INFORMACIÓN GENERAL DE LA SOLUCIÓN

ENDPOINT SOLUTIONS

Protección multicapa para endpoints, equipos portátiles y smartphones.

Progress. Protected

¿Qué es una **Plataforma de protección para endpoints?**

Es una solución que se implementa en endpoints para prevenir ataques de malware basados en archivos, detectar actividad maliciosa, y proporcionar las capacidades de investigación y remediación necesarias para responder a alertas e incidentes de seguridad dinámicos.

Las soluciones de ESET de protección para endpoints emplean un enfoque de varias capas donde múltiples tecnologías trabajan juntas dinámicamente, con la capacidad de ir equilibrando el rendimiento, la detección y los falsos positivos.

¿Por qué son importantes las **soluciones de protección para endpoints?**

RANSOMWARE

Desde el surgimiento de Cryptolocker en 2013, el ransomware ha sido una preocupación constante para las industrias de todo el mundo. A pesar de que el ransomware ya existía mucho antes, hasta ese momento nunca había constituido una amenaza significativa para las empresas. Sin embargo, en la actualidad, un incidente de ransomware puede cifrar los archivos importantes o necesarios de una empresa, e interrumpir por completo su funcionamiento. Cuando una empresa es víctima de un ataque de ransomware, por lo general pronto se da cuenta de que sus copias de seguridad no son lo suficientemente recientes y llega a la conclusión de que lo mejor es pagar el rescate.

Las soluciones de ESET de protección para endpoints proporcionan capas de defensa no solo para prevenir el ransomware sino también para detectarlo. Es importante poder prevenir y detectar el ransomware, ya que cada vez que alguien paga un rescate, está incentivando a los delincuentes a seguir utilizando este metodo de ataque.

ATAQUES DIRIGIDOS Y VIOLACIONES DE DATOS

El panorama actual de seguridad cibernética está en constante evolución, y sigue incorporando nuevos métodos de ataque y amenazas nunca antes vistas. Cuando se produce un ataque o una violación de datos, las organizaciones suelen sorprenderse de que sus defensas se hayan visto comprometidas, o directamente ignoran por completo la existencia del ataque. Una vez que finalmente descubren el ataque, implementan mitigaciones en forma reactiva para evitar que se repita. Sin embargo, esto no los protegerá si el siguiente ataque usa otro vector completamente nuevo.

Las soluciones de ESET de protección para endpoints utilizan la información de inteligencia de amenazas basada en sus soluciones. Las endpoints de todo el mundo funcionan como sensores; conforman la base de datos global para priorizar y bloquear efectivamente las amenazas más nuevas antes de que se distribuyan en el resto del mundo. Además, la mayoría de las plataformas de protección para endpoints suministran actualizaciones basadas en la nube para responder con mayor rapidez, sin tener que esperar a una actualización normal.

ATAQUES SIN ARCHIVOS

Las amenazas más nuevas no emplean archivos, es decir que existen exclusivamente en la memoria de la computadora, lo que hace que sean imposibles de detectar mediante las tecnologías de protección basadas en la exploración de archivos. Además, algunos ataques sin archivos aprovechan las aplicaciones instaladas que actualmente están integradas en el sistema operativo para dificultar aún más la detección del payload malicioso. Por ejemplo, en este tipo de ataques es muy común el uso de PowerShell.

Las plataformas de ESET de protección para endpoints incluyen capacidades de mitigación que detectan aplicaciones secuestradas o modificadas para proteger los equipos de los ataques sin archivos. ESET también ha creado módulos de exploración exclusivos que revisan constantemente la memoria en busca de cualquier elemento sospechoso. Al utilizar este enfoque en múltiples capas, nos aseguramos de estar siempre un paso por delante del malware más reciente.

Las soluciones de ESET de protección para endpoints suministran capas de defensa no solo para prevenir el malware sino también para detectarlo.

Cuando se produce un ataque o una violación de datos, las organizaciones suelen sorprenderse de que sus defensas se hayan visto comprometidas, o directamente ignoran por completo la existencia del ataque.

Las amenazas más nuevas no emplean archivos, es decir que existen exclusivamente en la memoria de la computadora, lo que hace que sean imposibles de detectar mediante las tecnologías de protección basadas en la exploración de archivos.

"ESET ha sido nuestra solución de seguridad confiable por años. Hace lo que tiene que hacer y no necesitamos preocuparnos. En resumen, ESET significa: confiabilidad, calidad y servicio."

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

Soluciones de ESET de protección para endpoints

ESET Endpoint Security para Windows/macOS/Android
ESET Endpoint Antivirus para Windows/macOS/Linux
ESET Server Security para Windows Server/Linux
ESET MDM para iOS y iPadOS

En qué se diferencia ESET

PROTECCIÓN EN MÚLTIPLES CAPAS

ESET combina tecnología de múltiples capas, aprendizaje automático y experiencia humana para proporcionarles a nuestros clientes el mejor nivel de protección. Nuestra tecnología se mejora y actualiza constantemente para brindar equilibrio entre detección, falsos positivos y rendimiento.

SOPORTE PARA PLATAFORMAS MÚLTIPLES

Los productos de ESET para la protección de endpoints son compatibles con todos los sistemas operativos, incluyendo Windows, Linux y Android. Todas las soluciones para endpoints se pueden administrar por completo desde una única pantalla. La administración de dispositivos móviles iOS y Android también está completamente integrada.

MÁXIMO RENDIMIENTO

Una de las mayores preocupaciones de las empresas suele ser el impacto que la solución de protección para endpoints tendrá en el rendimiento. Los productos de ESET continúan destacándose por su rendimiento lo que permite ganan las pruebas de evaluadores externos, que demuestran lo livianos que son en los sistemas.

PRESENCIA MUNDIAL

ESET tiene oficinas en 22 países, laboratorios de investigación y desarrollo en 13, y además cuenta con presencia en más de 200 países y territorios. Esto nos ayuda a recopilar datos para detener el malware antes de que se extienda por todo el mundo, y a priorizar el desarrollo de nuevas tecnologías basándonos en las amenazas más recientes o en los posibles nuevos vectores de ataque.

"¿El mejor testimonio? Las estadísticas de nuestra Mesa de ayuda: desde que implementamos ESET, nuestro personal de soporte no registra ninguna llamada, ¡ya no tienen que lidiar con problemas de antivirus o malware!"

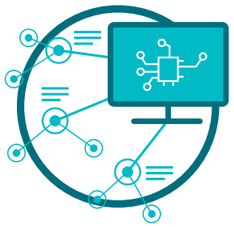
— Adam Hoffman, Gerente de Infraestructura de TI; Mercury Engineering, Irlanda; 1.300 equipos

La tecnología

Nuestros productos y tecnologías se basan en 3 pilares

ESET LIVEGRID®

Cada vez que aparece una amenaza o-day como el ransomware, el archivo se envía a nuestro sistema de protección contra malware basado en la nube, LiveGrid®, donde se activa la amenaza para monitorear su comportamiento. Los resultados se distribuyen a todas las endpoints a nivel mundial en cuestión de minutos, sin requerir ninguna actualización.



APRENDIZAJE AUTOMÁTICO

Combina la potencia de las redes neuronales y de algoritmos seleccionados para etiquetar correctamente las muestras entrantes como no infectadas, potencialmente no deseadas o maliciosas.

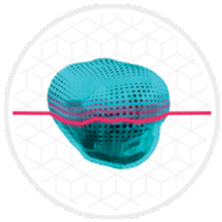
EXPERIENCIA HUMANA

Nuestros investigadores de seguridad de categoría mundial comparten sus conocimientos exclusivos para garantizar la mejor inteligencia de amenazas las 24 horas del día.

Una sola capa de protección no es suficiente para combatir el panorama de amenazas en constante evolución. Todos los productos de ESET para endpoints tienen la capacidad de detectar el malware antes, durante y luego de su ejecución. Al centrarnos en más de una parte específica del ciclo de vida del malware, proporcionamos el mayor nivel de protección posible.

APRENDIZAJE AUTOMÁTICO

Desde 1997, todas las soluciones de ESET para endpoints han utilizado el aprendizaje automático (además de las demás capas de defensa) que se basa especificamente resultados consolidados y redes neuronales.



EXPLORACIÓN AVANZADA DE MEMORIA

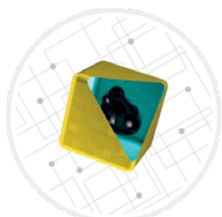
La Exploración avanzada de memoria de ESET monitorea el comportamiento de los procesos maliciosos y los explora cuando se muestran en memoria. El malware sin archivos no requiere componentes persistentes en el sistema de archivos que pueden detectarse de manera convencional. Únicamente la exploración de la memoria es capaz de descubrir y detener dichos ataques maliciosos con éxito.

RANSOMWARE SHIELD

La funcionalidad Ransomware Shield de ESET brinda a los usuarios una capa adicional de protección ante esta amenaza. Esta tecnología monitorea y evalúa todas las aplicaciones ejecutadas en función de su comportamiento y reputación. Fue diseñada para detectar y bloquear los procesos con un comportamiento similar al del ransomware.

BLOQUEO DE EXPLOITS

El Bloqueo de exploits de ESET monitorea las aplicaciones que suelen ser atacadas por exploits con mayor frecuencia (navegadores, lectores de documentos, clientes de correo electrónico, Flash, Java, etc.) y, en lugar de enfocarse solamente en ciertos identificadores de CVE (Vulnerabilidades y Exposiciones Comunes) en particular, se centra en técnicas de explotación. Cuando se activa, la amenaza se bloquea de inmediato en la máquina.

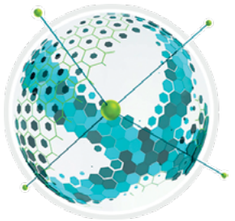


SANDBOXING INCORPORADO

El malware de hoy suele estar muy ofuscado y hace todo lo posible para evadir la detección. El uso del modo sandbox incorporado en el producto nos permite identificar su comportamiento real oculto bajo el aspecto superficial. Con la ayuda de esta tecnología, las soluciones de ESET emulan diferentes componentes de hardware y software para ejecutar las muestras sospechosas en un entorno virtualizado aislado.

PROTECCIÓN ANTE BOTNETS

La Protección ante botnets de ESET detecta las comunicaciones maliciosas que utilizan las botnets y al mismo tiempo identifica los procesos ofensivos. Bloquea todas las comunicaciones maliciosas detectadas y se lo informa al usuario.



PROTECCIÓN CONTRA ATAQUES DE RED

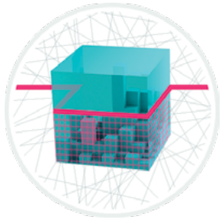
Esta tecnología mejora la detección de las vulnerabilidades conocidas en el nivel de la red. Constituye otra importante capa de seguridad ante la propagación del malware, los ataques que circulan por la red y el aprovechamiento de vulnerabilidades para las cuales aún no se lanzó al público o no se desarrolló la revisión correspondiente.

NAVEGADOR SEGURO

Diseñado para asegurar los activos de la organización con una capa especial de protección que se centra en el navegador, considerado el acceso más común hacia los datos críticos dentro de la intranet y en la nube. El Navegador Seguro brinda una protección de memoria mejorada para el proceso del navegador, junto con la protección del teclado, y permite a los administradores agregar URLs seguras.

HIPS

El Sistema de prevención de intrusiones basado en el host provisto por ESET monitorea la actividad del sistema y utiliza un grupo de reglas predefinidas que reconocen cualquier comportamiento sospechoso en el sistema. Además, el mecanismo de autodefensa de HIPS evita que el proceso malicioso lleve a cabo su actividad dañina.



MÓDULO DE EXPLORACIÓN UEFI

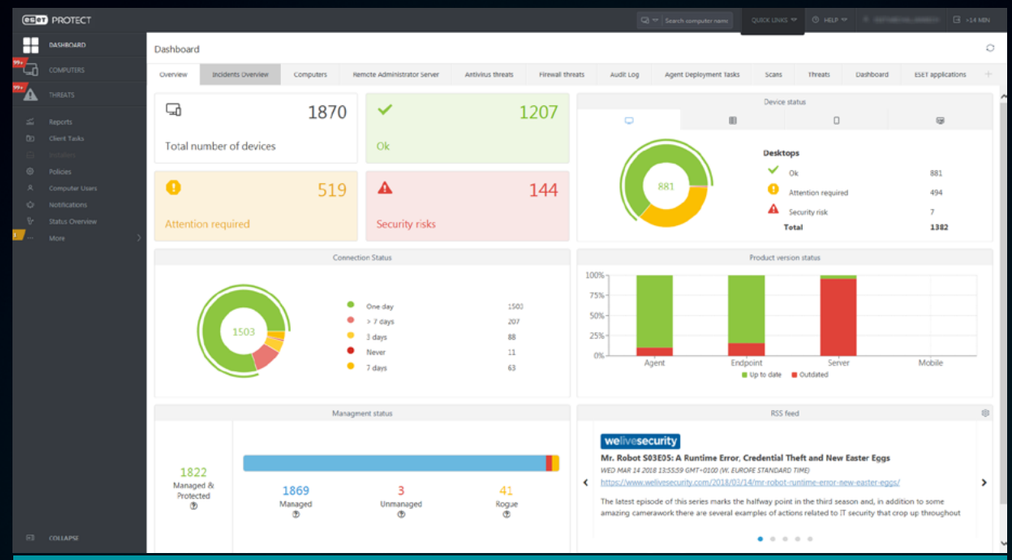
ESET es el primer proveedor de seguridad para endpoints en agregar una capa exclusiva a su solución para proteger la Interfaz de firmware extensible unificada (UEFI). El Módulo de exploración UEFI de ESET verifica y aplica las medidas de seguridad en el entorno previo al arranque y está diseñado para monitorear la integridad del firmware. Si detecta alguna modificación, se lo notifica al usuario.

PROTECCIÓN CONTRA ATAQUES DE FUERZA BRUTA

Una característica de seguridad que protege los dispositivos ante la posibilidad de adivinar las credenciales y una conexión remota ilícita. La protección se puede configurar fácilmente a través de una política desde la consola, y se pueden crear exclusiones cuando algo está bloqueado pero no debería estarlo.

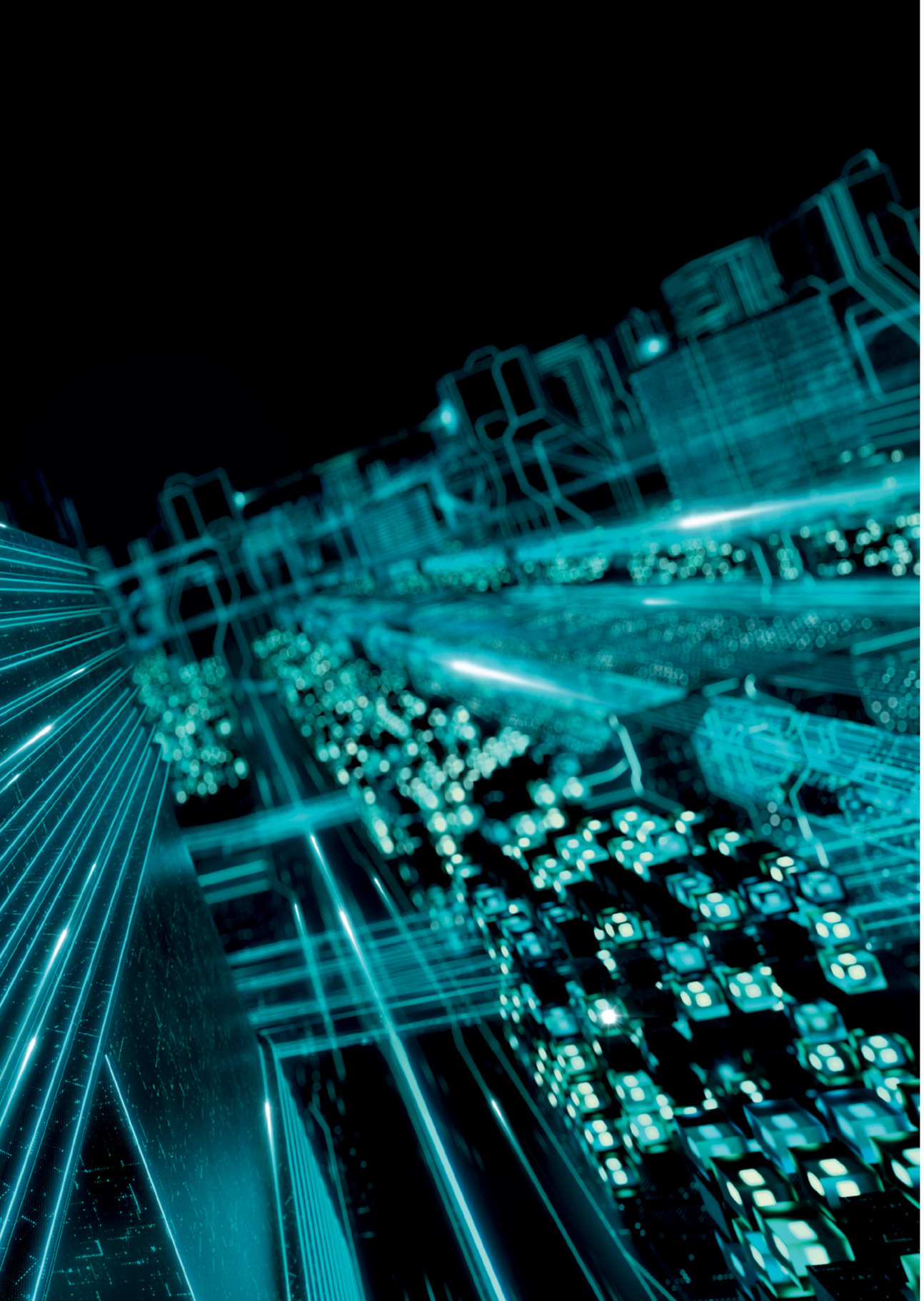
"Lo que más se destaca de las soluciones de ESET son sus ventajas tecnológicas al compararlos con otros productos del mercado. ESET nos ofrece una seguridad en la que podemos confiar, lo que me permite trabajar en cualquier proyecto y en cualquier momento con la tranquilidad de que nuestras computadoras están 100% protegidas."

— Fiona Garland, Analista de Negocios del Grupo de TI; Mercury Engineering, Irlanda; 1.300 equipos



ESET PROTECT

Todas las soluciones para endpoints de ESET se administran desde una única consola de ESET PROTECT, que puede estar basada en la nube o en las instalaciones, lo que garantiza una visión general completa de su red.



Casos de uso

Ransomware

Algunas empresas necesitan contar con una protección adicional para prevenirse de los ataques de ransomware.

SOLUCIÓN

- ✓ La Protección contra ataques de red evita que el ransomware infecte el sistema, ya que detiene los exploits en el nivel de la red.
- ✓ Nuestra completa defensa en múltiples capas incluye un modo sandbox integrado a los productos, encargado de detectar el malware que utiliza la ofuscación para evadir su detección.
- ✓ El sistema en la nube de protección contra malware lo resguarda automáticamente de las nuevas amenazas sin necesidad de esperar a la próxima actualización de detecciones.
- ✓ Todas las soluciones cuentan con la tecnología Ransomware Shield para proteger a las empresas del cifrado malicioso de archivos.

Malware sin archivos

El malware sin archivos es una amenaza relativamente nueva y, dado que solo existe en la memoria, su detección requiere un enfoque diferente al del malware tradicional basado en archivos.

SOLUCIÓN

- ✓ La Exploración avanzada de memoria, una tecnología exclusiva de ESET, lo protege de este tipo de amenazas. Monitorea la conducta de los procesos maliciosos y los explora cuando se muestran en memoria.
- ✓ Para reducir el tiempo de recopilación e investigación de datos, envíe las amenazas a ESET Threat Intelligence y recibirá información sobre su funcionamiento.
- ✓ La tecnología de múltiples capas, el aprendizaje automático y la experiencia humana les proporcionan a nuestros clientes el mejor nivel de protección posible.

Credenciales robadas

Los ataques de phishing y los sitios web falsos que imitan a organizaciones reales para robar credenciales de inicio de sesión y datos financieros van en aumento.

SOLUCIÓN

- ✓ Los productos ESET para endpoints están diseñados para proteger los activos de una organización con una capa única de protección, enfocándose en el navegador como la herramienta principal para acceder a datos críticos dentro del perímetro de la intranet y en la nube.
- ✓ La función Navegador seguro protege los datos confidenciales mientras navega en línea.
- ✓ Con un solo clic, los administradores pueden optar por incluir todos los portales bancarios y de pago y decidir proteger el navegador para sitios web específicos o no.

Ataques de adivinación de contraseñas

El protocolo de escritorio remoto (RDP) y el bloque de mensajes del servidor (SMB) son vectores de ataque atractivos que pueden permitir que un atacante obtenga el control remoto total de un sistema.

SOLUCIÓN

- ✓ **Brute Force Attack Protection** proporciona una defensa contra ataques frontales en puntos de acceso remoto protegidos con contraseña.
- ✓ Protege los dispositivos contra la posibilidad de adivinar las credenciales y el establecimiento ilegítimo de conexiones remotas.
- ✓ Se puede configurar fácilmente a través de una política directamente desde la consola; se pueden crear exclusiones cuando algo está bloqueado pero no debería estarlo.
- ✓ Versátil: los usuarios pueden agregar sus propias reglas o modificar las existentes.

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 Marketing Japan Group

protegido por ESET desde 2016, más de 32.000 endpoints

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".**