

McAfee Security for Email Servers

Proporciona seguridad de contenido robusta para sus servidores Microsoft Exchange

McAfee® Security for Email Servers detecta y filtra virus, gusanos, troyanos y otros programas potencialmente no deseados. Compatible con los servidores Microsoft Exchange, bloquea el spam y filtra los mensajes para evitar que la información inadecuada o confidencial entre o salga de la red, ayudándole a cumplir los requisitos de las normativas.

Como parte de la oferta de productos de McAfee, McAfee Security for Email Servers ofrece protección en varios niveles para el correo electrónico entrante y saliente, desde el análisis de malware bajo demanda a la implementación de directivas para evitar la pérdida o mala utilización de los datos confidenciales.

- **Protección líder del sector:** uso de nuestra galardonada función de análisis bajo demanda en memoria e incremental para eliminar virus, gusanos, troyanos y otras amenazas del correo entrante y saliente.
- **Detección de amenazas avanzadas:** la estrecha integración con McAfee Advanced Threat Defense a través de McAfee Threat Intelligence Exchange facilita el análisis en profundidad y la identificación de amenazas potenciales de tipo zero-day en los archivos adjuntos de mensajes de correo electrónico.
- **Potente protección interna:** detecta las amenazas que puedan haberse colado en las defensas del perímetro o entrado en la red a través de portátiles

infectados o correo interno. Además, bloquea el spam con el módulo antispam.

- **Eficaz filtrado de contenido:** implementa directivas corporativas para el filtrado del correo electrónico bloqueando los tipos de archivos prohibidos, el contenido ofensivo y las fugas de datos confidenciales.
- **Administración mediante una sola consola:** utiliza la plataforma McAfee ePolicy Orchestrator® (McAfee ePO™) para el despliegue, la administración de la seguridad y los informes gráficos detallados.

Protección del correo electrónico en varios niveles

Protección antimalware completa

McAfee Security for Email Servers emplea tecnología antimalware de reputación de archivos en tiempo real que reduce de manera significativa la exposición a las nuevas amenazas. Con nuestra información de Global Threat Intelligence (GTI) basada en la nube, enviamos huellas dactilares de cualquier archivo sospechoso a

McAfee combina inspección de contenido, análisis de reputación y protección contra malware para mantener protegido su correo electrónico. Ofrecemos varios niveles de defensa y opciones de despliegue para la seguridad del correo electrónico: transporte en el perímetro de la red, el servidor de transporte central y el servidor de buzón de correo.

Síguenos



FICHA TÉCNICA

McAfee Labs para su inmediato análisis de reputación. Si el rastro digital se identifica como malware conocido, en cuestión de milisegundos se envía la respuesta adecuada para bloquear o poner en cuarentena el archivo. Los archivos que siguen siendo sospechosos se envían automáticamente a McAfee Advanced Threat Defense para un análisis en profundidad en un entorno aislado. La integración a través de McAfee Threat Intelligence Exchange mejora la protección, ya que permite que McAfee Security for Email Servers y todas las soluciones conectadas en el ecosistema puedan tomar medidas frente a los adjuntos infectados.

Reputación de mensajes

Nuestro servicio global de reputación de mensajes y remitentes en tiempo real, basado en la nube, McAfee GTI, permite a nuestros productos proteger a nuestros clientes contra todas las amenazas que llegan a través del correo electrónico, como el spam, ya sean conocidas o nuevas. La reputación de los mensajes se combina con factores tales como patrones de envío de spam y comportamiento de direcciones IP con el fin de determinar la probabilidad de que el mensaje en cuestión sea malicioso. El resultado no solo se basa en la información colectiva procedente de los sensores que consultan la nube de McAfee y en los análisis que se realizan en McAfee Labs, sino también en la correlación de esta información con datos sobre amenazas procedentes de distintos sectores, como la Web, el correo electrónico y las redes.

Reputación de IP

Se pueden detectar las amenazas que llegan en los mensajes de correo electrónico, en función de la

dirección IP del servidor del remitente. El uso de la reputación de las direcciones IP evita daños y robos de datos mediante el bloqueo de los mensajes de correo electrónico en el gateway.

Reputación de URL

Protege frente a amenazas conocidas y nuevas basadas en la Web en función de la reputación de la URL incluida en el mensaje de correo electrónico.

Proteja sus servidores 7 días a la semana, 24 horas al día

Compruebe la existencia de virus, gusanos, troyanos y otro malware en los mensajes de correo electrónico entrantes y salientes. Además, puede analizar todos los mensajes internos para evitar que un gusano pueda propagarse en el interior de la red. McAfee Security for Email Servers descarga automáticamente las últimas definiciones de virus (archivos DAT) a través de HTTP, FTP, recursos compartidos de la red o la consola de administración centralizada de McAfee ePO.

Filtrado de mensajes

Filtre los mensajes según su tamaño, el tipo de archivo adjunto o el contenido. Bloquee o ponga en cuarentena los mensajes que incluyan contenido bajo control en el asunto, el cuerpo del mensaje o los archivos adjuntos.

Ahorro de tiempo y recursos

Los filtros de contenido predefinidos simplifican la creación e implementación de directivas. Cree reglas de forma global, con las excepciones necesarias para los distintos individuos y departamentos. Se puede gestionar mediante la interfaz HTML incorporada o la plataforma McAfee ePO.

Ventajas principales

- **Mantenga su sistema activo y en funcionamiento:** impida que entren gusanos, virus y amenazas avanzadas a través del correo electrónico o que se propaguen internamente a través de Microsoft Exchange.
- **Mantenga la productividad de sus empleados:** bloquee el spam y los ataques de phishing.
- **Administración desde una sola consola:** el software McAfee ePO ofrece una eficaz consola de administración para controlar, gestionar y ver informes.
- **Protección de datos críticos:** filtre los mensajes entrantes y salientes para garantizar la seguridad de la información y limitar la responsabilidad de la empresa, mediante tecnologías de DLP y reputación (de direcciones IP, mensajes, URL y archivos).
- **Interfaz gráfica de usuario:** la sencilla interfaz de usuario ofrece completos informes, gráficos y estadísticas del tráfico de correo electrónico en tiempo real.

Filtrado de contenido

Analiza el contenido y el texto de la línea del asunto o el cuerpo de los mensajes y adjuntos del correo electrónico. Cree sus propias reglas de filtrado de contenido utilizando expresiones regulares.

Prevención de pérdida de datos y cumplimiento de normas

La prevención de pérdida de datos (DLP) garantiza que los mensajes de correo electrónico enviados (desde un dispositivo móvil o desde la red) cumplen las normas de confidencialidad y otras normativas de su organización. Los diccionarios predefinidos con normativas de empresas y países concretos facilitan la configuración.

Especificaciones

Con el crecimiento exponencial del correo electrónico y los datos compartidos en los servidores de correo electrónico, McAfee Security for Email Servers admite el entorno Microsoft Exchange para mantener la productividad de los empleados y la continuidad de la actividad de las organizaciones 24 horas al día, 7 días a la semana.

Requisitos de McAfee Security for Microsoft Exchange

Requisitos del sistema operativo

- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Requisitos del servidor Microsoft Exchange

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- Se admiten servidores Microsoft Exchange Server con clúster

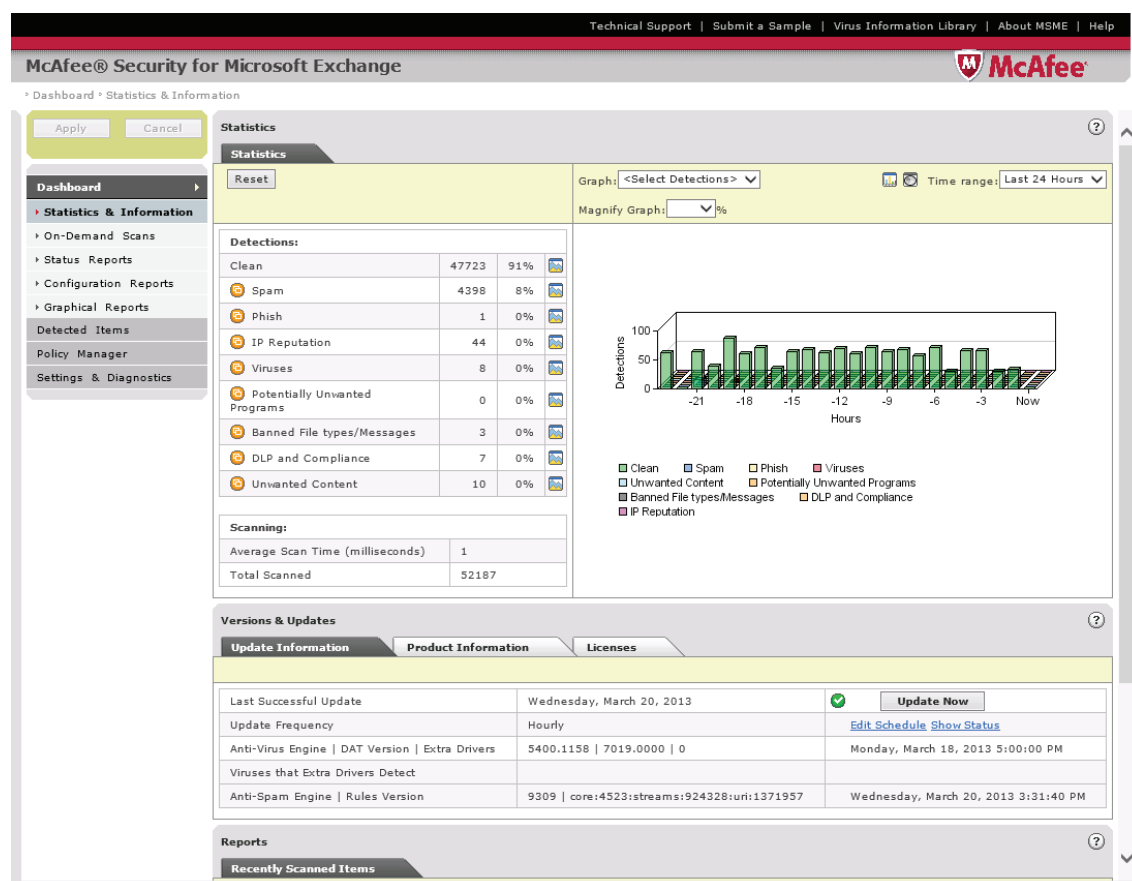


Figura 1. La sencilla interfaz de usuario ofrece completos informes, gráficos y estadísticas del tráfico de correo electrónico en tiempo real.

FICHA TÉCNICA

El flujo de trabajo incorporado reenvía de manera automática los mensajes en cuarentena a los auditores para que ellos los revisen.

Filtrado de spam y notable incremento de la productividad

Con el módulo antispam se pueden interceptar los mensajes de spam y phishing para mantener así la productividad de los empleados y reducir el espacio que se desperdicia en el servidor de correo electrónico. Los usuarios pueden crear sus propias listas blancas y listas negras. Una única solución de cuarentena compartida con nuestras soluciones de gateway para el correo electrónico ofrece a los usuarios un medio fácil para acceder a una sola zona de cuarentena.

Alertas de estado de los productos

McAfee Security for Email Servers envía notificaciones al administrador elegido en relación al estado de los productos. Supervisa el tiempo empleado en el análisis de cada archivo. Si surge algún problema, toma las medidas adecuadas para evitar un impacto negativo en el rendimiento del servidor Exchange.

Sencillas actualizaciones

Las actualizaciones automáticas le permiten mantenerse al día de lo último en información de seguridad de McAfee Labs, el principal centro de investigación de amenazas del mundo.

Centralización y consolidación de funciones de cuarentena de mensajes

McAfee Quarantine Manager, que se incluye en la solución, consolida las funciones de administración de cuarentena y antispam en una sola solución. McAfee Quarantine Manager es fácil de utilizar, permite enviar muestras a McAfee Labs y ofrece controles de administración muy específicos, sincronización automática de usuarios desde los servidores LDAP, administración de listas blancas y listas negras de usuarios o globales, y generación de informes detallados, todo ello gestionado desde la plataforma McAfee ePO.

Análisis y protección de almacenes de correo electrónico

McAfee Security for Email Servers ofrece análisis bajo demanda planificados con detalladas opciones de configuración para realizar los análisis rápidamente, a diferencia de los análisis completos tradicionales. Incluye opciones para analizar solamente mensajes con adjuntos, mensajes no leídos, o por asunto, remitente, destinatario, CC o ID del mensaje, así como mensajes recibidos en un período determinado o de un tamaño concreto.

Para obtener más información, visite [McAfee Security for Email Servers](#).



Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es

McAfee y el logotipo de McAfee, ePolicy Orchestrator y McAfee ePO son marcas comerciales o marcas comerciales registradas de McAfee LLC, o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros.
Copyright © 2020 McAfee, LLC. 4446_0420
ABRIL DE 2020