Seguridad para el correo electrónico de McAfee SaaS

Protección integral y acceso continuo al correo electrónico sin los costes operativos

En una situación económica difícil, muchas empresas posponen la decisión de invertir en tecnología, ya sea para mejorar su infraestructura de seguridad o contratar más personal de TI, o bien deciden recortar costes trasladando a la nube los buzones de entrada. Según en un estudio del SANS Institute, el 95 % de todos los ataques a redes de empresas son el resultado de técnicas de phishing dirigido[1]. Las amenazas de correo electrónico que propagan son ahora más sofisticadas que nunca y también más peligrosas.

Protección del clic
ClickProtect, una función fundamental de McAfee Email Protection, le ayuda a eliminar las amenazas asociadas a las URL incluidas en los mensajes de correo electrónico.

Módulos fáciles de adoptar:

- McAfee SaaS Email Protection & Continuity
- McAfee SaaS Email Encryption
- McAfee SaaS Email Archiving

Bloquear el spam y el malware no es más que la mitad de la batalla

Todo aquel que dependa del correo electrónico para su actividad laboral tiene que aplicar estas medidas de seguridad:

- Bloquear las amenazas y los datos inútiles entrantes antes de que afecten a la red, a los empleados o a las operaciones de la empresa.
- Identificar con precisión y bloquear los mensajes de correo electrónico de salida con contenido confidencial, inadecuado o procesable, tanto en el cuerpo del mensaje como en los archivos adjuntos, y adoptar las medidas adecuadas al respecto.
- Asegurar el acceso permanente a las comunicaciones por correo electrónico.
- Cumplir y documentar el cumplimiento de las normativas de la empresa, del sector y oficiales.
- Administrar todo el entorno del correo electrónico de manera que la seguridad, la continuidad y el cumplimiento de las normativas estén siempre al día.

Administrar a destiempo no es una alternativa

Mantenerse al día de todas estas áreas puede resultar especialmente costoso en tiempo y dinero. Afortunadamente, hay una forma mucho más fácil de administrar la seguridad del correo electrónico, proporcionar funciones fiables de almacenamiento y recuperación, y asegurar el acceso continuo, todo por un coste menor y un esfuerzo mínimo por parte del departamento de TI.

Protección del correo electrónico de bajo coste y fácil de administrar

Fáciles de instalar, las soluciones de seguridad para el correo electrónico de McAfee® SaaS (software como servicio) están siempre activas y actualizadas, y no requieren inversiones adicionales en hardware o software, ni más tiempo o recursos para su configuración y mantenimiento. Gracias a que estos servicios detienen el spam y las amenazas basadas en el correo electrónico antes de que se infiltren en su red, la cantidad de correo electrónico entrante se reduce considerablemente, lo que le ahorrará un valioso ancho de banda, así como capacidad de almacenamiento en el servidor. Y con el servicio de atención al cliente permanente e internacional de McAfee, contará con ayuda con una simple llamada telefónica.

intel Security

Protección optimizada

Aúnelo todo para simplificar la administración y lograr mayor visibilidad con un único panel.

- McAfee SaaS Email Protection está disponible como parte de McAfee Email Protection, lo que permite a los clientes elegir las opciones de despliegue que prefieran, entre ellas una solución híbrida integrada en una única consola de administración.
- Combine la seguridad para el correo electrónico, la Web y los endpoints de McAfee SaaS en una sola consola centralizada.

Administración y generación de informes simplificadas y basadas en la Web

Con una única consola de administración intuitiva basada en la Web, las actualizaciones de las directivas de correo electrónico son fáciles de gestionar en todos los dominios y ubicaciones. Además, los administradores pueden configurar e implementar directivas para el spam, el malware y el filtrado de contenido, incluidas las reglas para los archivos adjuntos. La integración con Microsoft Active Directory permite un mantenimiento fácil y regular. Las directivas se pueden aplicar a nivel global a grupos de usuarios o bien a determinados usuarios para disfrutar de una flexibilidad máxima. Los informes, registros, auditorías de mensajes y notificaciones de cuarentena ofrecen la visibilidad necesaria. Las soluciones McAfee SaaS para el correo electrónico también liberan valiosos recursos de TI y reducen el coste total de propiedad.

El correo electrónico es el motor actual de la productividad. Con los miles de mensajes que circulan cada día a través de los servidores de correo electrónico de una empresa típica, administrar el correo electrónico para garantizar su seguridad y disponibilidad se ha convertido en una labor ingente. Pero hay una forma mejor de hacerlo. Las soluciones de seguridad para el correo electrónico de McAfee SaaS le permiten controlar por completo la seguridad y la disponibilidad del correo electrónico y, a la vez, liberan recursos de TI para que pueda dedicarlos a las actividades estratégicas necesarias en la puesta en marcha de las iniciativas de la empresa.

Infraestructura y funcionamiento sólidos y fiables

La estrategia del centro de datos de McAfee SaaS incluye el mantenimiento de varios centros de datos repartidos por cuatro continentes. McAfee SaaS cuenta con la certificación ISO 27001 y el servicio ofrece una redundancia total mediante hardware redundante activo-activo en todos los niveles: firewalls, routers y conmutadores para equilibrio de carga. También ofrecemos supervisión automatizada de aplicaciones y redes en todos los centros de datos, lo que mejora la visibilidad de las alertas y alarmas. Los sistemas están supervisados por expertos en seguridad permanentemente.

Férrea protección del correo electrónico

El poder de ser millones: McAfee Global Threat Intelligence (McAfee GTI)

La plataforma Security Connected correlaciona la información de amenazas de distintos vectores, como el correo electrónico, la Web, la red y los endpoints. McAfee GTI aplica análisis de grandes volúmenes a la información colectiva, por lo que las soluciones de seguridad de McAfee para el correo electrónico siempre cuentan con los datos más recientes, actualizados al minuto para optimizar la seguridad.

Protección del clic

ClickProtect le ayuda a eliminar las amenazas de las URL incorporadas en los mensajes de correo electrónico. Busca variaciones en la legitimidad de una URL entre el momento en que se analiza el mensaje (momento de análisis), por inofensivo que este haya parecido, y el instante en que el usuario hace clic en ella (momento y evitar que hagan clic.). Esta segunda inspección puede incluir la comprobación de la reputación de la URL y su emulación proactiva utilizando el mismo motor McAfee Gateway Anti-Malware Engine, líder del sector, que incluye McAfee Web Protection. Los administradores pueden configurar directivas basadas tanto en el momento de análisis como en el momento del clic, y habilitar la emulación de URL para proteger a los usuarios y evitar que hagan clic. Y SafePreview permite echar un vistazo previo, aprovechando la inteligencia del usuario como una capa adicional de seguridad.

Protección máxima frente al spam

El sistema patentado de detección de spam Stacked Classification Framework aplica varias capas de análisis con un enfoque de filtrado basado en proxy para determinar la probabilidad de que un mensaje de correo electrónico sea spam, independientemente del idioma en el que esté escrito. Dado que cada tecnología de filtrado tiene sus propios puntos fuertes para identificar amenazas concretas, como el spam basado en imágenes, la combinación crea uno de los procesos de filtrado más precisos y completos del sector.

El servicio de reputación de mensajes de McAfee GTI inspecciona todos los mensajes para detectar las amenazas conocidas y de nueva aparición basadas en mensajes, como el spam, incluso aunque estos mensajes procedan de una fuente de confianza. Gracias al análisis de la reputación, McAfee SaaS Email Protection & Continuity bloquea o pone en cuarentena el correo electrónico de manera más eficiente y precisa.

Los métodos de validación SPF y DKIM proporcionan una capa más de seguridad. SPF valida los mensajes entrantes para asegurar que realmente proceden de dominios registrados y verificados por el remitente, mientras que DKIM corrobora que los mensajes están firmados electrónicamente por el remitente y son legítimos.

Filtrado del correo electrónico gris o masivo para reducir aún más los mensajes no deseados
En el correo no deseado podrían incluirse los mensajes masivos legítimos que una vez solicitó el cliente, pero que no desea seguir recibiendo y que pueden representar una molestia para los destinatarios. Gracias al uso de filtros de correo no deseado, los administradores pueden definir directivas al respecto e incluso delegar en los usuarios finales la decisión de activar esta función para mantener sus buzones de correo limpios de este tipo de mensajes.

Bloqueo bidireccional de virus y gusanos con análisis de tres capas
Además de bloquear los ataques entrantes, también se filtran los mensajes salientes, en los que se analiza tanto el cuerpo del mensaje como los archivos adjuntos, para proteger a sus clientes frente al malware. La solución incluye nuestra tecnología patentada de detección WormTraq y nuestro motor antivirus basado en firmas, líder del sector, respaldado por el servicio McAfee GTI. También está provista de tecnología antivirus de otros fabricantes, para ayudar a los clientes a satisfacer los requisitos de cumplimiento de normativas.

Escalabilidad total para protegerse frente a los ataques de envío masivo
Nuestra completa solución protege su red y los gateways de mensajería críticos frente a los ataques por correo electrónico, bloqueando de manera instantánea los ataques de denegación de servicio y otros ataques basados en SMTP: ataques de recopilación de directorios, envíos masivos de mensajes de correo electrónico y desbordamiento de canales.

Identificación de datos confidenciales para cumplir las normativas y prevenir fugas de datos

Reglas preconfiguradas, análisis de contenido avanzado e identificación por huella digital de documentos
Con las funciones avanzadas de prevención de pérdida de datos y de cumplimiento de normativas, podrá contar con reglas de contenido preconfiguradas para el cumplimiento de la norma PCI-DSS, las normativas aplicables al sector sanitario y los datos financieros, y la legislación local sobre protección de la intimidad, entre otros, lo que le ayudará a crear rápidamente directivas para el cumplimiento de tales normas. Además, le permitirán analizar y proteger más de 300 tipos de documentos para protegerse frente a las fugas de datos.

Avanzada tecnología de identificación de documentos por huellas digitales
Esta tecnología probada permite "enseñar" a su solución de seguridad del correo electrónico a determinar qué documentos se controlan mediante directivas. Mediante la creación y el almacenamiento de huellas digitales de documentos seleccionados, la solución "aprende" qué tipo de contenido debe estar controlado por las directivas. Las directivas pueden implementarse de forma específica en el contenido completo o en una parte del contenido del correo electrónico y los archivos adjuntos.

No se volverán a perder mensajes
Cuando se producen cortes de electricidad no se rechazan los mensajes de correo entrantes de gran importancia para la empresa. Todos los mensajes se guardan en una cola y se distribuyen de forma inteligente cuando los servidores recuperan la actividad.

Continuidad garantizada del correo electrónico, pase lo que pase
Al producirse una caída de la red debido a desastres naturales, cortes de electricidad o trabajos de mantenimiento regulares, McAfee SaaS Email Protection & Continuity mantiene a los empleados, clientes, partners y proveedores permanentemente conectados. Su interfaz web segura y fácil de usar permite a los usuarios enviar y recibir mensajes con total protección, buscar y recuperar mensajes almacenados, y administrar mensajes en cuarentena y almacenes de mensajes, de la misma forma que se haría en un entorno tradicional. Además, el servicio retiene todos los mensajes enviados y recibidos durante las interrupciones y, hasta que se restablezcan sus servidores de correo electrónico, lleva a cabo una sincronización inteligente y precisa de toda la actividad de correo electrónico.

Protección con cifrado

Cifrado TLS (seguridad de la capa de transporte) integrado para garantizar una comunicación segura entre organizaciones
Para las organizaciones que necesitan un mayor nivel de seguridad para el correo electrónico entrante y saliente, nuestro protocolo TLS acepta y filtra los mensajes entrantes y salientes cifrados, y los distribuye a través de un túnel seguro.

Cifrado y descifrado fáciles de utilizar
En el caso de las empresas que necesitan mantener una comunicación segura con sus clientes, McAfee SaaS Email Encryption permite cifrar la información confidencial aunque el destinatario no disponga de una solución de cifrado. Nuestra tecnología de cifrado y descifrado fácil de utilizar garantiza que sus datos estarán protegidos y a buen recaudo.

Personalización de marca para una experiencia online unificada
Los mensajes de correo electrónico de notificación de cifrado pueden personalizarse con su marca para conferirles el diseño de su empresa y brindar a sus clientes una experiencia online unificada.

Seguridad mejorada para Microsoft Office 365 y Google Apps

Es fácil reforzar la seguridad del correo electrónico de Microsoft Office 365 y Google Apps para los clientes de correo alojado en la empresa. Con una simple casilla de verificación en la consola de administración y redirigiendo los registros MX, los clientes pueden activar una protección incomparable contra amenazas entrantes, incluido ClickProtect, y la función de inspección del correo saliente para verificar si lleva contenido confidencial. De este modo se elimina la necesidad de introducir —y mantener— manualmente cientos de direcciones IP en el servicio de seguridad del correo electrónico para inspeccionar los mensajes procedentes de Google o Microsoft.

Enrutamiento inteligente como refuerzo de marca

A medida que su empresa crece, cada vez es más importante mantener una fuerte identidad corporativa. El servicio de enrutamiento inteligente de McAfee SaaS le permite añadir con facilidad nuevos dominios locales al actual dominio público y así enrutar directamente los mensajes de correo electrónico a los sistemas y los destinatarios adecuados. Recorta los costes de ancho de banda, ya que elimina la necesidad de redirigir el correo del centro principal a los usuarios de las oficinas satélites.

Almacenamiento ilimitado de datos de correo electrónico... sin hardware

Los volúmenes actuales de correo electrónico crecen vertiginosamente. A la vez, las normativas oficiales y del sector exigen cada vez más documentos para todo tipo de decisiones y procesos. Bajo semejante presión, las empresas necesitan métodos de archivado y recuperación rápidos, sencillos y asequibles. El servicio McAfee SaaS Email Archiving recorta los costes de almacenamiento y gestión del correo electrónico, y protege los mensajes entrantes, salientes, internos e incluso históricos de la compañía a medida que se crean; a la vez, reduce las bases de datos de Microsoft Exchange a un tamaño manejable. También satisface los requisitos de cumplimiento normativo y de e-discovery, lo que protege su empresa y a sus empleados. Sus potentes funciones de búsqueda ayudan a los usuarios autorizados a buscar y recuperar fácilmente los mensajes en cuestión de segundos sin necesidad de recurrir al personal de TI.

Al ser un servicio basado en la nube, con McAfee SaaS Email Archiving no hace falta comprar hardware o software, administrar soportes de copias de seguridad ni almacenar contenido fuera de las instalaciones del cliente. Es posible elegir un periodo de retención de hasta 10 años. McAfee SaaS Email Archiving se ofrece como servicio independiente o como parte de otras soluciones McAfee Email Protection.

Ficha técnica

Características	McAfee SaaS Inbound Filtering	McAfee SaaS Email Protection & Continuity	McAfee SaaS Email Protection & Continuity con cifrado
Infraestructura y servicios operativos			
Soporte ininterrumpido (24 horas al día, 7 días a la semana)	•	•	•
Gestión de rendimiento y capacidad	•	•	•
Mantenimiento y ampliaciones automáticos	•	•	•
Centros de datos con certificación ISO 27001	•	•	•
Suscripción mensual, anual o por varios años	•	•	•
Administración y asistencia al usuario final			
Auditoría de mensajes	•	•	•
Asistencia en más de 15 idiomas	•	•	•
Security Connected	•	•	•
Compatible con Google Apps y Microsoft Office 365	•	•	•
Protección del correo electrónico			
McAfee GTI	•	•	•
ClickProtect	•	•	•
Protección frente a spam y phishing entrante y contra malware	•	•	•
Filtrado de correo no deseado y masivo	•	•	•
Codificación TLS	•	•	•
Autenticación DKIM y SPF	•	•	•
Firma DKIM		•	•
Protección frente al malware e implementación de directivas para el tráfico saliente		•	•
Colas de correo electrónico		•	•
Acceso continuo al correo electrónico		•	•
Cifrado y descifrado			•
Personalización de marca en las notificaciones de cifrado			•
Análisis del contenido adjunto, más de 300 tipos de archivos			•
Más de 114 plantillas predefinidas de cumplimiento de normativas y prevención de pérdida de datos			•
Huella digital de los documentos			•
Opcional			
Archivado del correo electrónico	•	•	•
Enrutamiento inteligente	•	•	•

Es hora de cambiar

Proteja toda su empresa con menos tiempo, dinero y preocupaciones. No solo ahorrará en el momento de la compra. Descubra cómo puede reducir el mantenimiento con nuestro galardonado servicio, fácil de utilizar, y aliviar la carga de trabajo de su personal de TI para que pueda centrarse en proyectos de carácter más estratégico.

Si desea obtener más información, visite www.mcafee.com/es/products/email-and-web-security/email-security.aspx. Para solicitar una prueba gratuita, visite **www.mcafeesaas.com**.

1. SANS Institute en *Network World*, marzo de 2013

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com