



MAIL SECURITY

Protege tu servidor de correo electrónico, el vector de ataque más común

**CYBERSECURITY
EXPERTS ON YOUR SIDE**



¿Qué es una solución de seguridad para el correo electrónico?

Un producto de seguridad para el correo electrónico está diseñado para proteger este vector de ataque a la red de la empresa, ofreciendo protección directamente a través del servidor de correo. El correo electrónico es uno de los vectores más vulnerables con más del 90% del ransomware llegando a los usuarios por esta vía. Además de proteger contra las amenazas, también protege contra el correo basura (spam) y el phishing.

ESET Mail Security proporciona una capa adicional de seguridad a las empresas interesadas en impedir que las amenazas lleguen a sus usuarios con una seguridad multicapa proporcionada desde el propio servidor de correo.

¿Por qué elegir una solución de seguridad para el correo electrónico?

RANSOMWARE

El ransomware sigue siendo 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.

Las soluciones ESET de protección del correo electrónico proporcionan una capa de defensa adicional para evitar que el ransomware llegue a los buzones de correo de los usuarios. Además, la capacidad de bloquear ciertos tipos de archivos adjuntos limita más la exposición de la empresa al ransomware.

PROTECCIÓN ANTISPAM

La mayoría de usuarios de empresa ya tienen suficiente trabajo como para estar seleccionando entre grandes cantidades de correo basura (spam) para encontrar los correos electrónicos más importantes. De hecho, más del 54% de todo el correo entrante es correo basura. Los usuarios se enfrentan a muchos problemas para ser eficientes como para tener que determinar si cada correo electrónico que reciben es legítimo o no.

Las soluciones ESET Mail Security hacen la vida de los usuarios mucho más fácil evitando que el correo basura llegue a su cuenta de correo. Así, el filtrado del correo se lleva a cabo por el producto de seguridad en vez de por el usuario. Además de aumentar la eficiencia de la empresa, aumentará la seguridad porque los usuarios no tendrán la oportunidad de hacer clic en enlaces de correo no deseado de forma accidental.

La capacidad de bloquear ciertos tipos de documentos adjuntos limita más la exposición de la empresa al ransomware.

Más del 54% de todo el correo entrante es no deseado

“Como decimos en el hospital, mejor prevenir que curar.”

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

Las soluciones ESET Mail Security hacen la vida de los usuarios mucho más fácil evitando que el correo no deseado llegue a su cuenta de correo



Soluciones ESET de seguridad para el correo electrónico

ESET Mail Security para Microsoft Exchange Server

ESET Mail Security para IBM Domino

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

Fiona Garland, Analista de negocio del Grupo IT, Mercury Ingeniería, Irlanda, 1.300 puestos

“Contar con una seguridad administrada de forma centralizada en todos los equipos, servidores y dispositivos móviles ha sido una gran ventaja para nosotros. Sin embargo, las capacidades de monitorización, la eficacia y un precio menor que otros productos de seguridad también fue considerado a su favor.”

Director de sistemas; Diamantis Masoutis S.A., Grecia; +6.000 puestos

ESET marca la diferencia

ADMINISTRACIÓN TOTAL DE LA CUARENTENA

Los usuarios reciben correos electrónicos después de pasar por la cuarentena y pueden tratar los mensajes por ellos mismos. Además, los administradores pueden recibir informes de resumen con regularidad. Si alguna vez alguien está esperando un correo electrónico, el administrador puede decidir fácilmente si se elimina o libera el mensaje desde la cuarentena central.

PROTECCIÓN MULTICAPA

La primera capa funciona con nuestra tecnología antispam propia, que filtra los mensajes de correo no deseado con casi el 100% de precisión, como lo demuestran diversos análisis realizados por terceros. Una segunda capa es nuestro análisis antimalware, que detecta los documentos adjuntos sospechosos. También puede implementarse una capa adicional en forma de sandbox en la nube con ESET Dynamic Threat Defense.

TECNOLOGÍA PROPIA

Las soluciones ESET Mail Security utilizan un antispam, antiphishing y la protección del servidor a nivel del host de desarrollo propio en combinación con el machine learning, big data y la experiencia humana para obtener una única plataforma de seguridad para el correo electrónico premiada por diversos organismos independientes.

COMPATIBLE CON CLÚSTERES

Las soluciones ESET son compatibles con la creación de clústeres que permitan comunicarse unos con otros e intercambiar la configuración, notificaciones, información de la lista gris y otros. Además, es compatible con los clústers Windows Failover Clusters y Network Load Balancing (NLB) para obtener una protección a nivel de una gran empresa.

VELOCIDAD

El rendimiento y la estabilidad se encuentran entre las características más importantes de un producto para correo electrónico. Las empresas necesitan la seguridad de que su correo electrónico va a ser procesado sin retrasos. Este producto de ESET cuenta con 64 bits reales que permiten la creación de clústeres para garantizar que la velocidad nunca sea una preocupación para las empresas de cualquier tamaño.

EXPERIENCIA HUMANA REFORZADA POR EL MACHINE LEARNING

El uso del machine learning para automatizar decisiones y evaluar las posibles amenazas es una parte importante de nuestra estrategia, pero no la única. La experiencia humana es primordial para proporcionar la inteligencia más precisa posible frente a amenazas, ya que los creadores de amenazas son adversarios inteligentes.

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.

Casos de uso

Ransomware

El ransomware tiende a acceder a las cuentas de correo de usuarios confiados a través del correo electrónico.

SOLUCIÓN

- ✓ ESET Mail Security analiza el documento adjunto para determinar si es malicioso, desconocido o seguro.
- ✓ ESET Mail Security evalúa si un administrador ha introducido determinadas reglas al correo electrónico para evitar que los usuarios envíen cierto tipo de documentos adjuntos o determinados tamaños de archivos.
- ✓ Si ESET Mail Security no está seguro sobre la amenaza potencial, puede reenviar el documento adjunto a la solución adicional, ESET Dynamic Threat Defense, para su análisis.
- ✓ Dynamic Threat Defense entonces analiza la muestra en una sandbox en la nube, y envía el resultado de nuevo a Mail Security en unos minutos.
- ✓ Si se descubre que el archivo es malicioso, ESET Mail Security destruye automáticamente el correo electrónico con el contenido malicioso.

Combatir el phishing

Los usuarios reciben constantemente campañas de phishing que podrían contener otros componentes maliciosos.

SOLUCIÓN

- ✓ El sistema de alerta temprana ESET Threat Intelligence notifica sobre las campañas de phishing.

- ✓ Pueden implementarse reglas en ESET Mail Security para evitar recibir correos desde países y dominios maliciosos conocidos.

- ✓ ESET Mail Security usa un analizador sofisticado que busca en el cuerpo del mensaje del asunto para identificar enlaces maliciosos.

- ✓ Todos los correos con archivos o enlaces maliciosos entran en cuarentena, evitando así que los reciban los usuarios.

Prevenir problemas de continuidad de la empresa reduciendo el spam

Un usuario no será eficiente si tiene que decidir si los correos electrónicos son legítimos o no. Además, cada correo electrónico puede reenviarse al departamento de sistemas para confirmar su legitimidad.

SOLUCIÓN

- ✓ ESET Mail Security analiza el correo electrónico usando una tecnología propia para determinar si el correo es legítimo o spam.
- ✓ Los correos electrónicos sospechosos de spam entran en cuarentena y a los usuarios se les envía un mensaje indicando que se ha realizado esta acción.
- ✓ Los administradores, además del usuario que recibió el correo electrónico, pueden liberar correos o eliminarlos para evitar que lleguen al usuario.

Características técnicas de ESET Mail Security

ANTISPAM

Con nuestro propio motor de análisis premiado se evita que el spam llegue a los buzones de correo de tus usuarios. Incluye la validación SPF y DKIM, protección de la retrodispersión y del protocolo SMTP.

ANTIMALWARE

Nuestra segunda capa de protección integrada en ESET Mail Security proporciona detección de documentos adjuntos sospechosos o maliciosos para evitar que los usuarios se infecten.

PROTECCIÓN ANTIPHISHING

Evita que los usuarios accedan a páginas web conocidas por usar ataques de phishing, analizando el cuerpo de los mensajes y asuntos para identificar las URLs. Estas se comparan con una base de datos de URLs de phishing y otras reglas para decidir si el mensaje es legítimo o malicioso.

ANÁLISIS DE OFFICE 365 HÍBRIDO

Es compatible con empresas que usan Microsoft Exchange en una configuración híbrida.

REGLAS

El sistema exhaustivo de reglas de ESET permite a los administradores definir manualmente las condiciones del filtrado de correo electrónico y las acciones a tomar con los correos filtrados.

CUARENTENA BASADA EN WEBS

Se envían automáticamente correos electrónicos a los usuarios sobre sus correos spam que han sido enviados a la cuarentena. Los usuarios pueden iniciar sesión y administrar su propio correo spam en vez de ser gestionado por el administrador.

ESET Mail Security analiza el correo electrónico usando tecnología propia para determinar si un correo electrónico es legítimo o spam.

ESET Mail Security usa un sofisticado analizador que busca en el cuerpo del mensaje y en la línea de asunto para identificar enlaces maliciosos.

Acercas de ESET

Durante más de 30 años, ESET® ha desarrollado software y servicios de seguridad informática líderes en el sector, ofreciendo una protección inmediata y completa para las amenazas cambiantes de ciberseguridad para empresas y consumidores de todo el mundo.

ESET es una empresa privada. Sin deudas ni préstamos, somos libres de hacer lo que haya que hacer para ofrecer la máxima protección a todos nuestros clientes.

ESET EN CIFRAS

+110M de usuarios en todo el mundo	+400k clientes de empresa	+200 países y territorios	13 centros de I+D en el mundo
---	--	--	--

ALGUNOS DE NUESTROS CLIENTES



protegidos con ESET desde 2017,
con más de 14 000 endpoints



protegidos por ESET desde 2016,
más de 9 000 endpoints



protegidos con ESET desde 2016,
con más de 4 000 buzones de correo



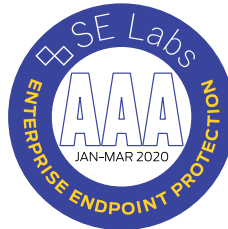
Colaborador de seguridad de ISP desde 2008,
con una base de 2 millones de clientes

¿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®

ESET recibió la calificación de «Strong Performer» en el Forrester Wave(TM): Suites de seguridad de endpoints, tercer trimestre de 2019.

THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

ESET recibió la calificación de «Top Player» en el informe 2019 Radicati Endpoint Security según dos criterios: funcionalidad y visión estratégica.

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.



ENJOY SAFER
TECHNOLOGY™