionados a través de ESET PROTECT.

# Casos de uso

## Implementación de VDI

### PROBLEMA

Los entornos de hardware no persistentes suelen requerir la interacción manual de un departamento de IT y crean problemas de informes y visibilidad.

### SOLUCIÓN

- ✓ Después de implementar una imagen patrón en los equipos que ya están presentes en ESET PROTECT, los equipos seguirán informando a la instancia anterior a pesar de la nueva imagen completa del sistema.
- ✓ Los sistemas que vuelven a su estado inicial de un turno de trabajo no causarán duplicados, sino que se adjuntarán en un solo registro.
- ✓ En el momento de implementar imágenes no persistentes, puedes crear una imagen que incluya el dispositivo, de forma que cada vez que se cree un nuevo equipo con otra huella de hardware, se creen automáticamente nuevos registros en ESET PROTECT.

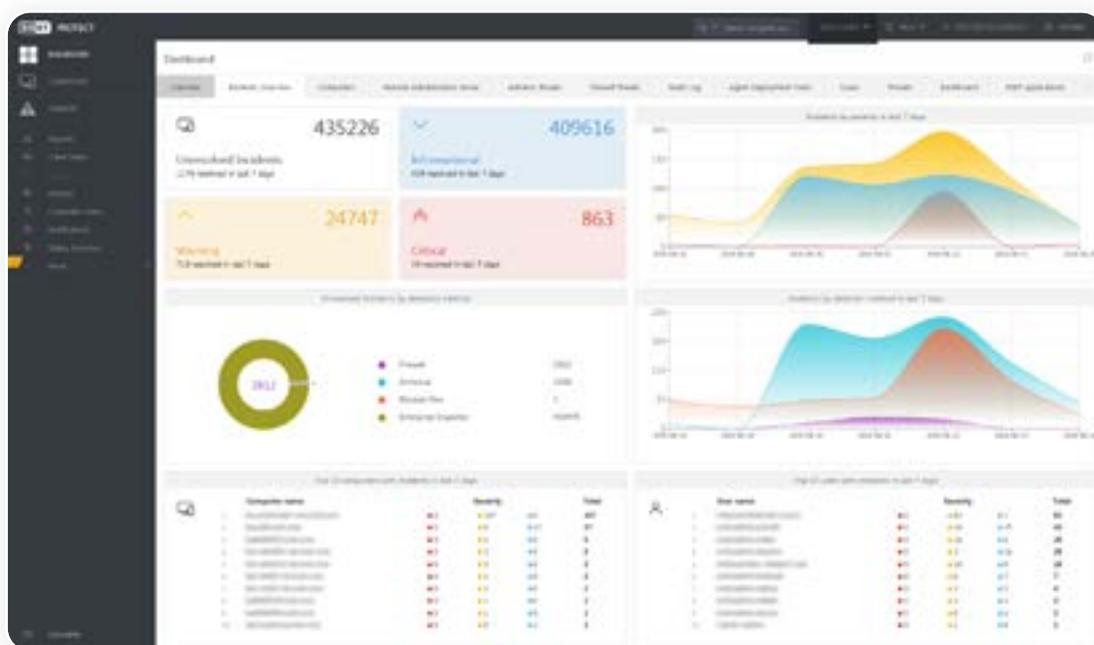
## Registro de hardware y software

### PROBLEMA

Las empresas necesitan saber cuándo se ha instalado software no autorizado y remediarlo posteriormente.

### SOLUCIÓN

- ✓ Configura un grupo dinámico dentro de ESET PROTECT para buscar software específico no deseado.
- ✓ Crea una notificación para alertar al departamento de IT cuando un ordenador cumpla este criterio.
- ✓ Configura una notificación de usuario que aparezca automáticamente en la pantalla del usuario, indicando que ha cometido una infracción de instalación de software al instalar el software en cuestión.



Panel de control ESET PROTECT: resumen de incidentes

# Ransomware

## PROBLEMA

Un usuario abre un correo electrónico malicioso que contiene un nuevo tipo de ransomware.

## SOLUCIÓN

- ✓ El departamento de IT y su SIEM reciben una notificación por correo electrónico de que se ha detectado una nueva amenaza en un determinado ordenador.
- ✓ Se inicia un análisis con un solo clic en el equipo infectado.
- ✓ El archivo se envía a ESET LiveGuard Advanced con un nuevo clic.
- ✓ Después de confirmar que la amenaza ha sido controlada, las advertencias en la consola de ESET PROTECT se borran automáticamente.

# Desarrolladores de código

## PROBLEMA

Los programadores que trabajan con código en sus ordenadores de empresa podrían crear falsos positivos debido a la compilación de software.

## SOLUCIÓN

- ✓ El departamento de IT y su SIEM reciben una notificación por correo electrónico de que se ha encontrado una nueva amenaza.
- ✓ La notificación muestra que la amenaza proviene del ordenador de un desarrollador.
- ✓ Con un clic, el archivo se envía a ESET LiveGuard Advanced para confirmar que el archivo no es malicioso.
- ✓ El departamento de IT, con un solo clic, pone una exclusión para evitar que se muestren futuros falsos positivos en esta carpeta.

# Inventario de hardware y software

## PROBLEMA

Las empresas necesitan saber qué programas están instalados en cada ordenador, así como su antigüedad.

## SOLUCIÓN

- ✓ Ver todos los programas instalados, incluido el número de versión, en el registro del ordenador.
- ✓ Consulta los detalles de hardware de cada ordenador, como dispositivo, fabricante, modelo, número de serie, procesador, RAM, espacio en disco duro y mucho más.
- ✓ Ejecuta informes para ver una visión más holística de una empresa con el fin de tomar decisiones presupuestarias sobre actualizaciones de hardware en los próximos años en función de las marcas y modelos actuales.

### CÓMO COMPRAR:

Solo tienes que adquirir cualquiera de las soluciones para empresas directamente en [nuestro sitio web](#).

### COMENZAR TUS 30 DÍAS DE PRUEBA

Obtén una versión de prueba gratuita de 30 días para probar la solución con todas sus funciones, incluida la protección de endpoints.

# Acercas de ESET

**CUANDO LA TECNOLOGÍA PERMITE EL PROGRESO, ESET® ESTÁ AQUÍ PARA PROTEGERLO.**

ESET cuenta con más de 30 años de innovación tecnológica y ofrece las soluciones de ciberseguridad más avanzadas del mercado. Nuestra moderna protección de endpoints está potenciada por las exclusivas tecnologías de seguridad multicapa ESET LiveSense®, combinadas con el uso continuo del aprendizaje automático y la tecnología en la nube. Respaldados por la mejor inteligencia e investigación de amenazas del mundo, los productos de ESET ofrecen el equilibrio perfecto de capacidades de prevención, detección y respuesta. Con una alta usabilidad y una velocidad sin precedentes, nos dedicamos a proteger el progreso de nuestros clientes, garantizando la máxima protección.

## ESET EN CIFRAS

**+110M**

de usuarios  
seguros en todo  
el mundo

**+400k**

clientes de  
empresa

**195**

países y  
territorios

**13**

centros de I+D  
en el mundo

## ALGUNOS DE NUESTROS CLIENTES



Protegido por ESET desde 2017, más de 9.000 equipos



Protegido por ESET desde 2016, más de 4.000 buzones de correo



Protegido por ESET desde 2016, más de 32.000 equipos



Distribuidor ISP desde 2008, 2 millones de clientes base

## RECONOCIMIENTO



ESET recibió el premio Business Security APPROVED de AV-Comparatives en el Business Security Test en diciembre de 2022.



ESET consigue de manera consecutiva las mejores clasificaciones en la plataforma global de revisión de usuarios G2 y sus soluciones son apreciadas por clientes de todo el mundo.



ESET ha sido reconocida como "Top Player" por cuarto año consecutivo en el Cuadrante de Mercado de Amenazas Persistentes Avanzadas 2023 de Radicati.