McAfee Email Gateway

Protección del correo electrónico empresarial

Principales ventajas

Protección total entrante y saliente

- Seguridad completa frente a todas las amenazas que llegan por el correo electrónico entrante
- Cifrado de correo electrónico integrado
- Formatos de cumplimiento de normativas y prevención de la pérdida de datos confidenciales integradas

Seguridad, administración y escalabilidad avanzadas

- Disponible como dispositivo virtual, dispositivo de hardware, servidor blade o solución híbrida integrada con McAfee SaaS Email Protection
- Administración centralizada, búsqueda de mensajes, reportes y cuarentena
- El uso de agrupaciones en clúster y equilibrio de carga integrado permite responder a los requisitos más exigentes de los despliegues in situ

Benefíciese de Security Connected a través del software McAfee® ePolicy Orchestrator® (McAfee ePO™), McAfee Global Threat Intelligence (McAfee GTI), McAfee Advanced Threat Defense, y las soluciones híbridas de protección del correo electrónico.

El correo electrónico es indispensable y uno de los servicios más importantes para el correcto funcionamiento de cualquier entorno empresarial. Su capacidad para distribuir de manera instantánea una amplia variedad de volúmenes de información traspasando límites organizativos, geográficos y políticos lo convierten en una herramienta básica y en un ingente desafío para la seguridad. McAfee® Email Gateway le ayuda a reforzar la seguridad del correo electrónico y a fortalecer las defensas con protección contra las amenazas entrantes, prevención de pérdida de datos a través del tráfico saliente, cifrado, funciones avanzadas de cumplimiento de normativas y administración centralizada en un solo dispositivo de fácil despliegue.

Desafíos para la seguridad del correo electrónico

Examinemos los problemas de seguridad críticos del correo electrónico a los que se enfrentan las empresas en la actualidad:

- Los ataques a través del correo electrónico entrante son cada vez más obra de bandas de delincuentes organizadas que tratan de obtener datos con los que poder lucrarse. Estos ataques se sirven de sofisticadas técnicas de ingeniería social y evolucionan con rapidez para eludir las defensas tradicionales basadas en firmas.
- El correo electrónico es uno de los principales vectores de pérdida o robo de datos confidenciales, ya sea por un simple descuido o por una acción malintencionada de algún empleado.
- Debido a su importancia operativa y a su gran vulnerabilidad, el correo electrónico se ha visto sometido al control de las entidades reguladoras tanto políticas como comerciales. Las disposiciones afectan a tarjetas de pago (PCI DSS), servicios financieros (GLBA), servicios sanitarios (HIPAA) y empresas públicas estadounidenses (SOX).
- Cerca del 75 % del volumen global de correo electrónico es spam, con diferencias marcadas entre países. Los ataques de phishing son cada vez más selectivos y efectivos, y están más orientados a obtener datos financieros que nunca.
- McAfee Labs identificó cerca de 2250 URL de phishing al día en el cuarto trimestre de 2013, y esta cifra se ha mantenido constante a lo largo del año.

intel Security

Reconocimientos recibidos en 2013

- Líder de la categoría de gateway del correo electrónico seguro en el Magic Quadrant de Gartner
- Líder de la categoría de seguridad del contenido del correo electrónico en Forrester Wave
- Cinco estrellas como producto "Best Buy" (mejor relación precio-calidad) de la revista SC Magazine en la categoría de seguridad del contenido del correo electrónico
- Innovadores del sector: protección de datos, según la revista *SC Magazine*

¿Por qué conformarse con defensas fragmentarias e inadecuadas?

Las defensas actuales del correo electrónico de las empresas han evolucionado; en particular, la mayoría de soluciones de seguridad de correo electrónico se centran exclusivamente en el correo entrante y no ofrecen protección frente a la pérdida de datos a través del correo saliente. Esto significa que encontrará defensas que se componen de una serie de soluciones puntuales —antimalware, antispam, antiphishing, antivirus, cifrado y prevención de pérdida de datos— de diferentes proveedores, desplegadas por separado y que deben escalarse continuamente. No obstante, muchas de ellas no cumplen los requisitos de buenas prácticas actuales.

Mientras que las principales soluciones antispam presentan un índice de precisión de detección del 99 % o más, muchas de las soluciones de protección del correo electrónico solo llegan al 95 % o menos. Si bien una diferencia del 4 % puede parecer insignificante, la realidad es que esto representa una diferencia en la entrada de spam y en las posibles infecciones de sistemas de un 400 %. Cuando se considera el spam en el contexto de los miles de millones de correos electrónicos, un aumento del 4 % puede marcar una diferencia importante para la empresa porque puede sobrecargar la infraestructura de correo electrónico y saturar el ancho de banda. Basta que una proporción minúscula de mensajes de correo electrónico no deseados traspase la defensa para que los usuarios pierdan tiempo examinando y eliminando el spam. Por otra parte, aumentan las probabilidades de sufrir infecciones de malware, con el consiguiente incremento de costos y pérdida de productividad, y posiblemente también de datos, que eso conlleva.

La consecuencia inevitable es que la mayoría de organizaciones de TI se ven obligadas a invertir demasiado tiempo y dinero en mantener defensas compuestas por varias soluciones, evitar que haya fugas de información confidencial en la organización, demostrar que cumplen las normativas y paliar las consecuencias de contar con una seguridad de correo electrónico inadecuada. El interés de las empresas en disponer de una solución de seguridad de correo electrónico integral que incluya la protección del correo entrante y saliente, simplifique la administración y facilite el cumplimiento de normativas es innegable. McAfee Email Gateway es esa solución.

Protección completa para el correo electrónico

Seguridad líder del mercado

McAfee Email Gateway integra la protección avanzada frente a amenazas entrantes con la prevención de pérdida de datos a través del correo saliente, el cumplimiento de normativas avanzado, el cifrado del correo electrónico, las ventajas de rendimiento, la generación de reportes y la administración unificada, todo en una plataforma única y reforzada por un precio único.

- Al combinar la información de la red local con la información de reputación de McAfee GTI, ofrece la protección más completa disponible actualmente frente a amenazas entrantes, spam y malware.
- El análisis de vínculos al hacer clic junto con las funciones de emulación de comportamientos que ofrece McAfee Gateway Anti-Malware Engine detiene los ataques utilizando las URL maliciosas como su catalizador.
- La integración con McAfee Advanced Threat Defense permite la detección del malware más sofisticado y evasivo mediante una combinación innovadora de análisis de código estático y dinámico (entorno aislado).
- Sus sofisticadas tecnologías de análisis de contenidos, sus numerosas técnicas de cifrado y la gestión detallada de mensajes basada en directivas evitan la pérdida de datos a través del correo saliente y simplifican el cumplimiento de normativas.
- Gracias a su total integración en el software McAfee ePO, se puede administrar completamente, en o entre clústeres, con registros e reportes de categoría empresarial que simplifican la administración y las tareas de cumplimiento de normativas con una reducción significativa de los costos.

Protección integral frente a las amenazas entrantes
McAfee Email Gateway identifica y bloquea el spam entrante con una precisión de más del 99 %, al mismo tiempo que ofrece una protección integrada frente a virus, malware, phishing, recopilación de directorios, ataques de denegación de servicio (DoS) y ataques de devolución de mensajes. Evita las amenazas de tipo "zero-hour" y los ataques focalizados y combinados, además de reducir drásticamente el impacto de las oleadas de spam gracias a la potente combinación de clasificación dinámica de spam y respuesta ante amenazas. McAfee Email Gateway utiliza la información de reputación de remitentes, mensajes y URL, procedente de McAfee GTI para proporcionar actualizaciones.

También se incluye un motor antivirus secundario para que los clientes dispongan de protección en varios niveles frente al malware y puedan cumplir los requisitos normativos.

El análisis de vínculos al hacer clic detiene los ataques que evolucionan.
McAfee ClickProtect, una función de McAfee Email Gateway, elimina las amenazas de las URL incrustadas en los mensajes de correo electrónico. Busca variaciones en la intención de una URL entre el momento en que se analiza el mensaje (momento de análisis), por inofensivo que parezca, y el instante en que el usuario hace clic en ella (momento de clic). Esta segunda inspección puede incluir la comprobación de la reputación de la URL y su emulación proactiva gracias a la misma tecnología antimalware, líder del sector de McAfee Gateway, incluida en McAfee Web Protection. Los administradores pueden configurar directivas tanto para el momento de análisis como para el momento del clic, y activar la emulación de URL para proteger a los usuarios del clic. Y Safe Preview permite echar un vistazo previo a las páginas que se van a abrir, aprovechando la inteligencia del usuario como otro nivel de seguridad. Para evitar totalmente el acceso a la Web desde los mensajes de correo electrónico, se pueden detectar y eliminar las URL completamente, o bien sustituirlas por un texto explicativo.

McAfee Advanced Threat Defense detecta el malware sofisticado y evasivo.
McAfee Advanced Threat Defense detecta el malware persistente, de tipo zero-day, con una estrategia innovadora por capas. Combina análisis de código estático en profundidad y análisis dinámico (entorno aislado) para analizar el comportamiento real del malware. La estrecha integración entre Mcafee Email Gateway y McAfee Advanced Threat Defense permite realizar este análisis de los archivos sospechosos adjuntos al correo electrónico, bloqueando los que se consideran maliciosos antes de que lleguen a una bandeja de entrada.

Los métodos de menor intensidad analítica, como las firmas y la emulación en tiempo real, favorecen el rendimiento y, por otra parte, la incorporación al entorno aislado de análisis de código totalmente estático ofrece información detallada de clasificación del malware, amplía la protección contra las amenazas camufladas y evasivas, y permite identificar la reutilización asociada de código de malware. Las rutas de ejecución retardada o eventual, que no suelen procesarse en un entorno dinámico, pueden detectarse gracias a la descompresión y al análisis del código completamente estático.

Juntos, el análisis de código estático y el análisis dinámico proporcionan una evaluación completa e información detallada, con datos de resumen de comportamiento, gravedad del malware, asociaciones de familias de malware, rutas de ejecución y porcentaje de código ejecutado durante el análisis dinámico.

El filtrado de correo gris reduce aún más el correo no deseado
En el correo no deseado podrían incluirse los mensajes masivos legítimos que una vez solicitó el cliente, pero que no desea seguir recibiendo (por ejemplo, boletines de noticias y notificaciones del sector). Aunque el correo no deseado no suele considerarse spam, puede resultar muy molesto a quien lo recibe. La aplicación de filtros para permitir acciones, como el bloqueo y la cuarentena, permite mantener limpias las bandejas de correo.

Protección total del correo saliente para garantizar la seguridad del contenido

Se incluye cifrado del correo electrónico.
Como función estándar se incluye el cifrado integrado del correo electrónico basado en directivas mediante el empleo de una combinación de tecnologías B2B (TLS, S/MIME y OpenPGP) y B2C (Push/Pull), lo que permite garantizar que incluso los destinatarios que no cuentan con funciones de cifrado puedan recibir y responder a los mensajes de correo electrónico seguros. La tecnología de cifrado y descifrado incluye un cliente de correo web adaptable a distintas marcas y permite recuperar y ver los mensajes cifrados en dispositivos móviles. El hecho de aplicar el cifrado en el gateway, en lugar de en los equipos de escritorio, evita que los usuarios tengan que determinar las necesidades de cifrado y acaba con el recurrente problema de que los usuarios olviden cifrar los datos confidenciales.

Cumplimiento de normativas y prevención de la pérdida de datos
También se integra y se proporciona como característica estándar una completa serie de formatos de cumplimiento de normativas, que es la misma que ofrece McAfee Data Loss Prevention. Las técnicas de identificación por huella digital, análisis léxico y agrupación en clúster complementan las búsquedas por coincidencia con patrones y palabras clave para ofrecer una detección integral tanto de los datos estructurados como no estructurados. El gateway identifica con precisión el contenido regulado (HIPAA, SOX, GLBA); es decir, la información que contiene datos personales, como números de tarjetas de crédito, números de documentos de identificación, identificadores regionales específicos y otros datos de clientes y empleados. También permite identificar datos no estructurados y de propiedad intelectual, como código fuente, patentes, información financiera y planes empresariales, y adoptar medidas al respecto. En caso de detectar cualquier anomalía, aplica una amplia gama de acciones basadas en directivas, lo que incluye cifrado forzado (push, pull o TLS), alertas, redireccionamiento, cuarentena, bloqueo y otras opciones personalizadas.

Control total de la administración
McAfee Email Gateway permite a los administradores ofrecer la mejor protección posible del correo electrónico y ofrece la posibilidad de demostrarla con reportes de categoría empresarial, completos registros exportables, paneles configurables en tiempo real, alertas y reportes detallados. La solución combina rendimiento, escalabilidad y estabilidad con un modelo de distribución flexible que garantiza la máxima rentabilidad con la mínima carga administrativa. Se puede administrar por completo desde la consola de administración de McAfee Email Gateway o desde el software McAfee ePO, e incluye además:

Sofisticados controles de directivas y uso, para facilitar la administración.

- Clara e intuitiva interfaz con asistentes de instalación y configuración
- Integración con el protocolo LDAP (Lightweight Directory Access Protocol) de Active Directory
- Administración centralizada de la seguridad del correo electrónico con implementación de directivas específicas, búsqueda de mensajes y registro detallado de conversaciones
- Generación de reportes en tiempo real, con paneles interactivos y reportes detallados

La arquitectura avanzada ofrece un alto rendimiento.

- Análisis asíncrono, basado en memoria
- Agrupación y equilibrio de cargas integrados para ofrecer alta disponibilidad.
- McAfee Quarantine Manager, interno o altamente escalable, ofrece servicios de cuarentena consolidados para varios dispositivos McAfee Email Gateway y colas de cuarentena personalizadas, permite rebajar la carga de almacenamiento y procesamiento con una capacidad de hasta 1,5 millones de mensajes y admite hasta 200 000 usuarios.

Certificaciones y soporte

- Certificación EAL2+ de Common Criteria, incluido el cumplimiento con NDPP
- Validación y certificación FIPS 140-2 L1
- Compatibilidad con Common Access Card (x.509)
- Compatibilidad con IPv6

Simplemente visión de futuro: protección integral del correo electrónico para todas las empresas

Flexibilidad de despliegue

McAfee Email Gateway puede desplegarse como dispositivo físico (con cuatro tamaños diferentes), como máquina virtual o en una arquitectura de servidor blade. Esta versatilidad ofrece protección y escalabilidad asequibles para los entornos de mensajería empresarial más exigentes. Como McAfee Email Gateway forma parte de McAfee Email Protection, ofrece la posibilidad de desplegar la seguridad del correo electrónico como gateway in situ (físico o virtual), solución de seguridad como servicio (SaaS, Security-as-a-Service) basada en la nube o una combinación híbrida integrada, por un único precio de suscripción.

Las organizaciones que desean aprovechar las ventajas de la nube y, al mismo tiempo, mantener el control en sus instalaciones, pueden utilizar la solución híbrida integrada, que incluye McAfee Email Gateway como centro de control de la administración de directivas in situ y basado en la nube, y las funciones consolidadas de generación de reportes, búsqueda de mensajes y cuarentena. Un caso típico de uso de las soluciones híbridas son las organizaciones que desean bloquear el paso del contenido malicioso o molesto a la red, reducir el ancho de banda y controlar la manipulación y el cifrado de la información confidencial en un dispositivo in situ.

Security Connected

La plataforma Security Connected ayuda a los clientes a mejorar el estado de su seguridad, optimizar la protección para mejorar la rentabilidad y alinear estratégicamente la seguridad con sus iniciativas empresariales. La integración con el software McAfee ePO permite reunir la administración y la generación de reportes entre soluciones de seguridad y dentro de ellas. McAfee Global Threat Intelligence (McAfee GTI), que aprovecha todas las soluciones de McAfee, recopila la información colectiva de cada posible vector de amenazas protegido por nuestras soluciones. Los datos y la información correlacionados se comparten entre nuestros productos y soluciones. Esto significa que la seguridad del correo electrónico de McAfee, parte de Intel Security, siempre dispone de la información más actualizada, al instante. McAfee Advanced Threat Defense detecta el malware actual oculto, zero-day, y se integra perfectamente con muchos productos, incluido McAfee Email Gateway. McAfee Advanced Threat Defense, que actúa como un recurso compartido entre varias soluciones, se adapta a la red mejorando la rentabilidad y minimizando los costos operativos.

Puede disfrutar de funciones de categoría empresarial para satisfacer las cargas de trabajo más amplias y exigentes, reduciendo al mínimo las necesidades de supervisión y los gastos. La combinación exclusiva de funcionalidad, rendimiento, fiabilidad y rentabilidad ha convertido a McAfee Email Gateway en la solución de seguridad de correo electrónico elegida por más de la mitad de las empresas de tecnologías de la información de Fortune 500. Para obtener más información sobre las soluciones McAfee Email Gateway, visite **www.mcafee.com/mx/products/email-and-web-security/email-security.aspx**.

McAfee. Part of Intel Security.
6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.intelsecurity.com

Intel y el logotipo de Intel son marcas comerciales registradas de Intel Corporation en EE. UU. y en otros países. McAfee, el logotipo de McAfee, ePolicy Orchestrator y McAfee ePO son marcas comerciales o marcas comerciales registradas de McAfee, Inc. o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros. Los planes, especificaciones y descripciones de productos mencionados en este documento se proporcionan únicamente a título informativo y están sujetos a cambios sin previo aviso; se ofrecen sin garantía de ningún tipo, ya sea explícita o implícita. Copyright © 2014 McAfee, Inc. 61084ds_email-gateway_0414B_fnl_ETMG