INFORMACIÓN GENERAL DE LA SOLUCIÓN

SERVER SECURITY

Protección confiable para servidores en múltiples capas

Progress. Protected

¿Qué son las **soluciones de seguridad para archivos?**

Los productos de seguridad para archivos están diseñados para proteger los servidores centrales de la organización ante las posibles amenazas. Estos productos deben instalarse en cualquier servidor no especializado para garantizar que los recursos de la organización no se infecten. Actualmente, las empresas se ponen en riesgo cuando les permiten a los usuarios guardar archivos en los recursos compartidos de la red corporativa, sin protegerla adecuadamente de los archivos maliciosos. Si un solo usuario guarda un archivo malicioso en una unidad de red puede causar instantáneamente un efecto cascada que dejará los archivos de su organización inaccesibles.

ESET Server Security suministra protección avanzada para todos los servidores generales, el almacenamiento de archivos de red y los servidores multipropósito. Presta atención especial para garantizar que los servidores se mantengan estables y libres de problemas, con la mínima cantidad de ventanas emergentes y reinicios de modo de no interrumpir la continuidad del negocio.

¿Por qué es importante la **seguridad para archivos?**

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 solo incidente de ransomware es capaz de 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.

En el caso de los servidores, el ransomware puede ser un problema aún mayor, ya que los usuarios pueden guardar ransomware en una unidad de red. Las soluciones ESET Server Security proporcionan varias capas de defensa que no solo previenen el ransomware sino que también lo detectan si en algún momento llega a aparecer en la organización. Es importante tratar de prevenir y detectar el ransomware, ya que cada vez que alguien paga un rescate, está incentivando a los delincuentes a seguir utilizando este 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 ESET Server Security utilizan la información de Threat Intelligence recopilada gracias a su presencia global para priorizar y bloquear con eficacia las amenazas más recientes antes de que se lleguen a entregar en cualquier parte del mundo. Los servidores suelen ser uno de los objetivos más buscados debido a que en general contienen datos confidenciales o valiosos. Para protegerse mejor contra estos ataques cada vez más frecuentes, las soluciones ESET Server Security suministran actualizaciones basadas en la nube que permiten responder con mayor rapidez en caso de que se pase por alto una detección, 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 actualmente que 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 soluciones ESET Server Security incluyen capacidades de mitigación que detectan aplicaciones secuestradas o modificadas para proteger los equipos de los ataques sin archivos. Otros han creado módulos de exploración exclusivos que revisan constantemente la memoria en busca de cualquier elemento sospechoso. De todas formas, los productos ESET Server Security siempre aceptaron el desafío de mantenerse un paso por delante del malware más nuevo.

Las soluciones de ESET suministran capas de defensa no solo para prevenir el malware sino también para detectarlo si en algún momento llega a aparecer en la organización.

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 ESET Server Security para servidores de archivos

ESET Server Security para Microsoft Windows Server

ESET Server Security para Linux

En qué se diferencia ESET

PROTECCIÓN EN MÚLTIPLES CAPAS

ESET combina tecnología en múltiples capas, machine learning y experiencia humana para proporcionarles a nuestros clientes el mejor nivel de protección posible. Nuestra tecnología se mejora y cambia constantemente para suministrar el mayor equilibrio entre detección, falsos positivos y rendimiento.

RENDIMIENTO INIGUALABLE

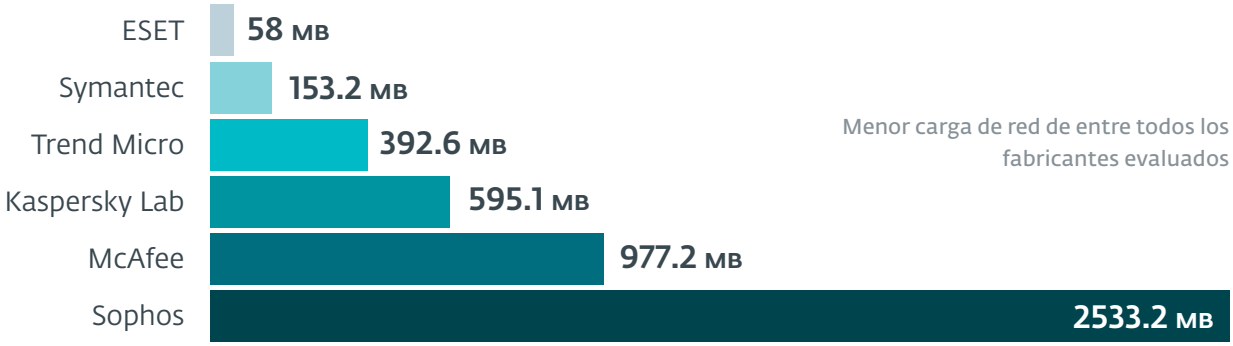
Una de las mayores preocupaciones de las empresas suele ser el impacto que la solución de protección para endpoints tendrá en el rendimiento. Los productos de ESET continúan sobresaliendo por su rendimiento y ganan las pruebas de evaluadores externos, que demuestran lo livianos que son en los sistemas.

SOPORTE PARA PLATAFORMAS MÚLTIPLES

Las soluciones ESET Server Security son compatibles con muchos sistemas operativos y plataformas, incluyendo Windows Server, Office365. Todas las soluciones de ESET se administran en su totalidad desde una única pantalla.

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.



Menor carga de red de entre todos los fabricantes evaluados

Fuente: AV-Comparatives: Prueba de Rendimiento de Red para Software de Seguridad Corporativa

"¿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!"

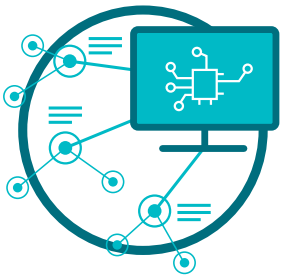
— Adam Hoffman, Gerente de Infraestructura de TI; Mercury Engineering, Irlanda; 1.300 equipos

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.



MACHINE LEARNING

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.

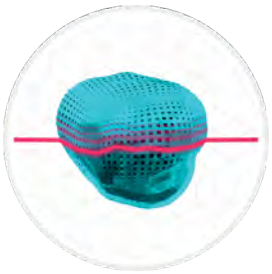
EXPERIENCIA HUMANA

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 defensa no es suficiente para combatir el panorama de amenazas en constante evolución. Todos los productos de seguridad de ESET 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.

MACHINE LEARNING

Todos los productos de ESET para endpoints han estado usando el machine learning además de todas las demás capas de defensa desde 1997 hasta la actualidad. Específicamente, el machine learning utiliza resultados consolidados y redes neuronales.



EXPLORACIÓN AVANZADA DE MEMORIA

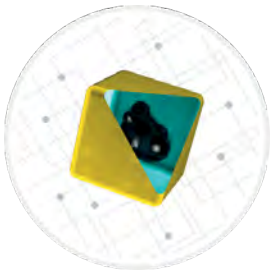
Monitorea el comportamiento de los procesos maliciosos y los explora cuando se muestran en memoria. El malware sin archivos no requiere componentes persistentes en el sistema de archivos que pueden detectarse de manera convencional. Únicamente la exploración de la memoria es capaz de descubrir y detener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

RANSOMWARE SHIELD

Es una capa adicional que protege a los usuarios del ransomware. 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.

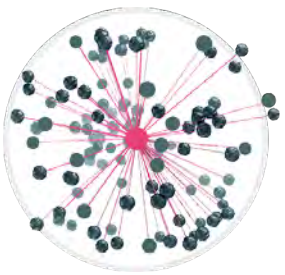
BLOQUEO DE EXPLOITS

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



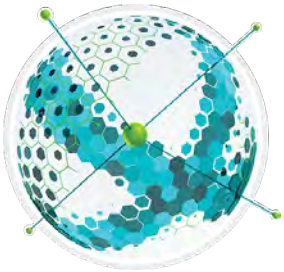
SANDBOXING INCORPORADO

El malware de hoy suele estar muy ofuscado y hace todo lo posible para evadir la detección. El uso del sandboxing 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

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

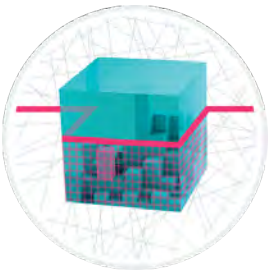
Esta tecnología mejora la detección de vulnerabilidades conocidas en el nivel de la red. Constituye otra importante capa de seguridad ante la propagación del malware, los ataques que circulan por la red y el aprovechamiento de vulnerabilidades para las cuales aún no se lanzó al público o no se desarrolló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

DETECCIÓN DEL COMPORTAMIENTO: HIPS

Monitorea la actividad del sistema y usa un grupo predefinido de reglas 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.

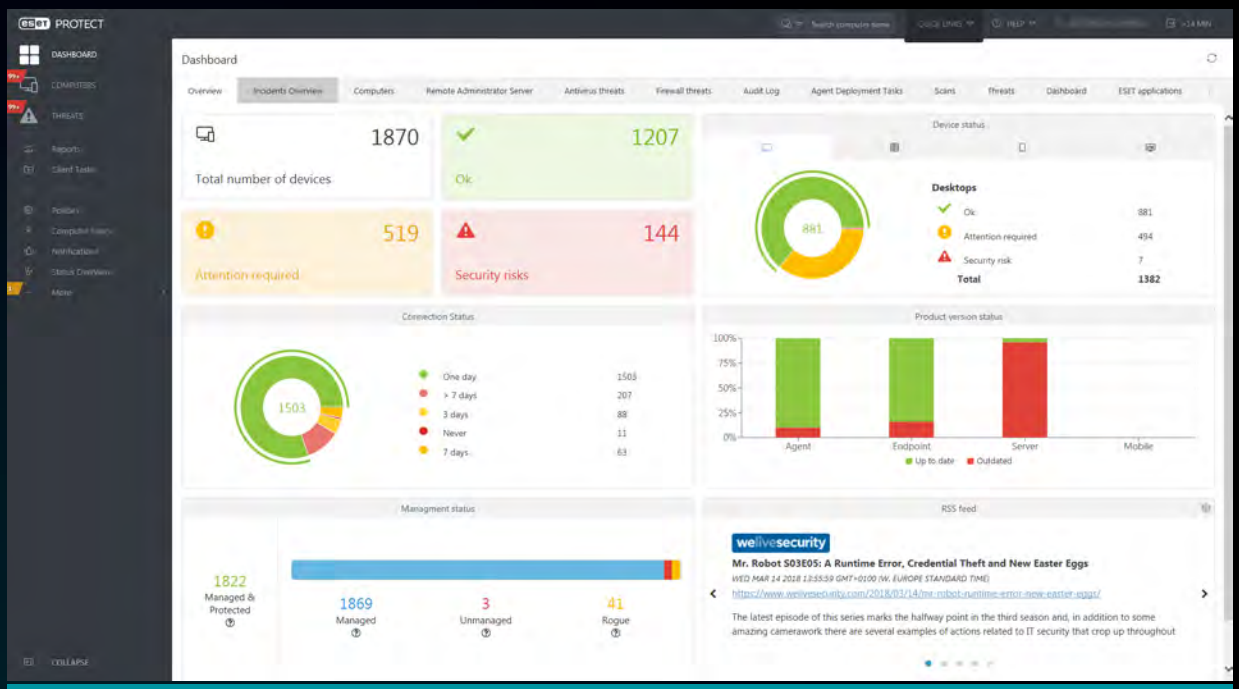


COMPATIBILIDAD CON AMSI Y EXPLORACIÓN DE SCRIPTS

Las soluciones de ESET son compatibles con la Interfaz de exploración antimalware (AMSI, del inglés) para suministrar una protección mejorada de usuarios, datos, aplicaciones y carga de trabajo. También utiliza la interfaz de Servicio protegido, el nuevo módulo de seguridad integrado de Windows, que únicamente permite la carga de código firmado y confiable, para brindar mayor seguridad contra los ataques de inyección de código.

"Lo que más se destaca de los productos 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 consola en la nube, ESET PROTECT, lo que garantiza una visión general y completa de su red.

"Cuando encontramos a ESET, supimos que era la elección correcta. Tecnología confiable, detección sólida, presencia local y excelente soporte técnico: tenía todo lo que necesitábamos."

— Ernesto Bonhoure, Gerente de Infraestructura de TI; Hospital Alemán, Argentina, más de 1.500 equipos

Casos de uso

Malware sin archivos

Caso de uso: 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.
- ✓ Cuando ESET Server Security no logra decidir si una muestra es una posible amenaza, la carga en el servicio de sandbox de ESET basado en la nube, ESET LiveGuard Advanced, para determinar con la mayor exactitud posible si es maliciosa.
- ✓ Para reducir el tiempo de recopilación e investigación de datos, envíe las amenazas confirmadas a ESET Threat Intelligence y recibirá información sobre su funcionamiento.

Amenazas 0-day

Caso de uso: Las amenazas 0-day son una gran preocupación para las empresas porque no saben cómo protegerse de algo que nunca antes habían visto.

SOLUCIÓN

- ✓ ESET Threat Intelligence proporciona datos sobre las últimas amenazas, tendencias y ataques dirigidos para ayudar a las empresas a predecir y prevenir las amenazas más recientes.
- ✓ Los productos de ESET para endpoints hacen uso de la heurística y el machine learning (parte de nuestro enfoque de seguridad en múltiples capas) para protegerse contra el malware nunca antes visto.
- ✓ 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

Ransomware

Caso de uso: Algunas empresas necesitan contratar seguros adicionales para protegerse de los ataques de ransomware. Además, quieren asegurarse de que sus unidades de red estén a salvo del cifrado malicioso.

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 sandboxing integrado a los productos, encargado de interceptar 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.
- ✓ Todos los productos cuentan con Ransomware Shield, una tecnología que actúa después de la ejecución del malware para proteger a las empresas del cifrado malicioso de archivos.
- ✓ Cuando ESET Server Security no logra decidir si una muestra es una posible amenaza, la carga en el servicio de sandboxing de ESET basado en la nube, ESET LiveGuard Advanced, para determinar con la mayor exactitud posible si es maliciosa.

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.

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".**


Progress. Protected.