INFORMACIÓN DE PRODUCTO

PROTECT

Plataforma de gestión de seguridad unificada que brinda una visibilidad superior de la red.

Progress. Protected

¿Qué es la **consola de gestión de seguridad para endpoints?**

ESET PROTECT es una consola UEM versátil, que se puede implementar las instalaciones o a través de la nube, y que garantiza la visibilidad en tiempo real de todas las endpoints, así como la gestión completa de informes y seguridad para 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).

¿Por qué es importante la **consola**?

VISIBILIDAD

Las amenazas persistentes avanzadas, 0-day, los ataques dirigidos y las botnets son algunos de los principales motivos de preocupación para las industrias de todo el mundo. Es indispensable tener visibilidad en tiempo real para que el equipo de TI pueda reaccionar con rapidez y mitigar cualquier riesgo generado. Por la creciente tendencia de las empresas a incorporar trabajadores móviles, la visibilidad también es necesaria fuera de la empresa.

ESET PROTECT brinda información actualizada para que el personal de TI conozca el estado de todas las endpoints, ya sean locales o externas. También proporciona visibilidad de todos los SO que puede llegar a tener una empresa. En la mayoría de los casos, también se incluye información sobre el dispositivo (como el inventario de hardware o software) para mejorar aún más la visibilidad y asegurar un conocimiento completo del entorno.

ADMINISTRACIÓN

El panorama actual de seguridad cibernética está en constante evolución, y sigue incorporando nuevos métodos de ataque y amenazas. Cuando se produce un ataque o una vulneración de datos, las organizaciones suelen mostrarse sorprendidas o directamente ignoran por completo la existencia de la amenaza. Una vez descubierto el ataque, las organizaciones en general ejecutan tareas específicas en los dispositivos, como las exploraciones. Esto a veces ocasiona que cambien radicalmente sus políticas de configuración para estar mejor protegidas ante amenazas futuras.

ESET PROTECT ofrece políticas predefinidas que permite a las organizaciones ajustar las configuraciones de los productos de seguridad en las endpoints cuando lo deseen. Asimismo, permite automatizar tareas, por lo que los administradores de TI ya no necesitarán ejecutarlas manualmente en cada equipo.

ELABORACIÓN DE INFORMES

Además de tener que cumplir con las normativas vigentes sobre la seguridad de los datos, la mayoría de las organizaciones cuentan con requisitos internos en lo que respecta a los informes. Independientemente de la organización, siempre habrá informes que se deben generar en intervalos programados y entregar a las partes pertinentes, o almacenar para uso futuro.

ESET PROTECT elabora informes en intervalos programados y los guarda en carpetas específicas, o los envía por correo electrónico directamente a la persona que los solicitó. Hay docenas de plantillas de informes útiles, que se pueden usar de inmediato o personalizar según lo que necesite el solicitante. Este proceso es fundamental, ya que les ahorra a los administradores de TI mucho tiempo y trabajo en la elaboración de informes.

Es indispensable tener visibilidad de estas amenazas en tiempo real de modo que el personal de TI pueda reaccionar con rapidez y mitigar cualquier riesgo que se haya generado.

Independientemente de la organización, siempre habrá informes que se deben generar en intervalos programados y entregar a las partes pertinentes, o almacenar para uso futuro.

"La principal ventaja de usar ESET es que uno tiene todos los usuarios a la vista en una única consola, y puede administrar y revisar adecuadamente su estado de seguridad."

—Jos Savelkoul, Líder de equipo en el Departamento de TIC; Hospital Zuyderland, Holanda; más de 10.000 equipos

¿En qué se diferencia ESET?

DE LA PREVENCIÓN A LA RESPUESTA

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

REMEDIACIÓN DE INCIDENTES

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

SISTEMA AVANZADO DE CONTROL DEL ACCESO BASADO EN ROLES

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

NOTIFICACIONES PERSONALIZABLE

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

INFORMES DINÁMICOS Y PERSONALIZADOS

ESET PROTECT ofrece más de 170 informes integrados y le permite crear informes personalizados a partir de más de 1.000 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 pueden ordenar los equipos según el estado actual del dispositivo o los criterios de inclusión definidos. Las tareas se pueden configurar para que desencadenen acciones de exploración, modificación de políticas o instalación/desinstalación de software, tras cada cambio de membresía en el grupo dinámico.

SOPORTE PARA VDI AUTOMATIZADO

ESET emplea un completo algoritmo 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 completamente automatizado.

MARCA COMPROBADA Y DE CONFIANZA

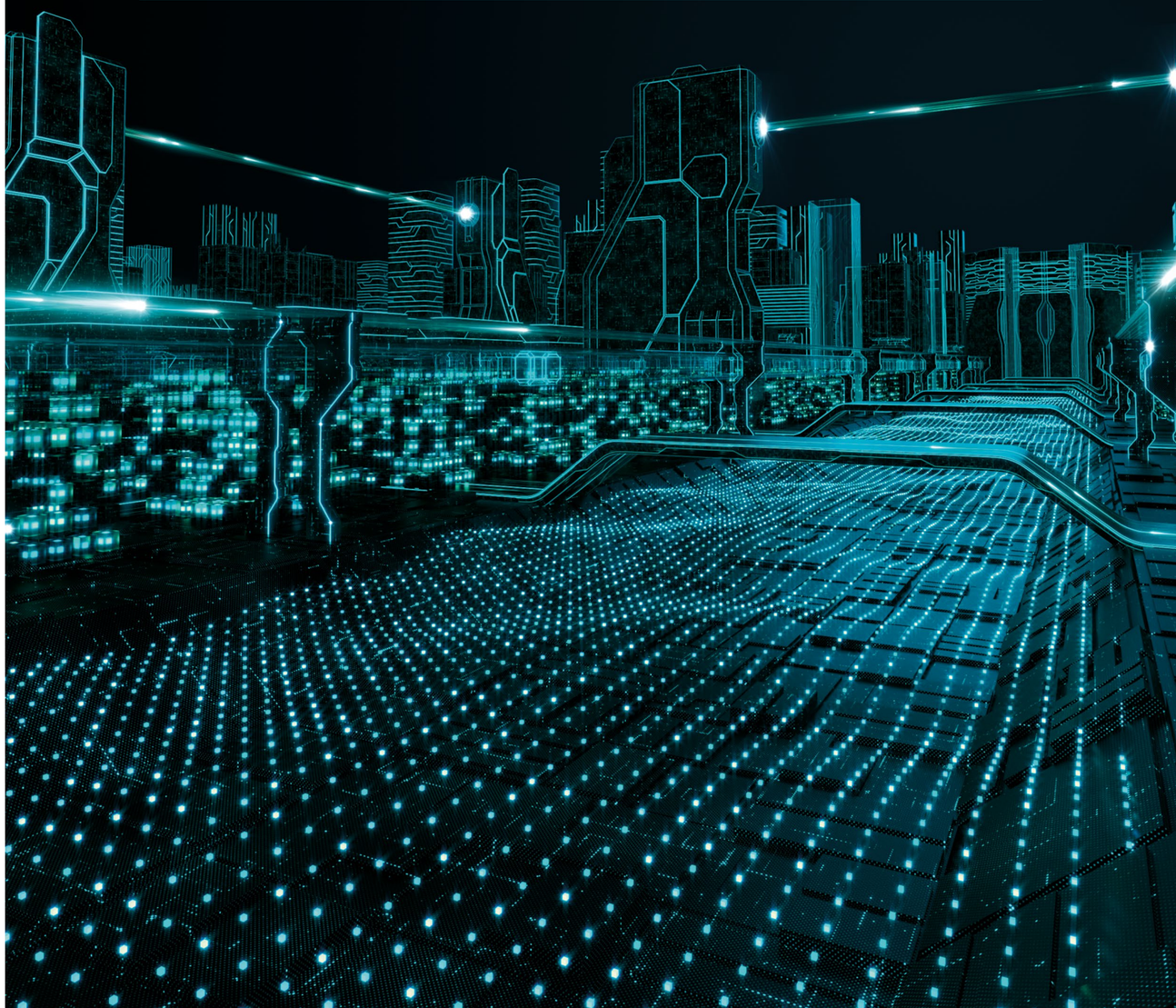
ESET ha formado parte de la industria de seguridad por más de 30 años y continúa mejorando su tecnología para estar siempre un paso por delante de las amenazas más recientes. Esta trayectoria ha logrado que más de 110 millones de usuarios de todo el mundo confíen en nuestros productos. Nuestra tecnología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

PREPARADO PARA MSP

Si usted es un proveedor de servicios gestionados (MSP) y se ocupa de las redes de sus clientes, la capacidad 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.

"Empresa sobresaliente; excelente soporte técnico; proporciona una fuerte protección contra amenazas y una administración centralizada."

— Dave, Gerente de TI; Deer Valley Unified School District, Estados Unidos; más de 15.500 equipos



Casos de uso

Ransomware

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

Los programadores que trabajan con código en su computadora laboral muchas veces crean 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.

Implementación de VDI

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

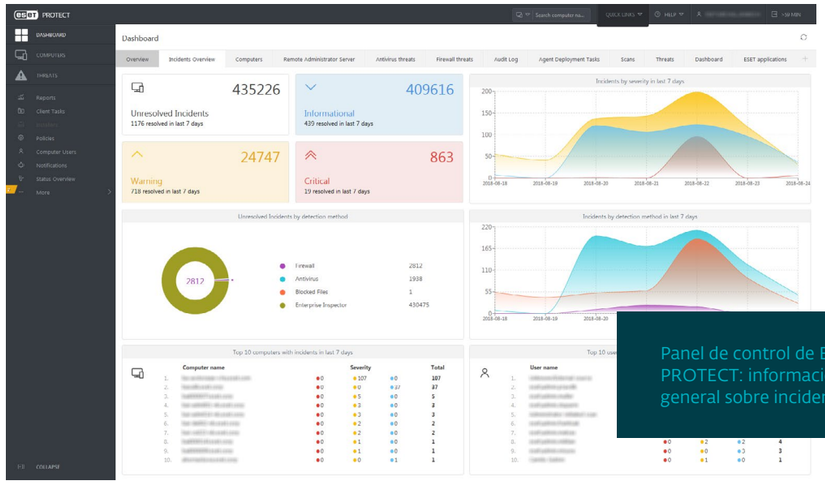
- ✓ Tras implementar una imagen maestra en las computadoras ya presentes en ESET PROTECT, los equipos continuarán informando a la instancia anterior a pesar de la existencia de una nueva imagen completa del sistema.
- ✓ Las máquinas que regresan a su estado inicial una vez terminado el turno de trabajo 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.

Inventario de hardware y software

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.



Panel de control de ESET PROTECT: información general sobre incidentes

Remediación de software

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.

ESET PROTECT puede ejecutarse como una consola en la nube, puede instalarse localmente en Windows o Linux o puede implementarse como un dispositivo virtual.

Al admitir usuarios múltiples y utilizar la autenticación en dos fases, se simplifican radicalmente las responsabilidades en los grandes equipos de trabajo corporativos.

"Para nosotros, la administración centralizada de la seguridad de todas las endpoints, los servidores y los dispositivos móviles fue un beneficio clave."

— Gerente de TI; Diamantis Masoutis S.A., Grecia; más de 6.000 equipos

Características técnicas

UNA ÚNICA PANTALLA

Los productos de ESET para endpoints se pueden administrar desde ESET PROTECT, incluyendo estaciones de trabajo, dispositivos móviles, servidores y máquinas virtuales, con los SO: Windows, macOS, Linux y Android.

SOPORTE PARA XDR

Para mejorar aún más el conocimiento de la situación y proporcionar visibilidad en toda la red, ESET PROTECT funciona junto con ESET Inspect, el componente habilitador de XDR de la plataforma ESET PROTECT. ESET Inspect es multiplataforma (Windows, macOS y Linux), permite la detección y corrección de amenazas avanzadas y puede integrarse perfectamente 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 y ayuda a cumplir con las regulaciones.

DEFENSA AVANZADA CONTRA AMENAZAS

El soporte para la defensa avanzada contra amenazas mejora en gran medida la detección de amenazas de 0-day, como el ransomware, al analizar rápidamente los archivos sospechosos en el entorno de pruebas en la nube de ESET. Además, ejecuta una batería de escaneos de malware muy completos, incluida la detonación en la nube.

INVENTARIO DE HARDWARE Y SOFTWARE

ESET PROTECT le brinda información sobre todas las aplicaciones de software instaladas en la organización y 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.

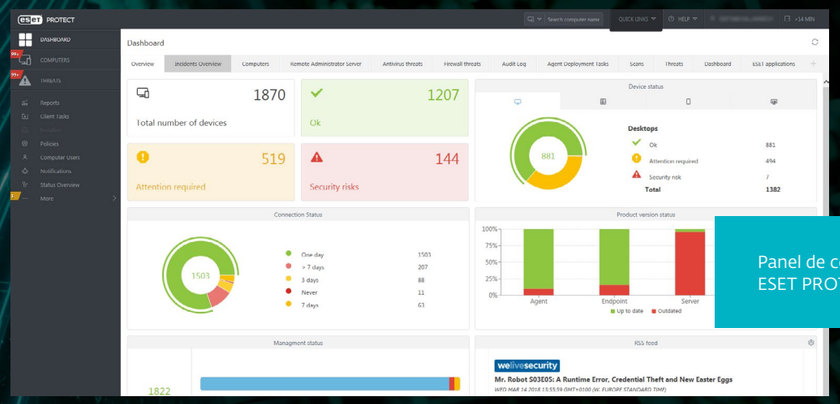
Esto le permite hacer más cosas desde una misma ubicación, por ejemplo, agrupar dinámicamente los equipos según la marca, el modelo, el sistema operativo, el procesador, la memoria RAM, el espacio en disco rígido y muchos otros elementos.

CONTROL GRANULAR DE POLÍTICAS

Las organizaciones pueden establecer múltiples políticas para una misma computadora o grupo, y anidar políticas para permisos heredados. Además, tienen la posibilidad de ajustar las políticas configuradas por el usuario, es decir que podrán bloquear las configuraciones que deseen 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 el formato JSON o LEEF, de uso muy extendido, lo que permite la integración con los Centros de operaciones de seguridad (SOC).



Panel de control de ESET PROTECT

Próximos pasos

¿Cómo comprar?
Todas nuestras soluciones se encuentran disponibles en *nuestro sitio web exclusivo*.

Pruebe gratis por 30 días:
Evalúe todas las funcionalidades del producto, incluyendo la protección para endpoints.

SOLICITAR

Migración desde la consola de ESET local:
¿Actualmente utiliza la consola de ESET local? Contacte a un partner de ESET en su área para que lo ayude con la migración.
www.eset.com/latam/buscador-partners

Acerca de ESET

Desde hace más de 30 años, desarrollamos soluciones de seguridad que ayudan a más de 100 millones de usuarios en el mundo a disfrutar la tecnología de forma segura.

Al no estar limitados por las exigencias de accionistas del mercado, podemos enfocarnos exclusivamente en la seguridad de la información, mediante investigación y desarrollo constante.

ESET EN NÚMEROS

+110 millones
de usuarios en el mundo

+400 mil
clientes corporativos

+200
países y territorios

13
centros de investigación y desarrollo

ALGUNOS DE NUESTROS CLIENTES

MITSUBISHI MOTORS
Drive your Ambition

protegido por ESET desde 2017, más de 9.000 endpoints

Allianz Suisse

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

Canon
Canon Marketing Japan Group

protegido por ESET desde 2016, más de 32.000 endpoints

T . . .

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

ALGUNOS DE NUESTROS PREMIOS MÁS IMPORTANTES

AV comparatives APPROVED Business Security DEC 2021

ESET recibió el premio Business Security APPROVED de AV-Comparatives en el Business Security Test en diciembre de 2021.

G2 Leader WINTER 2022

ESET logra consistentemente las mejores clasificaciones en la plataforma global de revisión de usuarios G2 y sus soluciones son avaladas por clientes de todo el mundo.

FORRESTER®

Las soluciones de ESET fueron reconocidas por el analista Forrester como sample vendor en **"The Forrester Tech Tide(TM): Zero Trust Threat Detection and Response, Q2 2021".**

eset® Digital Security
Progress. Protected.