kaspersky PREPARADOS PARA EL FUTURO

Kaspersky Security for Mail Server

Creamos resiliencia frente al vector de ataque más importante

El correo electrónico es el principal vector de ataque que amenaza la seguridad de TI empresarial. Los atacantes utilizan métodos cada vez más sofisticados para infiltrarse en las organizaciones mediante ataques por correo electrónico, lo que genera pérdidas económicas y operativas, así como daños en la reputación. Para combatir esos nuevos desarrollos, las empresas deben pensar en la resiliencia, así como en la protección. Al optimizar su resiliencia y minimizar su superficie de ataque, puede hacer que su negocio sea un objetivo menos atractivo e incluso inviable para los atacantes, independientemente de si su empresa opera una infraestructura de correo electrónico local, en la nube o híbrida.

Vector principal de filtraciones de datos

- Según el Informe de investigaciones de filtración de datos (DBIR) de Verizon, la ingeniería social es el patrón más común que trae aparejada una filtración de datos.
- El informe también establece que "...el phishing sigue siendo una de las principales variedades de acciones en las filtraciones, y lo fue durante los últimos dos años".

Fuente: Informe de investigaciones de filtración de datos de Verizon

Cree su resiliencia en el principal punto de entrada para los ataques

Las aplicaciones de Kaspersky Security for Mail Server permiten crear resiliencia frente a los ataques basados en correo electrónico mediante lo siguiente:

Identificación y filtrado de los correos electrónicos sospechosos o no deseados a nivel de puerta de enlace

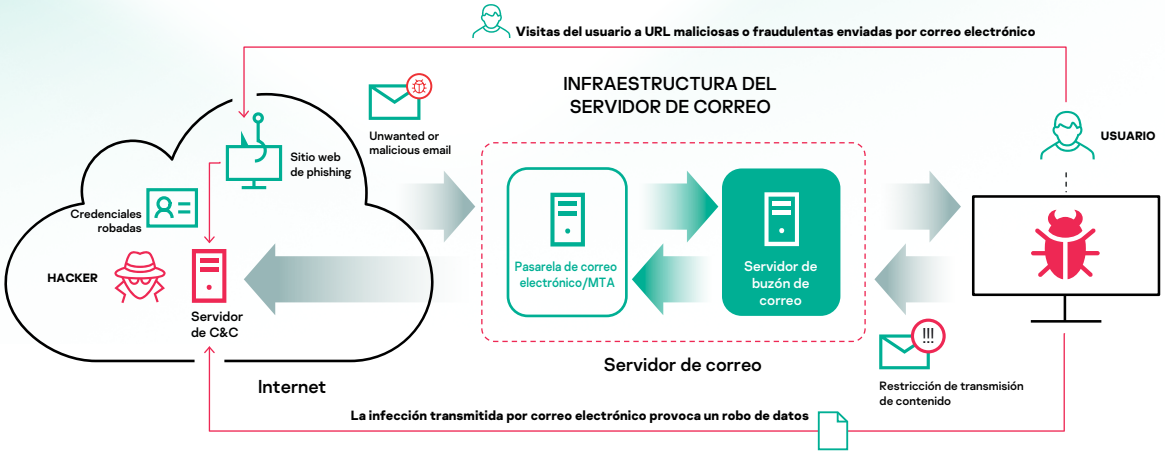
La mayoría de los ataques solo comienza a activarse a nivel de endpoint, y Kaspersky Security for Mail Server los detiene antes de que lleguen a ese nivel. Nuestra galardonada protección fortalece su resiliencia al detectar e interceptar ataques, justo en el inicio de la cadena de ataques, antes de que puedan penetrar su perímetro de seguridad y avanzar hacia sus endpoints y usuarios.

Procesamiento rápido y preciso de correos electrónicos legítimos

El rol fundamental del correo electrónico en las comunicaciones corporativas requiere que el procesamiento de la seguridad sea rápido, ágil y preciso, sin suponer un obstáculo para las comunicaciones legítimas. Kaspersky Security for Mail Server ofrece las tecnologías de protección más efectivas de la industria contra cualquier tipo de amenaza, desde el phishing y el spam hasta el correo electrónico empresarial comprometido (BEC) y el ransomware, sin prácticamente falsos positivos, al tiempo que permite que los correos electrónicos legítimos circulen sin ningún tipo de interrupción.

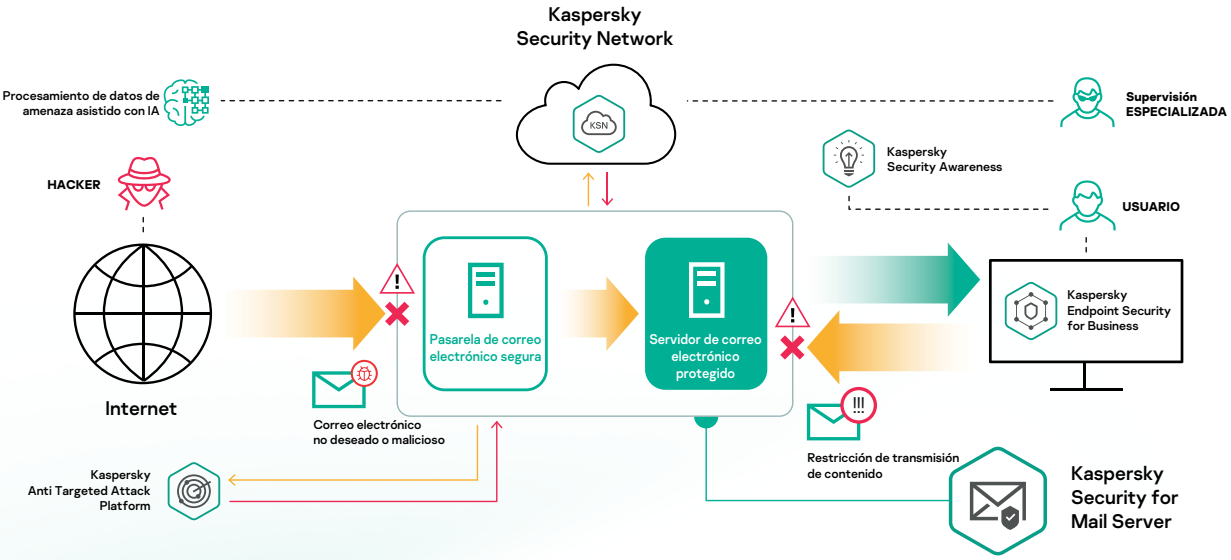
Protección de los correos electrónicos más allá de la puerta de enlace

Kaspersky Security for Mail Server detecta contenido malicioso o no deseado no solamente en la puerta de enlace, sino también en los buzones de correo individuales de Microsoft Exchange Server o Microsoft Exchange Online. Los ataques de phishing retrasados diseñados para evadir las contramedidas en la puerta de enlace, los mensajes de BEC generados después de la apropiación de cuentas y los escenarios de amenazas internas que nunca necesitan pasar a través de la puerta de enlace: todos estos pueden identificarse y erradicarse, lo que hace que la protección del buzón del servidor sea "imprescindible".



Modelo de amenazas basado en el correo electrónico

Características clave



Cómo Kaspersky Security for Mail Server combate las ciberamenazas transmitidas por correo electrónico

Protección multinivel contra malware

Los múltiples niveles de seguridad son capaces de detener el malware transmitido por correo electrónico más complejo, incluidos el spyware, los wipers, los mineros y el ransomware, los cuales suelen estar encabezados por el phishing dirigido. Los datos de reputación en la nube, la detección precisa, los modelos de aprendizaje automático local y en la nube, la inteligencia de amenazas adquirida a nivel global y los datos de investigación exclusivos se combinan para garantizar una de las mejores tasas de detección de falsos positivos en la industria.

Amplitud de situaciones: Una licencia para todo

Una sola licencia de producto cubre una variedad única de escenarios, incluido el refuerzo de la protección de su infraestructura de correo electrónico preexistente o la creación de una nueva y segura. Una variedad de arquitecturas de correo electrónico que abarcan las basadas en Linux o Windows, en las instalaciones, virtualizadas, basadas en la nube o una combinación de estas: todo está cubierto en un solo producto de Kaspersky.

Antispam automatizado (con reputación de dirección de origen y contenido)

El sistema antispam de Kaspersky usa motores inteligentes para minimizar la posibilidad de falsos positivos, que se adaptan continuamente a los cambios en las técnicas de los emisores de spam. Los datos sobre reputación recopilados a nivel global se procesan en la nube y se usan para alimentar algunos aspectos de la IA, lo que proporciona una base sólida para la detección eficiente del spam.

Protección contra correos electrónicos empresariales comprometidos (BEC)

Un sistema específico de detección basado en aprendizaje automático, con modelos algorítmicos constantemente actualizados con nuevos escenarios, procesa diferentes indicadores indirectos, lo que le permite al sistema bloquear incluso los correos electrónicos falsos más convincentes. El soporte para mecanismos de autenticación del remitente tales como SPF/DKIM/DMARC brinda protección contra la falsificación de fuente, una función de gran utilidad para hacer frente a los escenarios de correos electrónicos empresariales comprometidos (BEC).

Sandboxing

Para ofrecer protección incluso frente a los ataques de malware más sofisticados y ocultos, los archivos adjuntos se ejecutan en un entorno emulado seguro, donde se analizan para garantizar que las muestras maliciosas no accedan al sistema corporativo. Para los usuarios de Kaspersky Anti Targeted Attack, la integración agrega la "detonación" en un entorno sandbox externo y avanzado, lo que proporciona niveles mucho más profundos de evaluación y análisis dinámico.

Características antiphishing avanzadas

El sistema antiphishing de Kaspersky usa una red neuronal basada en el análisis para crear modelos de detección efectivos. Con más de 1000 criterios de uso, que incluyen imágenes, comprobaciones lingüísticas y scripts específicos, este enfoque con soporte en la nube recopila datos capturados a nivel global sobre direccione IP y URL maliciosas y de phishing para proporcionar protección tanto de los correos electrónicos de phishing de hora cero y conocidos o desconocidos.

Bloqueo de las transferencias de contenido no seguras

El sistema de filtrado de adjuntos configurable de Kaspersky puede detectar los archivos camuflados utilizados con frecuencia por los ciberdelincuentes para identificar los adjuntos potencialmente peligrosos. La funcionalidad similar a la prevención de pérdida de datos (DLP) permite al administrador configurar reglas complejas para evitar la fuga de datos, armado con el poder de las expresiones regulares y obteniendo beneficios de una gran cantidad de prácticas recomendables acumuladas por la comunidad.

Más allá de la puerta de enlace: Resiliencia a nivel de buzón de correo

Las tecnologías usadas en buzones de correo incluyen lo siguiente:

Doble análisis del correo electrónico: aborda escenarios como la activación retrasada de URL de phishing.

Cuarentena oculta antispam: ideal para entornos de baja tolerancia. Los correos electrónicos sospechosos pueden mantenerse en cuarentena de forma temporal hasta que Kaspersky Security Network disponga de pruebas suficientes para tomar una decisión final sobre si dichos correos son definitivamente seguros o no.

Visibilidad

Una interfaz basada en la Web y de fácil utilización permite a su administrador controlar sus niveles de protección del correo corporativo, con herramientas que incluyen las siguientes:

- Panel configurable.
- Visualización práctica de eventos con una potente búsqueda booleana de eventos.
- Exportación de eventos a su sistema SIEM.
- Informes en consola o por correo electrónico.
- Supervisión del estado del sistema.

Ampliación y resiliencia

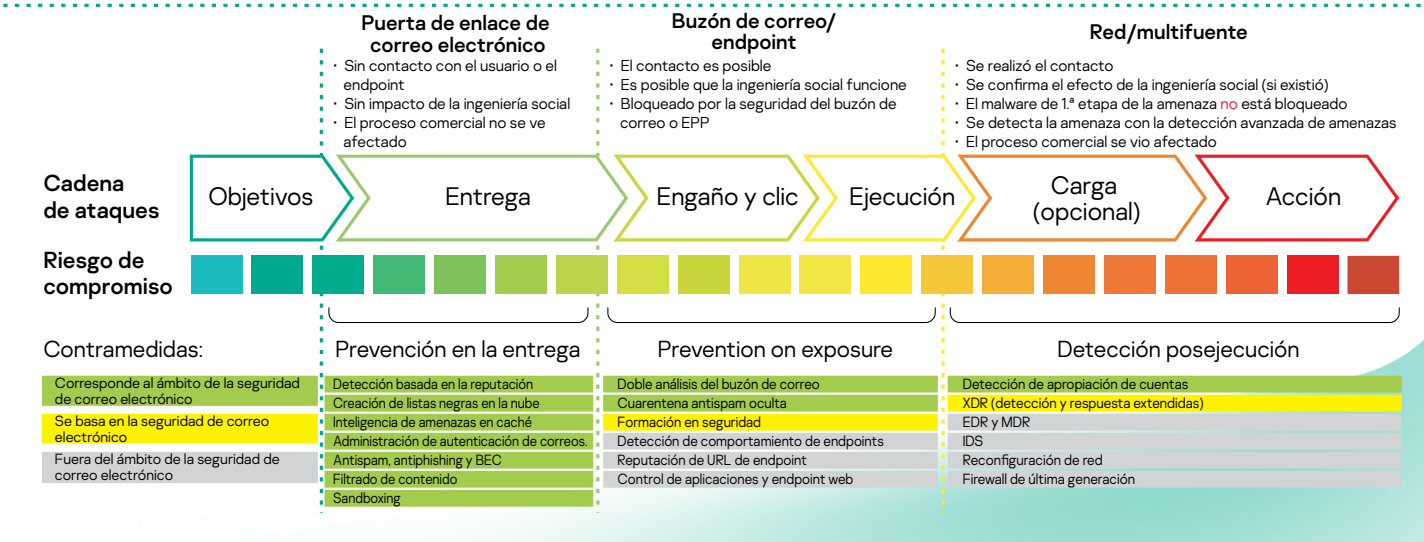
La solución admite arquitecturas en clúster para hacer frente a las crecientes cargas de tráfico y garantizar la resiliencia de todo el sistema de seguridad del correo electrónico en caso de desastre. Para garantizar que la desinfección, la eliminación o un percance técnico no provoquen la pérdida de datos críticos, se puede hacer una copia de seguridad de los mensajes originales de acuerdo con los criterios especificados por el administrador, lo que proporciona un acceso sin riesgos.

Administración y control de acceso

Las reglas flexibles le permiten al administrador establecer directivas que combinen múltiples criterios y hacer un seguimiento de los intentos de infracción. Para un dispositivo de correo electrónico seguro todo en uno, se ofrecen instrumentos especializados para configurar aspectos no relacionados con la seguridad del sistema en la misma consola de administración. El control de acceso basado en roles significa que se pueden asignar administradores independientes a diferentes áreas de la empresa o a diferentes clientes.

Extended Detection & Response

La integración con Kaspersky Anti Targeted Attack le brinda acceso a muchas tecnologías de detección de nivel experto que incluyen un sandbox avanzado, un analizador de amenazas móviles, fuentes de datos especiales que contienen datos de C&C y más. Después de una detección exitosa, se puede interrumpir un ataque dirigido bloqueando sus componentes mediante la localización y el aislamiento en diferentes niveles de la infraestructura, utilizando escenarios de productos cruzados XDR.



El rol de Mail Security en las diferentes etapas de la cadena de ataque cibernético

Mejore su protección con Kaspersky Security for Mail Server

Kaspersky Security for Mail Server es solo uno de los productos y soluciones de Kaspersky, desarrollado internamente, con base en más de 20 años de experiencia, construido a partir de una base de código único y diseñado para interconectarse a la perfección y proporcionar una plataforma de seguridad integral e inexpugnable.

Si ya utiliza Kaspersky Endpoint Security for Business, instalar Kaspersky Security for Mail Server significa que podrá tener la completa seguridad de que la protección de su puerta de enlace de correo ofrecerá los mismos estándares de alto rendimiento que el resto de sus sistemas de seguridad.

Si todavía no lo utiliza, puede que este sea el momento perfecto para fortalecer su perímetro y crear resiliencia instalando Kaspersky Security for Mail Server junto con su protección actual de correo electrónico o de forma independiente.

Cómo comprarla

Kaspersky Security for Mail Server se vende como una solución específica independiente o como un complemento exclusivo para los clientes de Kaspersky Endpoint Security for Business.

Aplicaciones incluidas

- Kaspersky Security for Linux Mail Server
- Kaspersky Secure Mail Gateway
- Kaspersky Security for Microsoft Exchange Server
- Kaspersky Security for Cloud Mail

Licencias

Kaspersky Security for Mail Server está disponible con las siguientes opciones:

- Licencia anual
- Suscripción mensual

También puede considerar lo siguiente:

Kaspersky Security for Internet Gateway: complemente su protección perimetral del correo electrónico con una seguridad igualmente potente para la puerta de enlace web, también incluida en Kaspersky Total Security for Business.

Kaspersky Endpoint Security for Business: nuestra solución de seguridad de endpoints líder, que ofrece la protección de endpoints más probada y premiada del mercado.

Kaspersky EDR Optimum: nuestra nueva solución de seguridad para endpoints líder de Kaspersky, que ofrece visibilidad mejorada e información detallada sobre las detecciones de malware, complementada con análisis de causa raíz y opciones de respuesta automatizada.

Pruebe antes de comprar

Explore nuestra solución Kaspersky Security for Mail Server con una versión de prueba gratuita con una validez de 30 días.

Solicite una llamada

¿Aún siente que necesita más información? ¡Contáctenos!

Compre a través de un partner de confianza

¿Siente que está listo para comprar? Busque un revendedor local para que lo ayude con su compra.

Noticias sobre amenazas cibernéticas: www.securelist.com
Noticias sobre seguridad de TI: business.kaspersky.com
Tecnologías de Kaspersky: kaspersky.com/technowiki
Seguridad de TI para pymes: kaspersky.com/business
Seguridad de TI para grandes empresas: kaspersky.com/enterprise

latam.kaspersky.com

Hemos pasado pruebas. Somos independientes. Somos transparentes. Estamos comprometidos con la construcción de un mundo más seguro, en el que la tecnología mejore nuestras vidas. Por eso la protegemos, para que todo el mundo pueda beneficiarse de las oportunidades que ofrece la tecnología. Incorpore ciberseguridad para un futuro más seguro.

Obtenga más información en latam.kaspersky.com/transparency

Proven. Transparent. Independent.