



RESUMEN GENERAL

PROTECT

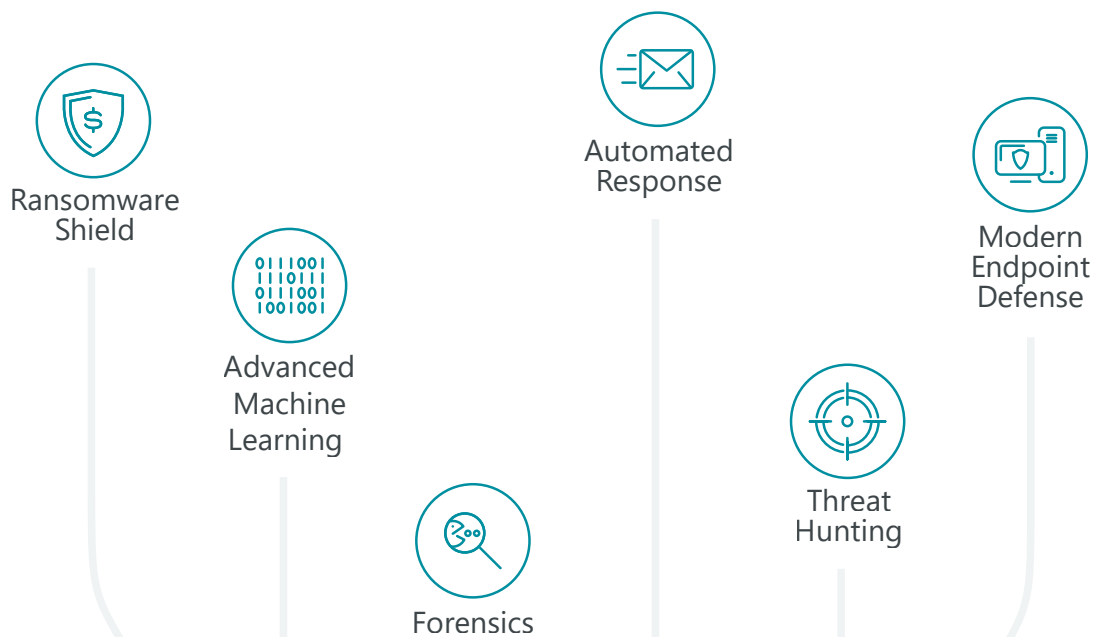
Plataforma unificada de gestión de la seguridad
que proporciona una visibilidad superior de la red

Progress. Protected.

¿Qué es una consola de administración de seguridad para endpoints?

ESET PROTECT es una versátil consola de administración unificada para endpoints que proporciona acceso a la potente plataforma ESET PROTECT. Se implementa tanto en forma local como desde la nube y asegura la visibilidad en tiempo real de las endpoints locales y externas, así como la elaboración de informes completos y la capacidad de administrar la seguridad en todos los sistemas operativos.

Muestra en una única pantalla todas las soluciones de seguridad de ESET desplegadas en la red. Controla las capas de prevención, detección y respuesta para endpoints en todas las plataformas, incluyendo los equipos de escritorio, los servidores, las máquinas virtuales e incluso los dispositivos móviles gestionados.



En qué se diferencia ESET

DE LA PREVENCIÓN A LA RESPUESTA

ESET PROTECT combina la administración de las distintas soluciones de seguridad de ESET desde una única consola. Protege su organización completa con múltiples capas de prevención, detección y respuesta ante amenazas, para ofrecer el mejor nivel de seguridad.

REMEDIACIÓN DE INCIDENTES CON UN SOLO CLIC

Desde el panel de control principal, el administrador de TI puede evaluar rápidamente la situación de seguridad y resolver problemas. Las acciones como crear una exclusión, enviar archivos para su análisis detallado o iniciar una exploración se ejecutan con un solo clic. Se pueden generar exclusiones por nombre de amenaza, dirección URL, valor de hash o una combinación de estos datos.

SISTEMA AVANZADO DE CONTROL DEL ACCESO BASADO EN ROLES

Comenzando con el acceso protegido por la autenticación en varias fases, la consola está equipada con un sistema avanzado de control de acceso basado en roles. Asigne administradores y usuarios de la consola a ramas de red o grupos de objetos determinados y especifique conjuntos de permisos con un alto nivel de granularidad.

PREPARADO PARA MSP

Si usted es un proveedor de servicios gestionados (MSP) y se ocupa de las redes de sus clientes, la funcionalidad de ESET PROTECT de admitir usuarios múltiples le será de gran utilidad. Las licencias del MSP se detectan y sincronizan automáticamente con el servidor de licencias, y la consola le permite llevar a cabo acciones avanzadas como instalar o eliminar cualquier aplicación de terceros, ejecutar scripts y comandos remotos, listar los procesos en ejecución, configurar el hardware, etc.

MARCA COMPROBADA Y DE CONFIANZA

ESET ha formado parte de la industria de seguridad por más de 30 años y continúa mejorando su tecnología para estar siempre un paso por delante de las amenazas más recientes. Esta trayectoria ha logrado que más de 110 millones de usuarios de todo el mundo confíen en nuestros productos. Nuestra tecnología es constantemente examinada y validada por evaluadores externos, que demuestran la efectividad de nuestro enfoque para detener las últimas amenazas.

INFORMES DINÁMICOS Y PERSONALIZADOS

ESET PROTECT ofrece más de 170 informes integrados y le permite crear informes personalizados a partir de más de mil puntos de datos. De esta forma, las organizaciones pueden crear informes con el aspecto exacto que desean. Una vez creados, los informes se pueden configurar para que se generen automáticamente y se envíen por correo electrónico en intervalos programados.

MARCO DE AUTOMATIZACIÓN

Los grupos dinámicos ordenan los equipos según el estado actual del dispositivo o los criterios de inclusión definidos. Se pueden configurar tareas para desencadenar acciones de exploración, modificación de políticas o instalación/desinstalación de software, tras cada cambio de membresía en el grupo dinámico.

SOPORTE PARA VDI TOTALMENTE AUTOMATIZADO

ESET emplea un algoritmo integral de detección de hardware para determinar la identidad de la máquina según su hardware. De esta forma, se pueden regenerar imágenes y clonar entornos de hardware no persistentes de manera automática. Por lo tanto, el soporte para VDI de ESET no requiere ninguna interacción manual y está totalmente automatizado.

SISTEMA DE NOTIFICACIONES COMPLETAMENTE PERSONALIZABLE

El sistema de notificaciones incluye un editor completo que le permite configurar exhaustivamente las notificaciones para recibir únicamente las alertas sobre la información que desea obtener.



Características técnicas

UNA ÚNICA PANTALLA

Todos los productos de ESET para endpoints se pueden administrar desde la misma consola de ESET PROTECT, incluyendo estaciones de trabajo, dispositivos móviles, servidores y máquinas virtuales, con los siguientes sistemas operativos: Windows, macOS, Linux y Android.

SOPORTE PARA XDR

Para mejorar aún más el conocimiento de la situación y obtener visibilidad en la red, ESET PROTECT trabaja a la par de ESET Inspect, el componente responsable de la detección y respuesta ampliada (XDR). ESET Inspect es multiplataforma (Windows, macOS y Linux), permite la cacería y remediación avanzadas de amenazas, y se integra sin problemas con su centro de operaciones de seguridad.

CIFRADO DE DISCO COMPLETO

El Cifrado de disco completo está integrado en forma nativa en ESET PROTECT: administra el cifrado de datos en endpoints Windows y Mac (FileVault), mejora la seguridad de los datos y ayuda a las empresas a cumplir con las reglamentaciones sobre protección de datos.

DEFENSA AVANZADA CONTRA AMENAZAS

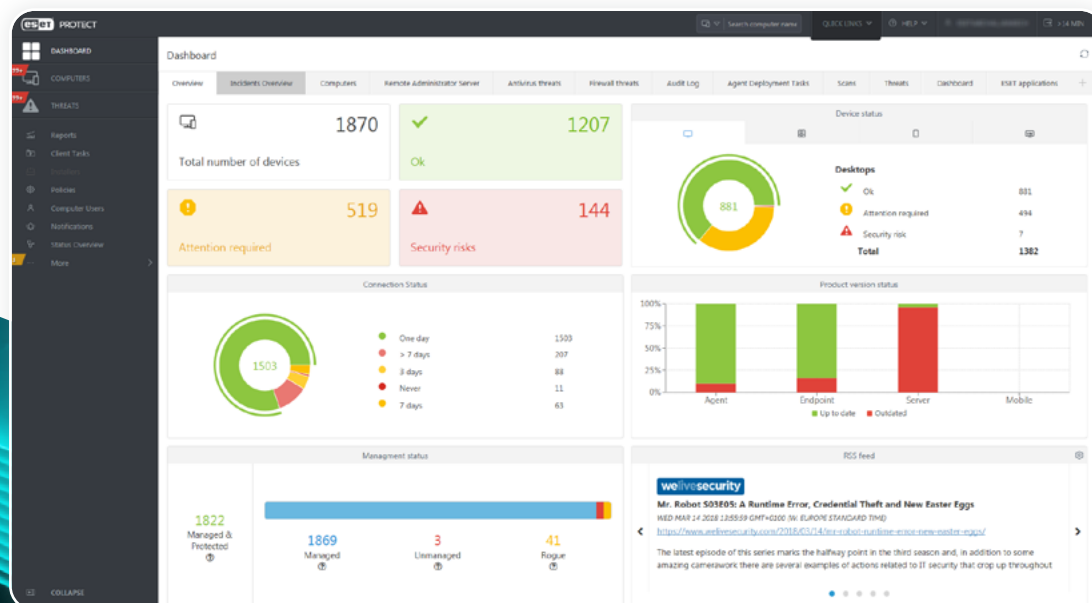
La compatibilidad con la defensa avanzada de amenazas mejora en gran medida la detección de amenazas 0-day como el ransomware, ya que analiza rápidamente los archivos sospechosos en un potente espacio aislado en la nube de ESET (modo sandbox). Además, ejecuta un conjunto muy completo de análisis de malware, incluyendo la detonación en la nube.

INVENTARIO DE HARDWARE Y SOFTWARE

ESET PROTECT no solo le brinda información sobre todas las aplicaciones de software instaladas en la organización, sino también sobre el hardware instalado.

ADMINISTRACIÓN MULTIUSUARIO

La posibilidad de crear usuarios y grupos de permisos múltiples limita el acceso a ciertos sectores de la consola de ESET PROTECT. De esta forma, se simplifican radicalmente las responsabilidades en los grandes equipos de trabajo corporativos. Esto le permite hacer más cosas desde una misma ubicación, por ejemplo, agrupar dinámicamente los equipos según la marca, el modelo, el sistema operativo, el procesador, la memoria RAM, el espacio en disco rígido y muchos otros elementos.



Panel de control de ESET PROTECT

CONTROL GRANULAR DE POLÍTICAS

Las organizaciones pueden establecer múltiples políticas para un mismo equipo o grupo, y anidar políticas para permisos heredados. Además, permite ajustar las políticas configuradas por el usuario, de modo que podrá bloquear las configuraciones que desee de los usuarios finales.

SOPORTE PARA SIEM Y SOC

ESET PROTECT es totalmente compatible con las herramientas SIEM y puede generar toda la información de registro en los formatos JSON o LEEF, de uso muy extendido, lo que admite la integración con los centros de operaciones de seguridad.

GESTIÓN DE VULNERABILIDADES Y PARCHES DE ESET

Rastrea activamente las vulnerabilidades de los sistemas operativos y las aplicaciones comunes, y permite la aplicación automática de parches en todas las endpoints gestionadas a través de ESET PROTECT.

Casos de uso

Implementaciones de VDI

PROBLEMA

Los entornos de hardware no persistentes normalmente requieren la interacción manual del departamento de TI, con lo que los informes y la visibilidad se convierten en una pesadilla.

SOLUCIÓN

- ✓ Tras implementar una imagen maestra en las computadoras ya presentes en ESET PROTECT, los equipos continuarán informando a la instancia anterior a pesar de la existencia de una nueva imagen completa del sistema.
- ✓ Las máquinas que regresan a su estado inicial una vez terminado el turno de trabajo no generarán máquinas duplicadas; en su lugar, se combinarán en un mismo registro.
- ✓ Al implementar imágenes no persistentes, puede crear una imagen que incluya el agente; de esta forma, cada vez que se cree una nueva máquina con otra huella digital de hardware, se crearán automáticamente nuevos registros en ESET PROTECT.

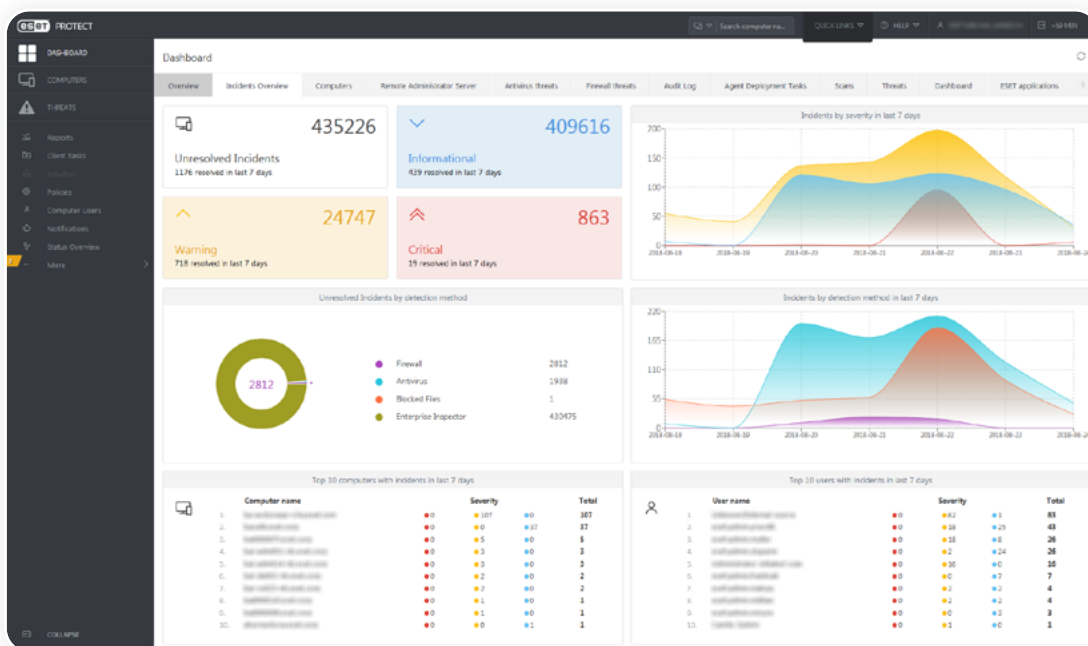
Remediación de software

PROBLEMA

Las organizaciones necesitan saber si se instala un software no permitido y deben poder solucionar el problema.

SOLUCIÓN

- ✓ Configure un grupo dinámico en ESET PROTECT para detectar un software específico no deseado.
- ✓ Cree una notificación para alertar al departamento de TI cada vez que una computadora cumpla con dicho criterio.
- ✓ Configure una tarea de desinstalación de software en ESET PROTECT para que se ejecute automáticamente cada vez que un equipo cumpla con los criterios del grupo dinámico.
- ✓ Configure una notificación que aparezca automáticamente en la pantalla del usuario para indicar que cometió una violación de las políticas corporativas por haber instalado software no permitido.



Panel de control de ESET PROTECT: información general sobre incidentes

Ransomware

PROBLEMA

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

SOLUCIÓN

- ✓ El departamento de TI recibe una notificación por correo electrónico y a través de su herramienta SIEM indicando que se detectó una nueva amenaza en una computadora determinada.
- ✓ Con un solo clic, se inicia una exploración en la computadora infectada.
- ✓ El archivo se envía a ESET LiveGuard Advanced con otro clic.
- ✓ Tras confirmar que la amenaza está contenida, las advertencias en la consola de ESET PROTECT se borran automáticamente.

Desarrolladores de código

PROBLEMA

Los programadores que trabajan con código en su computadora laboral muchas veces generan falsos positivos durante la compilación de software.

SOLUCIÓN

- ✓ El departamento de TI recibe una notificación por correo electrónico y a través de su herramienta SIEM indicando que se detectó una nueva amenaza.
- ✓ La notificación muestra que la amenaza provino de la computadora de un desarrollador.
- ✓ Con un solo clic, el archivo se envía a ESET LiveGuard Advanced para confirmar que no es malicioso.
- ✓ El departamento de TI, con un solo clic, genera una exclusión para evitar que se muestren falsos positivos en esta carpeta.

Inventario de hardware y software

PROBLEMA

Las organizaciones necesitan saber qué software está instalado en cada equipo, así como la antigüedad de cada equipo.

SOLUCIÓN

- ✓ Vea todas las aplicaciones de software instaladas (incluyendo el número de versión) en el registro de equipos.
- ✓ Vea los detalles de hardware de cada equipo, como dispositivo, fabricante, modelo, número de serie, procesador, RAM, espacio en disco rígido y más.
- ✓ Cree informes y manténgase al día con el panorama integral de la empresa para poder tomar decisiones presupuestarias sobre las actualizaciones de hardware que deberá hacer en los próximos años en función de las marcas y los modelos actuales.

CÓMO COMPRAR:

Simplemente compre cualquiera de las soluciones corporativas directamente desde [nuestro sitio web exclusivo](#).

COMIENZE AHORA SU PRUEBA DE 30 DÍAS

Desbloquee su prueba gratuita de 30 días con todas las funcionalidades del producto, incluyendo la protección para endpoints.

Acercas de ESET

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

ESET aporta más de 30 años de innovación impulsada por la tecnología y ofrece las soluciones de ciberseguridad más avanzadas del mercado. Nuestra moderna protección para endpoints se basa en las exclusivas tecnologías de seguridad multicapa ESET LiveSense®, combinadas con el uso continuo del aprendizaje automático y la computación en la nube. Gracias al respaldo de la mejor inteligencia e investigación sobre amenazas del mundo, los productos de ESET ofrecen el equilibrio perfecto entre capacidades de prevención, detección y respuesta. Con una gran facilidad de uso y una velocidad insuperable, nos dedicamos a proteger el progreso de nuestros clientes, garantizando la máxima seguridad.

ESET EN NÚMEROS

**MÁS DE 1000
MILLONES**

de usuarios de
Internet protegidos

**MÁS DE
400 MIL**

clientes
corporativos

195

países y
territorios

13

centros de
investigación
y desarrollo
mundiales

ALGUNOS DE NUESTROS CLIENTES



protegido por ESET desde
2017 más de 9.000 endpoints



protegido por ESET desde
2016 más de 4.000 buzones
de correo



protegido por ESET desde
2016 más de 32.000
endpoints



partner de seguridad ISP
desde 2008
base de clientes de 2 millones

RECONOCIMIENTOS



ESET recibió el premio Business Security APPROVED en las Pruebas de seguridad para empresas realizadas en diciembre de 2022 por AV-Comparatives.



ESET obtiene sistemáticamente las mejores clasificaciones en la plataforma global de reseñas de usuarios G2 y sus soluciones son valoradas por clientes de todo el mundo.



ESET recibió la mención Top Player por cuarto año consecutivo en el Cuadrante de Mercado de Radicati para la Protección frente a Amenazas Persistentes Avanzadas de 2023.