



FICHA DE PRODUCTO

PROTECT

Una interfaz de plataforma de gestión de seguridad unificada que ofrece una visibilidad superior de la red

Progress. Protected.

¿Qué es una consola de gestión de seguridad?

ESET PROTECT es una potente consola de gestión unificada de endpoints (UEM) que sirve de puerta de acceso a todas las capacidades de la plataforma ESET PROTECT. Accesible a través de una interfaz intuitiva y fácil de navegar, tanto en la implementación local como en la nube, ofrece visibilidad en tiempo real y un control unificado sobre todos tus endpoints, independientemente de dónde operen.

Diseñada como un auténtico «panel único», ESET PROTECT centraliza la gestión de la seguridad de ESET en todo tu entorno. Coordina las capas de prevención, detección y respuesta en ordenadores de sobremesa, servidores, máquinas virtuales, cargas de trabajo en la nube y dispositivos móviles gestionados, garantizando que cada plataforma reciba una protección coherente y completa.



ESET marca la diferencia

DE LA PREVENCIÓN A LA RESPUESTA

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

RESOLUCIÓN DE INCIDENTES CON UN SOLO CLIC

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

RBAC AVANZADO

Además del acceso protegido mediante autenticación multifactorial (MFA), la consola cuenta con un sistema avanzado de control de acceso basado en roles (RBAC). Asigna administradores y usuarios de la consola a ramas específicas de la red o a grupos de objetos, y especifica conjuntos de permisos con un alto grado de granularidad.

PREPARADO PARA MSP

Si eres un proveedor de servicios gestionados (MSP) que se encarga de las redes de tus clientes, agradecerás las capacidades completas de multitenencia de ESET PROTECT. Las licencias de MSP se detectan automáticamente y se sincronizan con el servidor de licencias, y la consola te permite realizar acciones avanzadas como instalar o eliminar cualquier aplicación de terceros, ejecutar scripts y comandos remotos, listar los procesos en ejecución, las configuraciones de hardware, etc.

COMPROBADO Y DE CONFIANZA

ESET lleva más de 30 años en el sector de la seguridad y seguimos desarrollando nuestra tecnología para ir un paso por delante de las amenazas más recientes. Esto nos ha llevado a ganarnos la confianza de más de 110 millones de usuarios en todo el mundo. Nuestra tecnología es sometida constantemente a un minucioso escrutinio y validación por parte de organismos de pruebas independientes, que demuestran la eficacia de nuestro enfoque a la hora de detener las amenazas más recientes.

INFORMES DINÁMICOS Y PERSONALIZADOS

ESET PROTECT ofrece más de 170 informes integrados y te permite crear informes personalizados a partir de más de 1.000 puntos de datos. Esto permite a las empresas crear informes con el aspecto y la estructura exactos que deseen. Una vez creados, los informes pueden configurarse para que se generen y se envíen por correo electrónico a intervalos programados.

MARCO DE AUTOMATIZACIÓN

Los grupos dinámicos pueden clasificar los ordenadores en función del estado actual del dispositivo o de criterios de inclusión definidos. A continuación, se pueden configurar tareas para que activen acciones como análisis, cambios en las políticas o instalaciones/desinstalaciones de software en función de los cambios en la pertenencia a los grupos dinámicos.

SOPORTE DE VDI TOTALMENTE AUTOMATIZADO

Se utiliza un algoritmo completo de detección de hardware para determinar la identidad del equipo en función de su hardware. Esto permite la clonación y el redespigado automatizado de imágenes en entornos de hardware no persistentes. Por lo tanto, la compatibilidad con VDI de ESET no requiere ninguna intervención manual y está totalmente automatizada.

SISTEMA DE NOTIFICACIONES TOTALMENTE PERSONALIZABLE

El sistema de notificaciones cuenta con un editor completo de tipo «lo que ves es lo que obtienes», en el que podrás configurar al detalle las notificaciones para recibir alertas sobre la información exacta que desees que se te comunique.



Características técnicas

PANEL ÚNICO DE CONTROL

Todas las soluciones de ESET para endpoint se pueden gestionar desde una única consola de ESET PROTECT. Esto incluye estaciones de trabajo, dispositivos móviles, servidores y máquinas virtuales, así como los siguientes sistemas operativos: Windows, macOS, Linux y Android.

COMPATIBILIDAD CON XDR

Para mejorar aún más la conciencia situacional y proporcionar visibilidad en toda la red, ESET PROTECT funciona conjuntamente con ESET Inspect, el componente de la plataforma ESET PROTECT que habilita la tecnología XDR. ESET Inspect es multiplataforma (Windows, macOS y Linux), permite la detección avanzada de amenazas y su corrección, y se integra a la perfección con tu centro de operaciones de seguridad.

MDM EN LA NUBE

MDM en la nube está incluido y no requiere herramientas especializadas para su funcionamiento. Es compatible con Microsoft Intune, Apple Business Manager y VMware Workspace ONE.

CIFRADO DE DISCO COMPLETO (FDE)

El cifrado completo del disco es una función nativa de ESET PROTECT, que gestiona el cifrado de datos tanto en endpoints Windows como Mac (FileVault), mejorando la seguridad de la información y ayudando a las empresas a cumplir con la normativa sobre protección de datos.

DEFENSA CONTRA AMENAZAS AVANZADAS

La compatibilidad con la defensa contra amenazas avanzadas mejora considerablemente la detección de amenazas de día cero, como el ransomware, mediante el análisis rápido de archivos sospechosos en el potente entorno de pruebas en la nube de ESET. Además, ejecuta una serie de análisis muy exhaustivos de malware, incluida la detonación en la nube. Esto te permite hacer más desde una única ubicación al agrupar dinámicamente los ordenadores en función de la marca, el modelo, el sistema operativo, el procesador, la RAM, el espacio en disco duro y muchos otros criterios.

PROTECCIÓN DE CARGAS DE TRABAJO EN LA NUBE

ESET PROTECT incluye protección integrada de cargas de trabajo en la nube que protege las máquinas virtuales en AWS, Azure y Google Cloud sin coste adicional. Reduce la superficie de ataque en la nube, mejora la visibilidad para una detección y respuesta más rápidas ante las amenazas, y unifica la gestión de la seguridad entre los endpoints y las cargas de trabajo en la nube en una única consola.

PREPARADO PARA MDR

ESET PROTECT está preparado para MDR, lo que ofrece a los clientes una vía sencilla hacia una protección experta permanente. Al habilitar el servicio de detección y respuesta gestionadas (MDR) de ESET, las empresas obtienen monitorización de amenazas las 24 horas del día, los 7 días de la semana, detección rápida y respuesta guiada o automatizada ante incidentes. Esto ayuda a prevenir filtraciones y ataques de ransomware, y garantiza que las amenazas críticas sean gestionadas rápidamente por especialistas cualificados.

INVENTARIO DE HARDWARE Y SOFTWARE

ESET PROTECT no solo genera informes sobre todas las aplicaciones de software instaladas en toda la empresa, sino que también informa sobre el hardware instalado. Esto permite una distribución eficiente de responsabilidades entre los equipos de las grandes empresas.

TOTALMENTE MULTIUSUARIO

Se pueden crear múltiples usuarios y grupos de permisos para permitir el acceso a una parte limitada de la consola de ESET PROTECT. Esto permite optimizar la distribución de responsabilidades entre los equipos de las grandes empresas.

CONTROL DETALLADO DE LAS POLÍTICAS

Las empresas pueden configurar varias políticas para un mismo ordenador o grupo y anidar políticas para heredar permisos. Además, las empresas pueden configurar los ajustes de las políticas para que sean configurables por el usuario, lo que permite restringir cualquier número de ajustes a los usuarios finales.

ACCESO REMOTO SEGURO E INTEGRADO

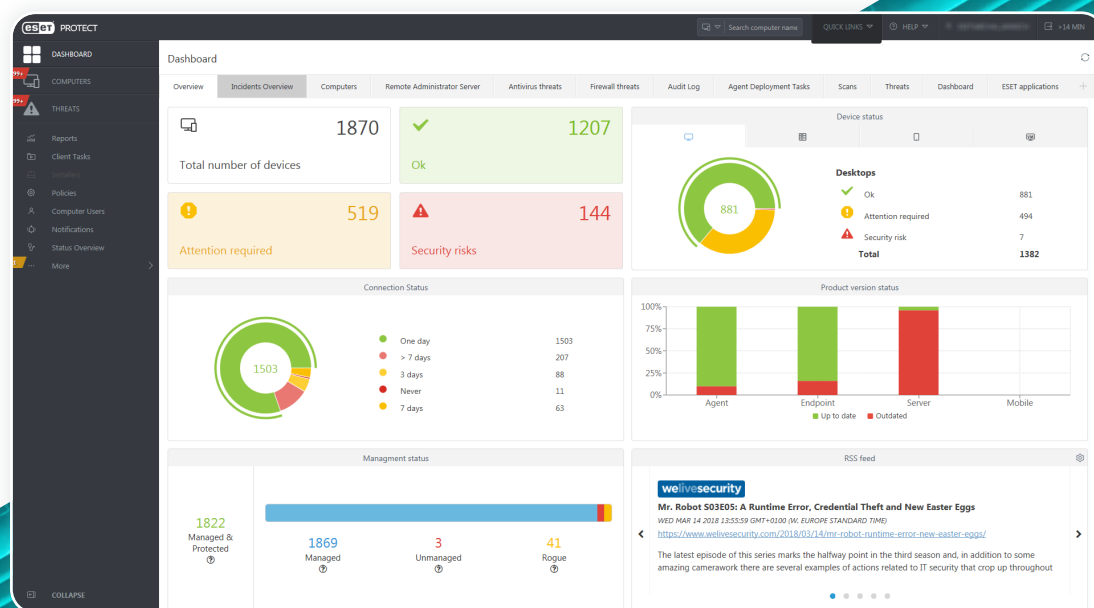
Integrado de forma nativa en el ecosistema de ESET PROTECT, ESET Remote Access permite a los administradores conectarse de forma segura y en tiempo real a múltiples dispositivos y servidores. Gestionada desde la consola en la nube de ESET PROTECT, garantiza sesiones protegidas y una conectividad fiable, incluso cuando un dispositivo está aislado de la red, lo que permite un soporte IT rápido y fluido, así como la resolución de incidencias.

INTEGRACIONES EXHAUSTIVAS

La integración con herramientas como SIEM y SOAR es posible gracias a nuestras API completas y fáciles de usar, documentadas a través de Swagger. Además, ESET PROTECT admite los formatos JSON y LEEF para toda la información de los registros.

GESTIÓN DE VULNERABILIDADES Y PARCHES DE ESET

Realiza un seguimiento activo de las vulnerabilidades en los sistemas operativos y las aplicaciones más comunes, y permite la aplicación automatizada de parches en todos los endpoints gestionados a través de ESET PROTECT.



Panel de control de ESET PROTECT

Casos de uso

Implementaciones de VDI

PROBLEMA

Los entornos de hardware no persistentes suelen requerir la intervención manual del departamento de IT y suponen un verdadero quebradero de cabeza en cuanto a la generación de informes y la visibilidad.

SOLUCIÓN

- ✓ Tras la implementación de una imagen maestra en los ordenadores que ya figuran en ESET PROTECT, estos seguirán enviando informes a la instancia anterior a pesar de que se haya realizado una reinstalación completa del sistema.
- ✓ Los equipos que vuelvan a su estado inicial al final de un turno de trabajo no provocarán la aparición de equipos duplicados, sino que se agruparán en un único registro.
- ✓ Al realizar la implementación de imágenes no persistentes, puedes crear una imagen que incluya el agente, de modo que, cada vez que se cree un nuevo equipo con otra huella de hardware, se generen automáticamente nuevos registros en ESET PROTECT.

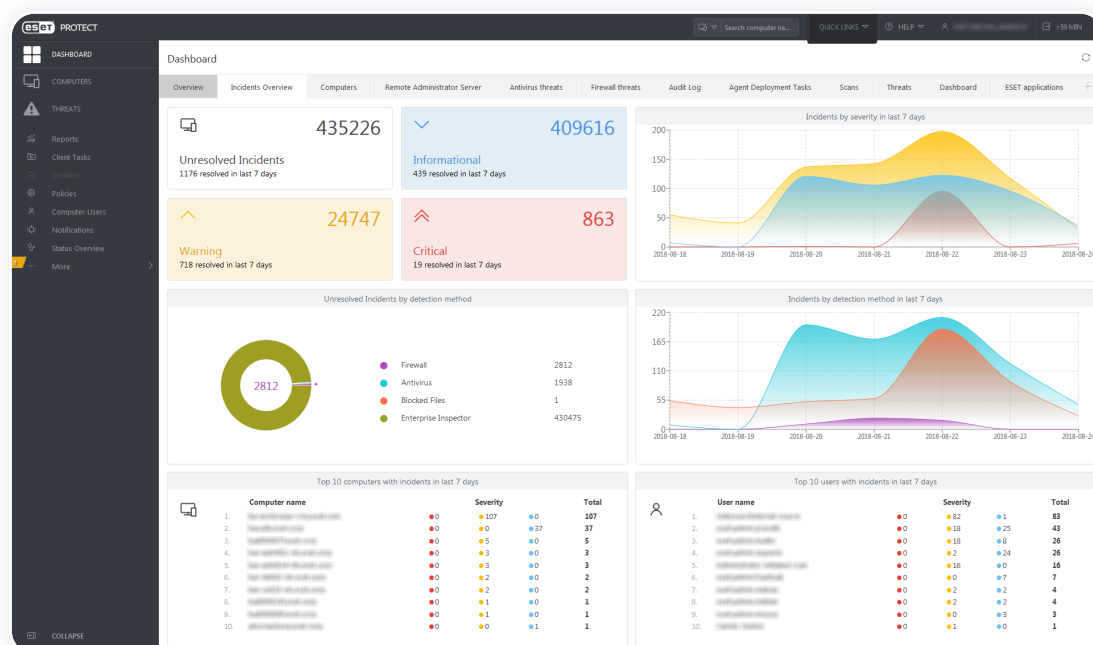
Corrección de software

PROBLEMA

Las empresas necesitan saber cuándo se ha instalado software no autorizado y subsanar la situación posteriormente.

SOLUCIÓN

- ✓ Configura un grupo dinámico en ESET PROTECT para buscar un software no deseado específico.
- ✓ Crea una notificación para alertar al departamento de IT cuando un ordenador cumpla este criterio.
- ✓ Configura una tarea de desinstalación de software en la consola de ESET PROTECT para que se ejecute automáticamente cuando un ordenador cumpla los criterios del grupo dinámico.
- ✓ Configura una notificación para el usuario que aparezca automáticamente en su pantalla, indicándole que ha cometido una infracción de instalación de software al instalar el programa en cuestión.



Panel de control de ESET PROTECT: resumen de incidentes

Ransomware

PROBLEMA

Un usuario abre un correo electrónico malicioso que contiene una nueva variante de ransomware.

SOLUCIÓN

- ✓ El departamento de IT recibe una notificación por correo electrónico y a través de su SIEM de que se ha detectado una nueva amenaza en un ordenador concreto.
- ✓ Se inicia un análisis con un solo clic en el ordenador infectado.
- ✓ El archivo se envía a ESET LiveGuard Advanced con otro clic.
- ✓ Tras confirmar que la amenaza ha sido contenida, las alertas de la consola de ESET PROTECT se borran automáticamente.

Desarrolladores de código

PROBLEMA

Los programadores que trabajan con código en sus ordenadores de trabajo pueden tender a generar falsos positivos debido a la compilación de software.

SOLUCIÓN

- ✓ El departamento de IT recibe una notificación por correo electrónico y a través de su SIEM de que se ha detectado una nueva amenaza.
- ✓ La notificación indica que la amenaza procedía del ordenador de un desarrollador.
- ✓ Con un solo clic, el archivo se envía a ESET LiveGuard Advanced para confirmar que no es malicioso.
- ✓ El departamento de IT, con un solo clic, establece una exclusión para prevenir que se muestren futuros falsos positivos en esta carpeta.

Inventario de hardware y software

PROBLEMA

Las empresas necesitan saber qué software está instalado en cada ordenador, así como la antigüedad de cada uno de ellos.

SOLUCIÓN

- ✓ Consulta todo el software instalado, incluido el número de versión, en el registro del ordenador.
- ✓ Consulta los detalles de hardware de cada ordenador, como el dispositivo, el fabricante, el modelo, el número de serie, el procesador, la memoria RAM, el espacio en el disco duro y mucho más.
- ✓ Genera informes para obtener una visión más global de la empresa, con el fin de tomar decisiones presupuestarias sobre actualizaciones de hardware en los próximos años basándose en las marcas y modelos actuales.

CÓMO COMPRAR:

Solo tienes que comprar cualquiera de las soluciones para empresas directamente desde [nuestra página web](#).

EMPIEZA AHORA TU PRUEBA DE 30 DÍAS

Activa tu prueba gratuita de 30 días para probar la solución con todas sus funciones, incluida la protección de los endpoints.

Esto es ESET

Ciberseguridad diseñada para ofrecer confianza y control

ESET ofrece soluciones de ciberseguridad diseñadas específicamente para que las empresas y los particulares puedan alcanzar la independencia digital en un mundo cada vez más impulsado por la IA.

Con sede en la Unión Europea y de propiedad privada, ESET desarrolla tecnologías propias de ciberseguridad basadas en la inteligencia artificial y modelos de IA soberanos diseñados para proteger el ecosistema digital y la infraestructura de IA.

Cada solución que crea ESET se basa en más de 35 años de experiencia en ciberseguridad, incorporando la experiencia humana, el criterio y los valores humanos a cada decisión. Combinado con un enfoque proactivo centrado en la prevención, ESET protege frente a las ciberamenazas convencionales y las impulsadas por IA. Basándose en el rigor científico y con el respaldo de 11 centros de I+D repartidos por todo el mundo, ESET impulsa continuamente la investigación y la innovación para ofrecer una ciberseguridad sencilla y siempre supervisada por expertos. Sus tecnologías son validadas de forma constante por las principales empresas de pruebas independientes.

ESET protege a millones de usuarios y empresas en 178 países. Guiada por su compromiso con una IA responsable y la confianza de los clientes, ESET protege el progreso que la tecnología hace posible.

ESET EN CIFRAS

+1.000M

de usuarios protegidos
en todo el mundo

+500k

clientes de empresa

178

países

11

centros de I+D en todo
el mundo

ALGUNOS DE NUESTROS CLIENTES



protegidos por ESET
desde 2017: más de 9.500
dispositivos



protegidos por ESET desde
2019: 1.200 dispositivos
y 2.700 buzones de correo

Canon

Canon Marketing Japan Group

protegidos por ESET desde
2016: más de 23.000
dispositivos



socio de seguridad de ISP
desde 2008: 2 millones
de clientes

RECONOCIMIENTOS



Ganador de los premios **al mejor endpoint para empresas y al mejor endpoint para pequeñas empresas** en los SE LABS Awards 2025



Nombrado **«Customers' Choice»** en el informe **«Voice of the Customer»** de Gartner® Peer Insights™ sobre plataformas de protección de endpoint de 2026

FROST & SULLIVAN

Nombrado **«líder»** en el informe «Frost Radar: Endpoint Security 2025», lo que demuestra su excelencia en crecimiento e innovación

Gartner y Peer Insights™ son marcas comerciales de Gartner, Inc. y/o sus filiales. Todos los derechos reservados. El contenido de Gartner Peer Insights consiste en las opiniones de usuarios finales individuales basadas en sus propias experiencias, y no debe interpretarse como declaraciones de hechos, ni representa las opiniones de Gartner o sus filiales. Gartner no respalda a ningún proveedor, producto o servicio representado en este contenido, ni ofrece ninguna garantía, expresa o implícita, con respecto a este contenido, sobre su exactitud o integridad, incluida cualquier garantía de comerciabilidad o idoneidad para un fin determinado.