



# ENDPOINT SOLUTIONS

La tecnología de protección multicapa, el machine learning y un equipo experimentado de personas trabajando juntos, proporcionan un equilibrio perfecto para la protección de tus equipos. Somos el proveedor nº1 de la Unión Europea.

**Progress. Protected.**



# ¿Qué es una Plataforma de Protección de equipos?

**Una plataforma de protección de equipos (EPP) es una solución que se instala en dispositivos para prevenir ataques de malware basados en archivos, detectar actividad maliciosa y proporcionar la capacidad de investigación y solución necesarias para responder eficaz y rápidamente a incidencias y alertas de seguridad.**

Las soluciones de protección de equipos de ESET usan un enfoque multicapa con múltiples tecnologías funcionando conjuntamente para obtener un equilibrio constante de rendimiento, detección y falsos positivos.

# ¿Por qué elegir las Soluciones de Protección de equipos?

## 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 se quede inoperativa por el cifrado de 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.

Las soluciones de protección de endpoints de ESET proporcionan capas de defensa no solo para prevenir el ransomware, sino para detectarlo si en algún momento hay un ataque a algún dispositivo de la empresa. Es importante prevenir y detectar el ransomware, ya que cada vez que se paga un rescate se está animando a los ciberdelincuentes 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.

Las soluciones de protección de endpoints de ESET recopilan la información de las amenazas (threat intelligence) a través de los productos de protección instalados por todo el mundo. Usa los equipos como sensores gracias a su presencia global para priorizar y bloquear eficazmente las últimas amenazas antes de que se propaguen por otros lugares del mundo. Además, las plataformas de protección de endpoints proporcionan actualizaciones en la nube para responder rápidamente a cualquier tipo de ataque antes de esperar a la actualización habitual.

## 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 de estos ataques usan aplicaciones legítimas, instaladas en el equipo, para que la parte maliciosa sea más difícil de detectar. Por ejemplo, el uso de PowerShell en estos ataques es muy común.

Las diferentes capas de protección de ESET poseen sistemas para detectar aplicaciones ilegítimas o secuestradas para proteger contra ataques sin archivos. ESET también ha creado motores de análisis dedicados para analizar la memoria constantemente en busca de cualquier elemento sospechoso. Usando este enfoque multicapa, nos aseguramos de permanecer siempre un paso por delante de las últimas ciberamenazas.

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

Cuando se produce un ataque o fuga de información, las empresas se sorprenden de que sus defensas hayan sido puestas en riesgo o ni tan siquiera son conscientes de que ha ocurrido el ataque.

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



# Soluciones ESET para la protección de endpoints

ESET Endpoint Security para Windows/macOS/Android

ESET Endpoint Antivirus para Windows/macOS/Linux Desktop

ESET Server Security para Windows Server/Linux/Azure

ESET MDM para macOS y iPadOS

# ESET marca la diferencia

## PROTECCIÓN MULTICAPA

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

## EL MEJOR RENDIMIENTO

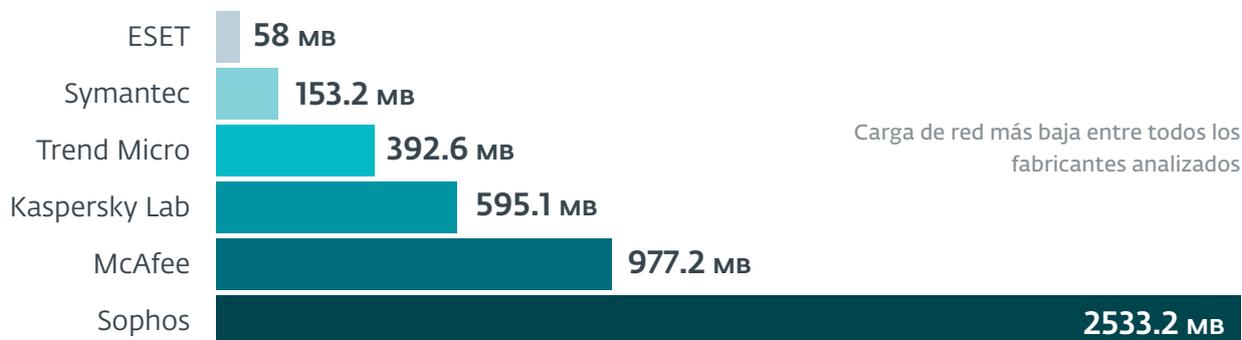
En la mayoría de los casos, la mayor preocupación de las empresas es el impacto que produce la solución de protección en el rendimiento de sus equipos. Los productos ESET continúan ofreciendo un rendimiento sobresaliente y son líderes en los análisis de terceros que evalúan el impacto de las soluciones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

## PROTECCIÓN MULTIPLATAFORMA

Los productos de protección ESET para empresas son compatibles con todos los sistemas operativos incluyendo Windows, macOS, Linux y Android. Todos los productos pueden ser administrados completamente desde un único panel de control, también con Mobile Device Management para iOS y Android totalmente integrado.

## PRESENCIA GLOBAL

ESET cuenta con oficinas en 22 países en todo el mundo, 13 en laboratorios de I+D 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.



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

*“¿... 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 Engineering, Irlanda. 1.300 puestos

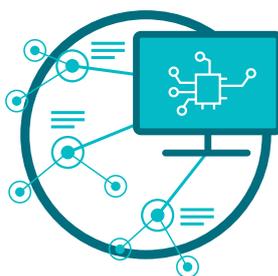
# La tecnología

## 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 pocos minutos sin necesidad de hacer nada por parte del administrador de sistemas y sin tener que actualizar los productos ESET.



### 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

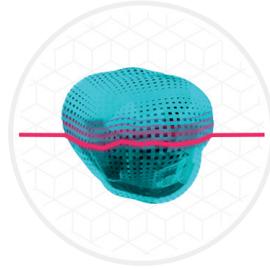
Investigadores líderes a nivel mundial compartiendo su experiencia y conocimientos para garantizar la mejor respuesta frente a amenazas en todo momento.

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 machine learning, además de todas las otras capas de defensa, desde 1997. ESET usa actualmente el machine learning 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.



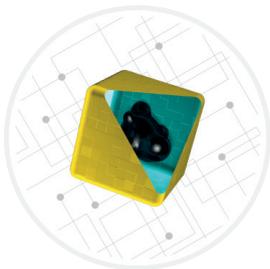
## ESCUDO ANTIRANSOMWARE

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.



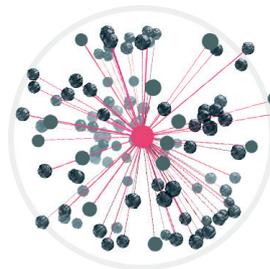
## BLOQUEO DE EXPLOITS

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.



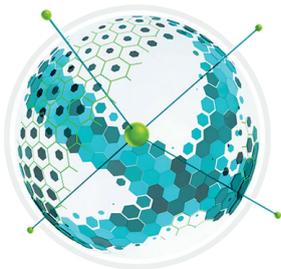
## SANDBOX INTEGRADA EN EL PRODUCTO

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.



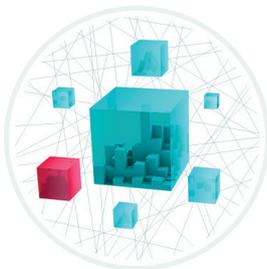
## PROTECCIÓN CONTRA ATAQUES DE RED

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.



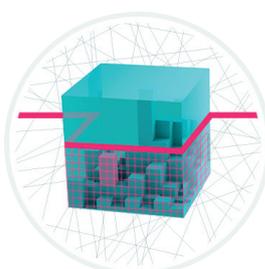
## NAVEGADOR SEGURO

Protección diseñada especialmente para proteger los activos de la empresa, se centra en el navegador, ya que es la principal herramienta utilizada para acceder a datos críticos dentro del perímetro de intranet y en la nube. Proporciona protección mejorada de memoria para el proceso del navegador, junto con la protección del teclado, y permite a los administradores agregar las URL que necesiten proteger.



## 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.

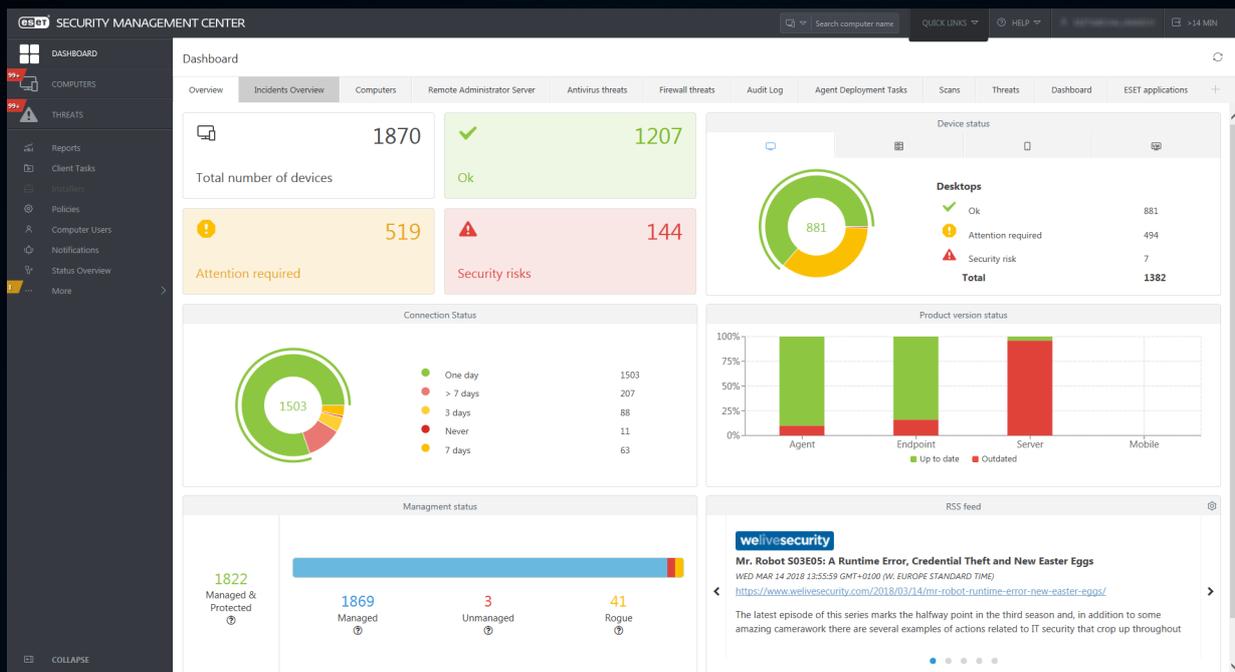


## ANÁLISIS DE LA UEFI

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.

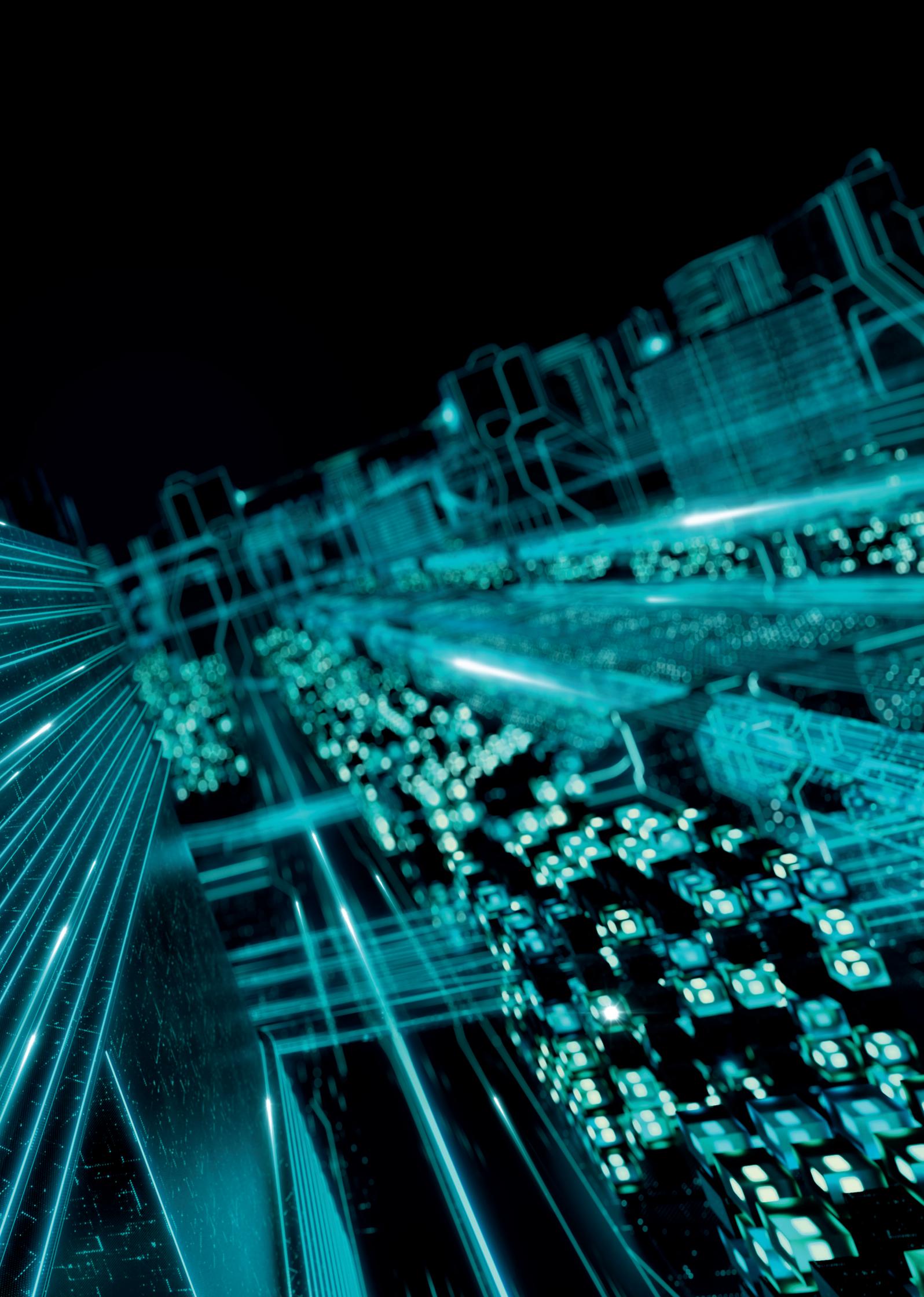
*“Lo que más destaca es su fuerte ventaja técnica sobre otros productos del mercado. ESET nos ofrece una seguridad fiable, lo cual significa que puedo trabajar en cualquier proyecto en cualquier momento sabiendo que nuestros equipos están protegidos al 100%.”*

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



## ESET PROTECT On-Prem

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



# Casos de uso

## Ransomware

Algunas empresas requieren una seguridad adicional que los proteja de los 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 de ESET en la nube contra el malware 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.

## Robo de datos

Los ataques de phishing cada vez son más frecuentes, actúan a través de páginas web fraudulentas que se hacen pasar por legítimas para acceder a tus datos.

### SOLUCIÓN

- ✓ Los productos endpoint de ESET están diseñados para proteger los activos de la empresa con una única capa de protección, centrándose en el navegador como herramienta principal para acceder a los datos críticos dentro del perímetro de intranet y en la nube.
- ✓ La función de navegador seguro protege los datos confidenciales mientras estás navegando en línea.
- ✓ Con un solo clic, los administradores pueden decidir qué portales bancarios y de pagos incluir para proteger al navegador de sitios web específicos.

## 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.

*“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

# Acercas de ESET

Durante más de 30 años, ESET® ha desarrollado software y servicios de seguridad informática líderes en el sector para ofrecer una protección completa y multicapa contra las ciberamenazas a empresas y consumidores de todo el mundo.

ESET es pionera en tecnologías de aprendizaje automático y en la nube que previenen, detectan y responden al malware. ESET es una empresa privada que promueve la investigación y el desarrollo científico en todo el mundo.

## ESET EN CIFRAS

|  |  |  |  |
|--|--|--|--|
| <b>+110M</b><br>de usuarios<br>seguros en todo<br>el mundo | <b>+400k</b><br>clientes de<br>empresa | <b>+200</b><br>países y<br>territorios | <b>13</b><br>centros de I+D<br>en el mundo |
|--|--|--|--|

## ALGUNOS DE NUESTROS CLIENTES



**MITSUBISHI  
MOTORS**

Drive your Ambition

Protegido por ESET desde  
2017, con más de 9.000  
endpoints

**Canon**

Canon Marketing Japan Group

Protegidos por ESET desde  
2016, con más de 32.000  
endpoints

**Allianz**   
Suisse

Protegido por ESET desde  
2016, con más de 4.000  
buzones de correo



Colaborador de seguridad de  
ISP desde 2008, con una base  
de 2 millones de clientes

# ¿Por qué elegir ESET?



ESET cumple la norma [ISO/IEC 27001:2013](#), una norma de seguridad reconocida y aplicable internacionalmente en el despliegue y la gestión de la seguridad de la información. La certificación es otorgada por el organismo de certificación acreditado por [SGS](#) y demuestra el cumplimiento total de ESET de las mejores prácticas de la industria.

## ALGUNOS DE NUESTROS PREMIOS MÁS IMPORTANTES



## RECONOCIMIENTO DE LOS ANALISTAS

### Gartner

ESET fue nombrado el único Challenger en 2019 en el Gartner Magic Quadrant para plataformas de protección de endpoints, por segundo año consecutivo.

### FORRESTER®

Las soluciones de ESET son constantemente reconocidas por las principales firmas analistas, incluyendo en "The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021" como fabricante ejemplar.

### THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

ESET "Top Player" por tercera vez en Radicati APT Protection MQ 2022.

Gartner Inc, Magic Quadrant para plataformas de protección de endpoints, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, 20 de agosto de 2019. Gartner no respalda a ningún proveedor, producto o servicio descrito en sus publicaciones de investigación. Los estudios publicados por Gartner recogen solo las opiniones de la organización de investigación de Gartner y no deben considerarse declaraciones de hechos. Gartner excluye cualquier garantía, explícita o implícita, en relación con este estudio, incluidas las garantías de comercialización o idoneidad para un uso en concreto.

Gartner Peer Insights es una plataforma gratuita de revisión y calificación por pares diseñada para los responsables de la toma de decisiones de software y servicios empresariales. Las reseñas pasan por un estricto proceso de validación y moderación para garantizar la autenticidad de la información. Las reseñas de Gartner Peer Insights representan las opiniones subjetivas de usuarios basadas en sus propias experiencias y no representan los puntos de vista de Gartner o sus asociados.



Digital Security  
Progress. Protected.

