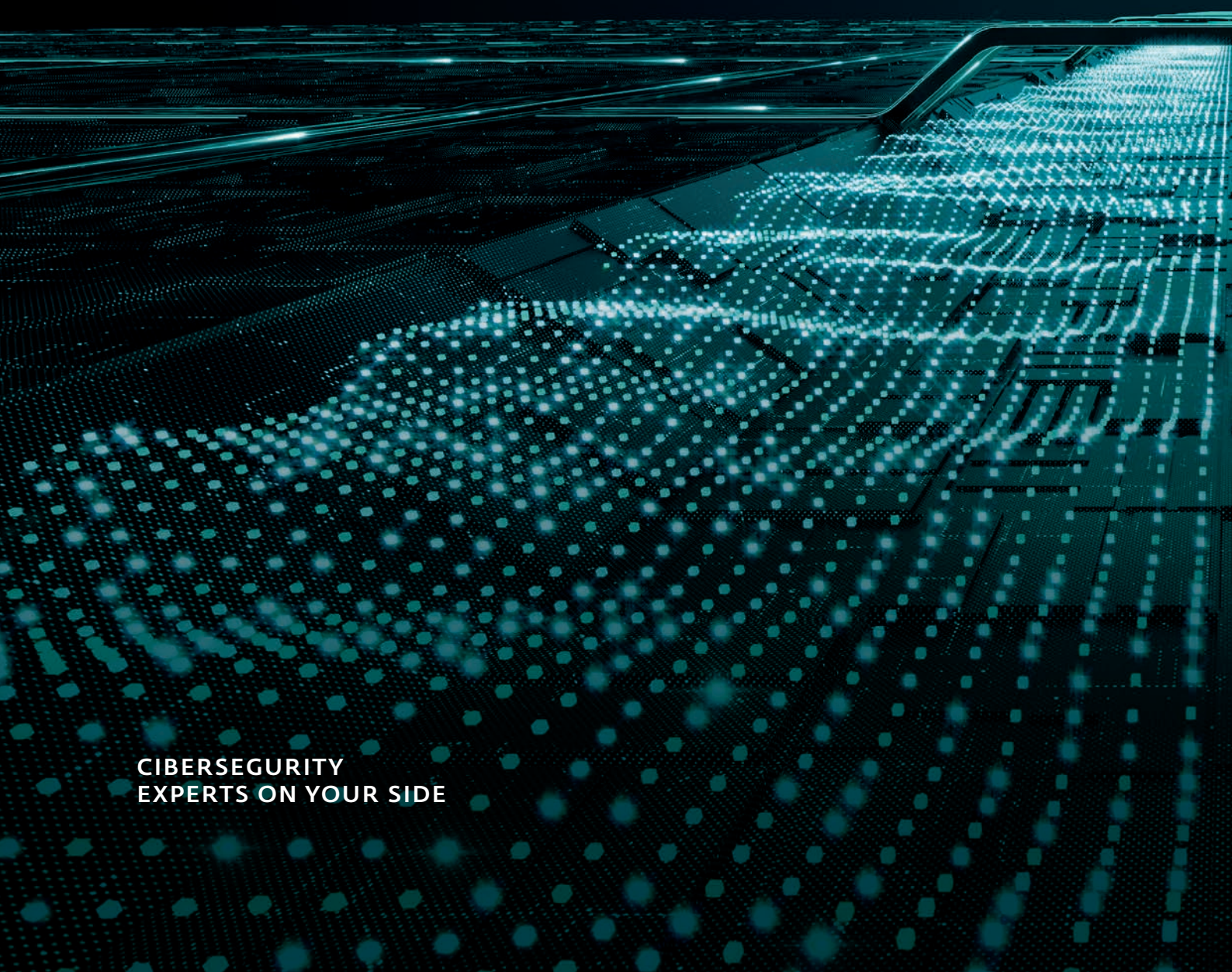
SECURITY
PARA MICROSOFT SHAREPOINT SERVER

Protege la información sensible en Microsoft SharePoint con una tecnología multicapa



CIBERSEGURITY
EXPERTS ON YOUR SIDE

¿Qué es una **solución de seguridad para SharePoint?**

Un producto de seguridad para SharePoint está diseñado para proteger los servidores de colaboración centrales de una empresa frente a cualquier tipo de amenaza. Este producto debería instalarse en cualquier servidor SharePoint de una empresa para garantizar que no se infecten los recursos. Hoy en día, las empresas ponen en riesgo su infraestructura permitiendo que los usuarios guarden o suban archivos al servidor de la empresa, sin proteger adecuadamente su SharePoint de archivos maliciosos. Con que tan solo un usuario suba un archivo malicioso a un servidor de colaboración, puede causar inmediatamente un efecto cascada que puede dejar inaccesible toda la información de la empresa.

ESET Security para Microsoft SharePoint ofrece una protección avanzada contra todos los archivos maliciosos o no deseados. Garantiza que los servidores permanezcan estables y libres de conflictos para mantener las ventanas de mantenimiento y no entorpecer la continuidad de la empresa.

¿Por qué elegir la **Solución de seguridad para SharePoint?**

RANSOMWARE

El ransomware ha sido una preocupación constante para las empresas a nivel mundial desde la aparición de Cryptolocker en 2013. A pesar de que el ransomware ha existido desde hace mucho tiempo, nunca fue una amenaza que preocupara especialmente a las empresas. Sin embargo, una única incidencia de ransomware puede hacer que una empresa quede inoperativa cifrando sus archivos más importantes. Cuando una empresa experimenta un ataque de ransomware y se da cuenta de que las copias de seguridad no son suficientemente recientes, inmediatamente siente que la única opción que tiene es pagar el rescate.

Con un servidor SharePoint, el ransomware puede ser un problema mucho mayor debido a la mayor capacidad de los usuarios de almacenar o subir un archivo malicioso accidentalmente. La solución ESET SharePoint Security proporciona capas de defensa para prevenir contra el ransomware o detectarlo si se produce un ataque a algún equipo de la empresa. Es importante intentar prevenir y detectar el ransomware, ya que cada vez que alguien paga un rescate, se motiva a los cibercriminales a continuar usando este tipo de ataque.

ATAQUES DIRIGIDOS Y FUGAS DE INFORMACIÓN

El panorama actual de la ciberseguridad se encuentra en constante evolución con nuevos métodos de ataque y amenazas nunca antes vistas. Cuando se produce un ataque o fuga de información, las empresas se suelen sorprender de que sus defensas hayan sido puestas en riesgo o ni siquiera son conscientes de que se ha producido el ataque. Una vez se percatan, las empresas implementan las medidas para evitar de forma reactiva que este ataque vuelva a suceder. Sin embargo, esto no las protege del próximo ataque que podría usar otro vector totalmente nuevo.

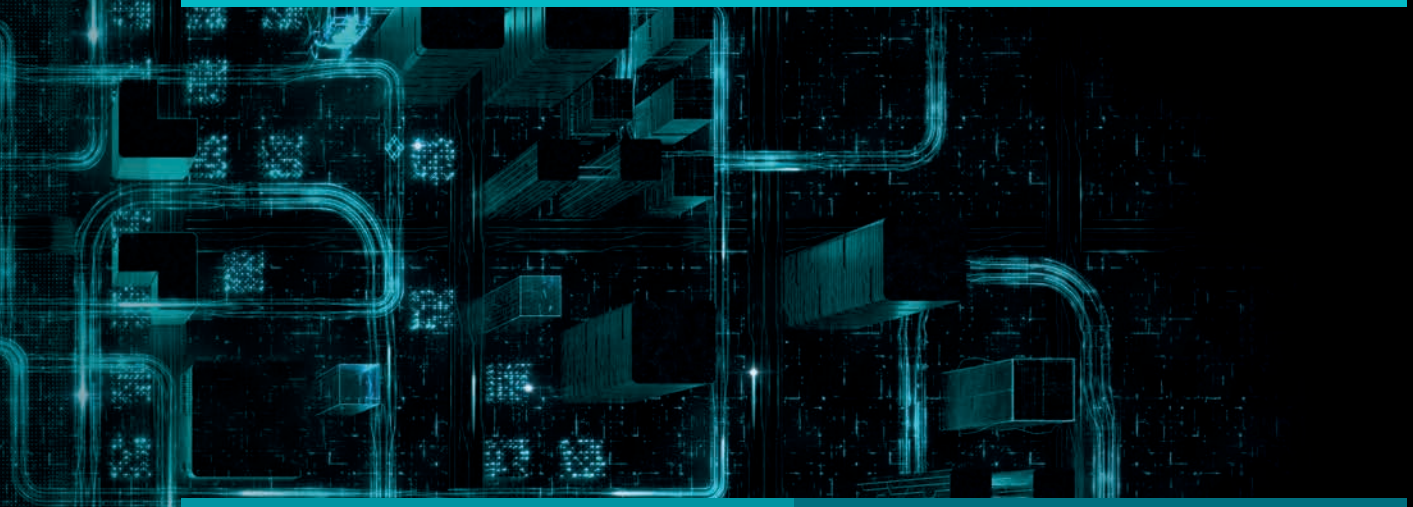
La solución ESET SharePoint Security usa información de las amenazas (threat intelligence) gracias a su presencia global para priorizar y bloquear eficazmente las últimas amenazas antes de que se propaguen por otros lugares del mundo. Los servidores son un objetivo más buscado porque contienen mucha más información sensible o confidencial. Para proteger mejor contra este mayor número de ataques, la solución ESET SharePoint Security cuenta con actualización en la nube para ofrecer una respuesta rápida en caso de no detectar una muestra sin tener que esperar a una actualización periódica.

ATAQUES SIN ARCHIVOS

Las amenazas más novedosas llamadas “malware sin archivos” existen exclusivamente en la memoria del equipo, haciendo que sea imposible de detectar para protecciones basadas en análisis de archivos. Además, algunos ataques usarán aplicaciones instaladas en el sistema operativo para que la carga maliciosa sea más difícil de detectar si cabe. Por ejemplo, el uso de PowerShell en estos ataques es muy común.

La solución ESET SharePoint Security tiene también la capacidad de detectar aplicaciones que han sido hackeadas para proteger contra los ataques sin archivos. También incluye un análisis constante de la memoria en busca de cualquier elemento sospechoso.

Las soluciones de protección de equipos de ESET proporcionan capas de defensa, no solo para prevenir el malware, sino para detectarlo si en algún momento se produce un ataque a algún equipo de la empresa.



Con un servidor SharePoint central, el ransomware puede convertirse en un problema mucho más grande debido a la capacidad de los usuarios de guardar o subir ransomware al propio servidor.

Las amenazas más novedosas llamadas "malware sin archivos" existen exclusivamente en la memoria del equipo, haciendo que sea imposible de detectar para protecciones basadas en análisis de archivos.

"ESET lleva siendo nuestra solución de seguridad fiable durante años. Hace lo que tiene que hacer y no tienes que preocuparte. En resumen, ESET significa: fiabilidad, calidad y servicio."

—Jos Savelkoul, jefe de departamento de tecnología; Zuyderland Hospital, Holanda; +10.000 puestos

ESET marca la diferencia

PROTECCIÓN MULTICAPA

ESET combina la tecnología de protección multicapa, el machine learning y un equipo experimentado de personas para proporcionar el mejor nivel de protección posible a nuestros clientes. Nuestra tecnología está en cambio constante para proporcionar el mejor equilibrio de detección, falsos positivos y rendimiento.

ACCESO DIRECTO A LA BASE DE DATOS

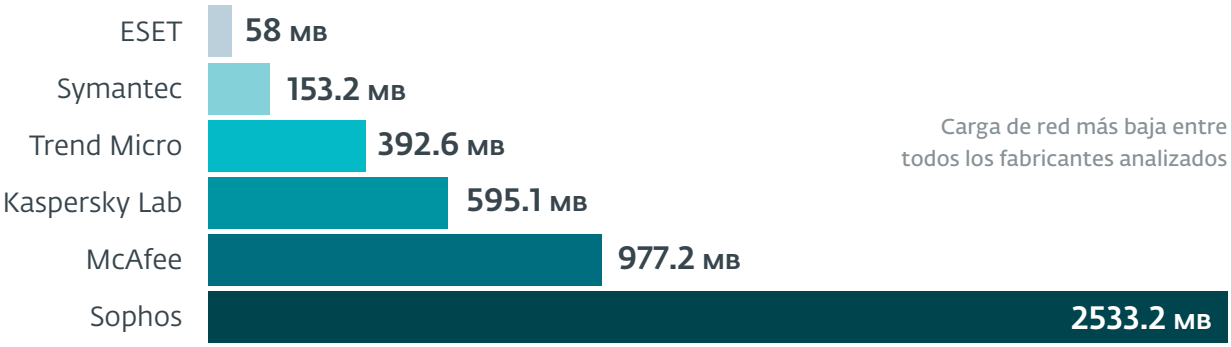
Posee un método opcional para extraer archivos donde ESET SharePoint Security omite el modelo de objetos de SharePoint y extrae el archivo directamente del servidor de base de datos dedicado para proporcionar un rendimiento aún mejor.

EL MEJOR RENDIMIENTO

En la mayoría de los casos, la mayor preocupación de las empresas es el impacto que produce la solución de protección en el rendimiento de sus equipos. Los productos ESET continúan ofreciendo un rendimiento sobresaliente y son líderes en los análisis de terceros que evalúan el impacto de las soluciones en los sistemas.

PRESENCIA GLOBAL

ESET cuenta con oficinas en 22 países en todo el mundo, laboratorios de I+D en 13 y presencia en más de 200. Esto contribuye a proporcionar información para bloquear el malware antes de que se propague a nivel global, así como priorizar nuevas tecnologías basadas en las amenazas más recientes o nuevos vectores posibles.



Carga de red más baja entre todos los fabricantes analizados

Fuente: AV-Comparatives: Test de rendimiento de la red, productos de seguridad para empresas

"¿... El mejor testimonio? Las estadísticas de nuestro servicio de soporte técnico: después de instalar ESET, nuestros chicos de soporte no registran llamadas, ¡ya no tienen que ocuparse de ninguna incidencia relacionada con el antivirus o malware!"

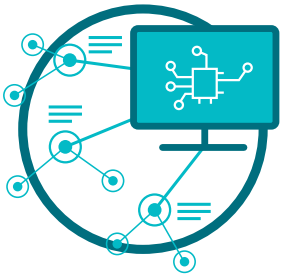
-Adam Hoffman, Director de infraestructuras de sistemas; Mercury Ingeniería, Irlanda. 1.300 puestos

La tecnología

Nuestros productos y tecnologías se apoyan en tres pilares

ESET LIVEGRID®

Siempre que aparece una amenaza zero-day como por ejemplo un ataque de ransomware, el archivo se envía a nuestro sistema de protección contra el malware en la nube LiveGrid®, donde se activa la amenaza y se monitoriza el comportamiento. Los resultados de este sistema se proporcionan a todos los equipos globalmente en minutos sin necesidad de actualizar.



MACHINE LEARNING

Utiliza la potencia combinada de redes neuronales y algoritmos seleccionados cuidadosamente para determinar correctamente las muestras que llegan como seguras, potencialmente no deseadas o maliciosas.

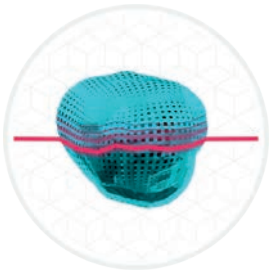
EXPERIENCIA HUMANA

Investigadores líderes a nivel mundial compartiendo su experiencia y conocimientos para garantizar la mejor respuesta frente a amenazas en todo momento.

Una única capa de defensa no es suficiente para un escenario en constante cambio como es el de las amenazas informáticas. Todos los productos de seguridad ESET tienen la capacidad de detectar el malware antes de la ejecución, durante la ejecución y después de su ejecución. Nos centramos en más de una parte específica del ciclo de vida del malware, esto nos permite proporcionar el máximo nivel de protección posible.

MACHINE LEARNING

Todos los productos ESET Endpoint llevan usando aprendizaje automático, además de todas las otras capas de defensa, desde 1997. ESET usa actualmente el aprendizaje automático en conjunción con todas nuestras otras capas de defensa, específicamente en forma de resultado consolidado y redes neuronales.



ANÁLISIS AVANZADO DE MEMORIA

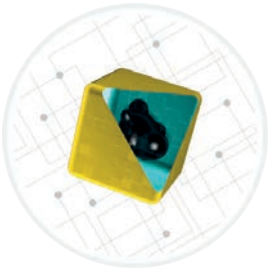
El Análisis avanzado de memoria de ESET monitoriza el comportamiento de un proceso malicioso y lo analiza cuando se ejecuta en memoria. El malware sin archivos opera sin necesidad de componentes persistentes en el sistema de archivos que puedan ser detectados convencionalmente. Solo el análisis de memoria puede descubrir y detener con éxito tales ataques maliciosos.

ESCUDO ANTIRANSOMWARE

El Escudo antiransomware de ESET es una capa adicional que protege a los usuarios frente al ransomware. Esta tecnología monitoriza y evalúa todas las aplicaciones ejecutadas según su comportamiento y reputación. Está diseñado para detectar y bloquear procesos similares al comportamiento del ransomware.

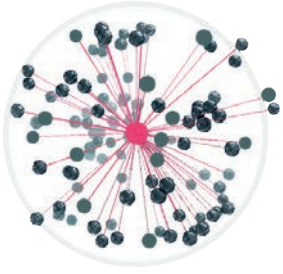
BLOQUEO DE EXPLOITS

El Bloqueo de exploits de ESET monitoriza las aplicaciones cuyas vulnerabilidades pueden ser aprovechadas con facilidad (navegadores, lectores de documentos, clientes de correo electrónico, Flash, Java y muchas más) centrándose en las técnicas de aprovechamiento de las mismas. Cuando se activan, la amenaza se bloquea inmediatamente.



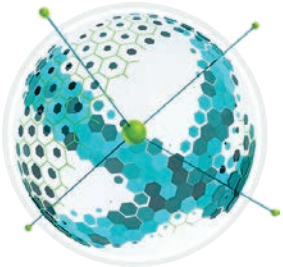
SANDBOX INTEGRADA EN EL PRODUCTO

El malware de hoy en día está fuertemente ofuscado e intenta evitar su detección al máximo. Para llevar a cabo esto e identificar el comportamiento real oculto bajo la superficie, usamos el aislamiento de procesos (sandboxing) integrado en el producto. Con la ayuda de esta tecnología, las soluciones ESET emulan diferentes componentes del hardware y software del equipo para ejecutar una muestra sospechosa en un entorno virtualizado aislado.



PROTECCIÓN ANTIBOTNETS

La Protección antibotnets de ESET detecta las comunicaciones maliciosas usadas por las botnets y al mismo tiempo identifica los procesos ofensivos. Se bloquean todas las comunicaciones maliciosas detectadas y se informa al usuario.



PROTECCIÓN CONTRA ATAQUES DE RED

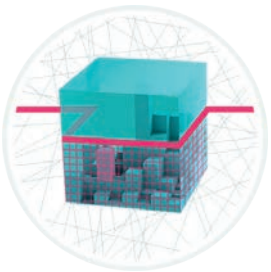
Esta protección mejora la detección de vulnerabilidades conocidas a nivel de red. Constituye otra capa importante de protección contra el malware, los ataques a través de la red, y el aprovechamiento de vulnerabilidades para las que todavía no se ha lanzado o creado ningún parche.

DETECCIONES POR ADN

Los tipos de detección varían desde hashes muy específicos hasta las detecciones por ADN de ESET, que son definiciones complejas de comportamiento malicioso y características de malware. Mientras el código malicioso puede ser fácilmente modificado u ofuscado por los atacantes, el comportamiento de los objetos no puede ser modificado tan fácilmente. Por eso, las detecciones por ADN de ESET han sido diseñadas para aprovecharse de este principio.

HIPS

El Sistema de prevención de intrusiones de ESET monitoriza la actividad del sistema y utiliza un conjunto predefinido de reglas para reconocer comportamientos sospechosos en el sistema. Además, el mecanismo de autodefensa HIPS evita que el proceso de ataque lleve a cabo la actividad dañina.

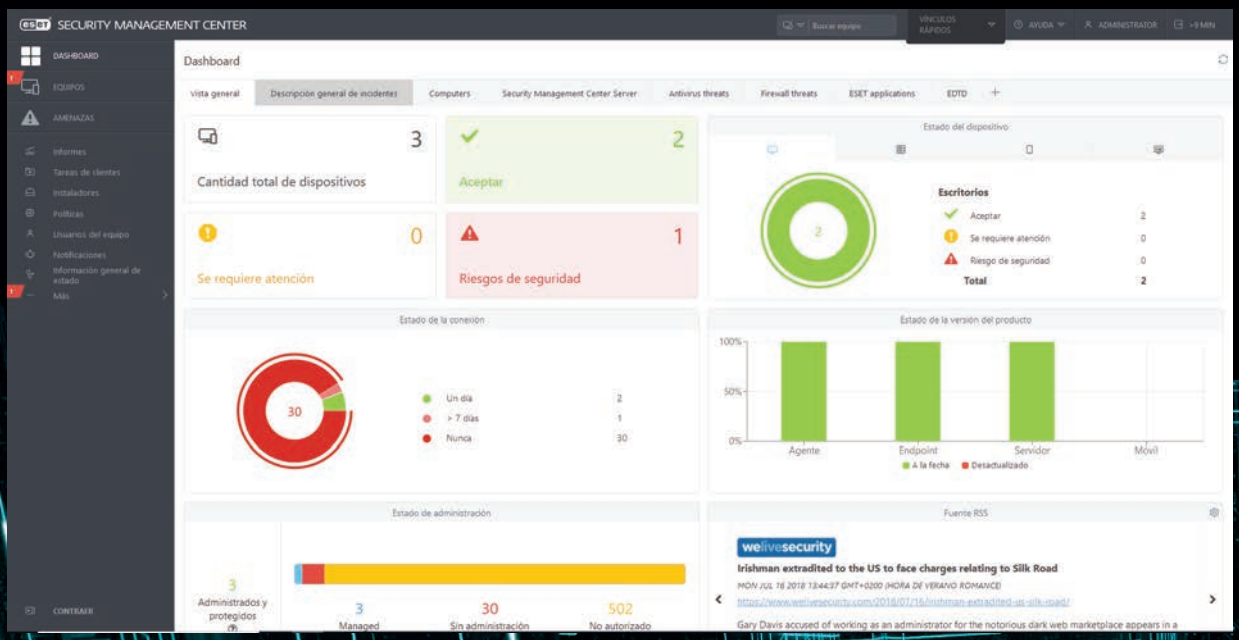


ANÁLISIS DE LA UEFI

ESET es el primer fabricante de seguridad para equipos en añadir una capa específica a su solución que protege la UEFI (Interfaz de Firmware Extensible Unificada). El Análisis de la UEFI de ESET revisa y refuerza la seguridad del entorno de prearranque y está diseñado para monitorizar la integridad del firmware. Si se detecta alguna modificación, lo notifica al usuario.

"Lo que más destaca es su fuerte ventaja técnica sobre otros productos del mercado. ESET nos ofrece una seguridad fiable, lo cual significa que puedo trabajar en cualquier proyecto en cualquier momento sabiendo que nuestros equipos están protegidos al 100%."

Fiona Garland, analista de negocio en Mercury Ingeniería, Irlanda; 1.300 puestos



ESET PROTEC

Todas las soluciones de ESET Endpoint se administran desde un único panel de control: ESET PROTEC, que puede instalarse en Windows o Linux. Además de instalarlo, ESET tiene una aplicación virtual que puedes importar con facilidad para una instalación fácil y rápida.

"Cuando descubrimos ESET sabíamos que era la opción adecuada: una tecnología fiable, detección robusta, presencia local y un excelente soporte técnico... Todo lo que necesitábamos."

-Ernesto Bonhoure, director de sistemas informáticos; Hospital Alemán, Argentina, +1.500 puestos

Casos de uso

Malware sin archivos

El malware sin archivos es una amenaza relativamente nueva y, debido a que solo existe en memoria, requiere un enfoque diferente al malware tradicional basado en archivos.

SOLUCIÓN

- ✓ Una tecnología única de ESET, el Análisis avanzado de memoria, protege contra este tipo de amenaza monitorizando el comportamiento de procesos maliciosos y analizándolos cuando se ejecutan en la memoria.
- ✓ Reduce la recopilación de información y el tiempo de investigación cargando la amenaza a ESET Threat Intelligence para proporcionar información sobre cómo funciona la amenaza.
- ✓ La tecnología multicapa, el aprendizaje automático y la experiencia humana proporcionan a nuestros clientes el mejor nivel de protección posible.

Amenazas zero-day

Las amenazas zero-day constituyen una preocupación importante para las empresas porque no saben cómo protegerse contra algo que no han visto antes.

SOLUCIÓN

- ✓ Los productos ESET Endpoint hacen uso de la heurística y del aprendizaje automático como parte de nuestro enfoque multicapa para prevenir y proteger contra malware nunca antes visto.
- ✓ 13 laboratorios de I+D globales para responder rápidamente al malware sugieren que a la primera incidencia se inicia la investigación en cualquier parte del mundo.
- ✓ El sistema de protección en la nube de ESET protege automáticamente contra nuevas amenazas sin necesidad de esperar a la próxima actualización.

Ransomware

Algunas empresas quieren la seguridad adicional de que estarán protegidos frente a ataques de ransomware.

SOLUCIÓN

- ✓ La Protección contra ataques de red tiene la capacidad de evitar que el ransomware infecte los equipos bloqueando los exploits a nivel de red.
- ✓ Nuestra defensa multicapa proporciona una sandbox integrada en el producto que puede detectar el malware que intenta evitar su detección usando la ofuscación del código.
- ✓ Hace uso del sistema de protección ESET contra malware en la nube para proteger automáticamente contra nuevas amenazas sin necesidad de esperar a la próxima actualización.
- ✓ Todos los productos contienen protección en forma de Escudo antiransomware para garantizar que las empresas estén protegidas frente al cifrado malicioso de archivos.

Acerca de ESET

ESET, pieza clave en la seguridad de la información, ha sido nombrado el único Challenger en el Cuadrante mágico Gartner para plataformas de protección de equipos*

Durante más de 30 años, ESET ha desarrollado programas de seguridad informática y servicios líderes en el sector, que proporcionan una protección exhaustiva al instante contra las amenazas a la seguridad informática en constante evolución para empresas y consumidores en todo el mundo.

ESET es una empresa privada. Sin deudas ni préstamos, tenemos la libertad de hacer lo necesario para la máxima protección de todos nuestros clientes.

ESET EN NÚMEROS

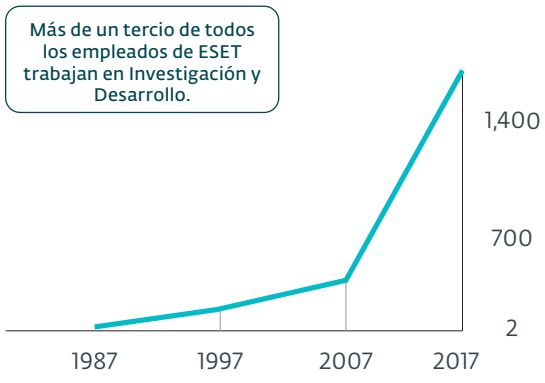
+110M
usuarios en todo el mundo

+400k
clientes empresa

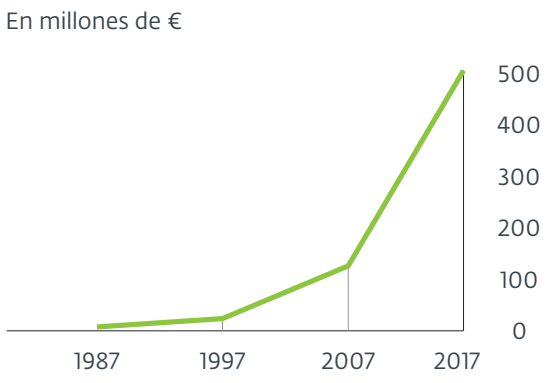
+200
países y territorios

13
centros globales de I+D

EMPLEADOS DE ESET



FACTURACIÓN DE ESET



*Gartner no promociona a ningún fabricante, producto o servicio que aparezca en sus artículos de investigación. Los artículos de investigación de Gartner representan la opinión de la empresa de investigación Gartner y no deberían interpretarse como exposición de hechos. Gartner niega cualquier responsabilidad, expresa o implícita, respecto a esta investigación, incluyendo toda garantía de comercialización o idoneidad para un objetivo determinado.

ALGUNOS DE NUESTROS CLIENTES

MITSUBISHI MOTORS
Drive your Ambition

protegido por ESET desde 2017,
más de 14.000 equipos

Canon
Canon Marketing Japan Group

protegido por ESET desde 2016,
más de 9.000 equipos

Allianz Suisse

protegido por ESET desde 2016,
más de 40.000 buzones de correo

Distribuidor ISP desde 2008.
2 millones de clientes base

ALGUNOS DE NUESTROS PREMIOS MÁS IMPORTANTES

"Cash Converters necesita una solución segura y eficaz ante la sofisticación de los últimos virus divulgados. Seguiremos confiando en ESET, ya que ha reunido todos los requisitos para aportar un valor añadido a las soluciones de IT".

David Polonio, CIO de Cash Converters

ENJOY SAFER TECHNOLOGY™