



MAIL SECURITY

Protección para los usuarios y sus
correos: el vector de ataque más
utilizado

PROGRESS. PROTECTED



¿Qué es la **seguridad para correo?**

Los productos de seguridad para correo están diseñados para proteger el vector de ataque principal de las amenazas que ingresan a la red: el correo electrónico. Este es uno de los vectores más vulnerables; más del 90% del ransomware se distribuye a través de este medio. Además de las amenazas, las soluciones de seguridad para correo también brindan protección contra el spam y el phishing.

ESET Mail Security les proporciona a las organizaciones una capa adicional de seguridad para impedir que las amenazas lleguen a los usuarios. Suministra protección en múltiples capas directamente del propio host.

¿Por qué es importante la seguridad para correo?

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.

Las soluciones ESET Mail Security proporcionan una capa adicional de defensa para evitar que el ransomware llegue a los buzones de los usuarios. Además, la capacidad de bloquear algunos o todos los tipos de archivos adjuntos limita aún más la exposición de la organización al ransomware.

PROTECCIÓN CONTRA SPAM

Los usuarios de la mayoría de las organizaciones ya tienen suficiente trabajo sin necesidad de tener que filtrar grandes cantidades de correo no deseado para encontrar los que sí son relevantes. De hecho, más del 54% de todos los correos electrónicos entrantes son spam. Los usuarios no serán eficientes en su trabajo si deben revisar uno de cada dos correos para determinar si son spam o no.

Las soluciones ESET Mail Security facilitan la vida de los usuarios ya que evitan que el spam llegue a su buzón de correo. Deje la decisión en manos del producto de seguridad para correo y no del usuario. Además de aumentar la eficiencia de la organización, mejorará la seguridad, porque los usuarios no tendrán la oportunidad de hacer clic, ya sea accidental o intencionalmente, en los vínculos de los correos de spam.

La capacidad de bloquear algunos o todos los tipos de archivos adjuntos limita aún más la exposición de la organización al ransomware.

Más del 54% de los correos electrónicos entrantes son spam

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

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

Las soluciones ESET Mail Security facilitan la vida de los usuarios ya que evitan que el spam llegue a su buzón de correo



Soluciones de ESET para correo electrónico

ESET Mail Security para Microsoft Exchange Server
ESET Mail Security para IBM Domino

“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

“Para nosotros, la administración central de la seguridad de todas las endpoints, los servidores y los dispositivos móviles fue un beneficio clave. Otras ventajas importantes fueron la capacidad de monitoreo, la efectividad y el menor costo comparado a otros productos de seguridad.”

Gerente de TI; Diamantis Masoutis S.A., Grecia; más de 6.000 equipos

¿En qué se diferencia ESET?

SÓLIDA ADMINISTRACIÓN DE LA CUARENTENA

Los usuarios reciben un aviso por correo electrónico cuando uno de sus mensajes se pone en cuarentena y pueden gestionarlo ellos mismos. Además, los administradores reciben informes con resúmenes periódicos. De todas formas, si en algún momento alguien está esperando recibir un mensaje de correo electrónico específico, el administrador puede eliminar o liberar fácilmente el mensaje de la cuarentena central.

PROTECCIÓN EN MÚLTIPLES CAPAS

La primera capa de defensa está compuesta por nuestra tecnología exclusiva antispam, que filtra los mensajes de spam con casi el 100% de precisión, como lo demuestran las pruebas de terceros. En la segunda capa, nuestro módulo de exploración antimalware se encarga de detectar archivos adjuntos sospechosos. Se puede implementar una tercera capa adicional con ESET Dynamic Threat Defense, que prueba los archivos en un sandboxing en la nube.

TECNOLOGÍA EXCLUSIVA DE ESET

Las soluciones ESET Mail Security utilizan su propia tecnología Antispam, Anti-Phishing y de protección de servidores host, combinando el machine learning, la gestión de grandes grupos de datos y la experiencia humana en una única plataforma multipremiada de seguridad para correo.

SOPORTE PARA ENTORNOS DE CLÚSTER

Las soluciones de ESET admiten la creación de clústeres, lo que les permite a los productos comunicarse entre sí e intercambiar configuraciones, notificaciones, información de la base de datos de listas grises, entre otros datos. Además, admiten los clústeres de conmutación por error de Windows y los clústeres de equilibrio de carga de red para permitir la protección de grandes corporaciones.

VELOCIDAD

El rendimiento y la estabilidad se encuentran entre las características más importantes de los productos para correo. Las empresas necesitan asegurarse de que sus correos electrónicos se procesarán sin demoras. ESET presenta un verdadero producto de 64 bits que admite el uso de clústeres para garantizar que las organizaciones de cualquier tamaño nunca deban preocuparse por la velocidad.

EXPERIENCIA HUMANA, CON EL RESPALDO DEL MACHINE LEARNING

El uso de técnicas de machine learning para automatizar las decisiones y evaluar las posibles amenazas es una parte vital de nuestro enfoque; de todas formas, sólo será tan fuerte como las personas que administran el sistema. La experiencia humana es primordial para proporcionar la inteligencia de amenazas más precisa posible, dado que los actores maliciosos son oponentes inteligentes.

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.

Casos de uso

Ransomware

El ransomware llega a través del correo electrónico y logra ingresar a los buzones de los usuarios desprevénidos.

SOLUCIÓN

- ✓ ESET Mail Security analiza los archivos adjuntos para determinar si son maliciosos, desconocidos o seguros.
- ✓ ESET Mail Security evalúa si un administrador ingresó reglas de correo electrónico específicas para impedir que se envíen ciertos tipos o tamaños de archivos adjuntos a los usuarios.
- ✓ Si ESET Mail Security no logra determinar con seguridad si un archivo adjunto es una posible amenaza, lo reenvía a la solución complementaria ESET Dynamic Threat Defense para su análisis.
- ✓ A continuación, ESET LiveGuard Advanced analiza la muestra en sandboxing en la nube y luego envía el resultado a Mail Security en un lapso de pocos minutos.
- ✓ Si ESET Mail Security descubre que el archivo es malicioso, destruye automáticamente el correo electrónico que lo contiene.

Detener el phishing

Los usuarios reciben ataques constantes de campañas de phishing que pueden contener componentes maliciosos.

SOLUCIÓN

- ✓ El sistema de alerta temprana ESET Threat Intelligence notifica sobre las campañas activas de phishing.
- ✓ Se pueden implementar reglas en ESET Mail Security para bloquear los correos electrónicos provenientes de países y dominios maliciosos conocidos.

- ✓ ESET Mail Security utiliza un sofisticado módulo de exploración que busca en el cuerpo y el asunto del mensaje para identificar vínculos maliciosos.

- ✓ Todos los correos electrónicos que contienen archivos o vínculos maliciosos se ponen en cuarentena y los usuarios no los pueden recibir.

Reducción del spam

Los usuarios no son eficientes si tienen que examinar los correos electrónicos para determinar si son legítimos o no. Además, cada correo electrónico no deseado puede enviarse al departamento de TI para confirmar su legitimidad.

SOLUCIÓN

- ✓ ESET Mail Security analiza los correos electrónicos con su tecnología patentada para determinar si son legítimos o si son spam.
- ✓ Cuando se descubre que un correo electrónico es spam, se pone en cuarentena y se envía un mensaje a los usuarios afectados.
- ✓ Además del usuario que recibió el correo electrónico, los administradores también están habilitados a eliminar el correo o liberarlo de cuarentena para su entrega.

Características técnicas de ESET Mail Security

ANTISPAM

El multipremiado motor exclusivo de ESET impide que el spam llegue a los buzones de sus usuarios. Incluye validación SPF y DKIM, así como protección para spam de retrodispersión y SMTP.

ANTIMALWARE

Nuestra segunda capa de protección integrada a ESET Mail Security detecta los archivos adjuntos sospechosos o maliciosos para evitar que infecten a los usuarios.

ANTI-PHISHING

Analiza el cuerpo y el asunto de los mensajes para identificar las direcciones URL e impedir que los usuarios accedan a páginas Web de phishing conocidas. Las URL se comparan con la base de datos y las reglas de phishing para decidir si son inofensivas o maliciosas.

EXPLORACIÓN EN ENTORNOS HÍBRIDOS

Protege las empresas que utilizan Microsoft Exchange en implementaciones híbridas.

REGLAS

El exhaustivo sistema de reglas de ESET les permite a los administradores definir las condiciones de filtrado de los correos y las acciones que se deben realizar con los mensajes filtrados.

CUARENTENA BASADA EN LA WEB

Los usuarios reciben correos electrónicos automáticos sobre los mensajes de spam que fueron puestos en cuarentena. Luego, pueden iniciar sesión y administrar su propio correo de spam en lugar de que lo gestione únicamente el administrador.

ESET Mail Security analiza los correos electrónicos con su tecnología patentada para determinar si son legítimos o si son spam.

ESET Mail Security utiliza un sofisticado módulo de exploración que busca en el cuerpo y el asunto del mensaje para identificar vínculos maliciosos.

Acercas 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



protegido por ESET desde 2017, más de 9.000 endpoints



protegido por ESET desde 2016, más de 4.000 buzones de correo

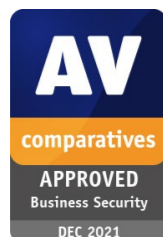


protegido por ESET desde 2016, más de 32.000 endpoints



partner de seguridad ISP desde 2008 con una base de clientes de 2 millones

ALGUNOS DE NUESTROS PREMIOS MÁS IMPORTANTES



ESET recibió el premio Business Security APPROVED de AV-comparatives en el Business Security Test en diciembre de 2021.



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.



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".

