

McAfee SpamKiller for Microsoft Exchange Powered by McAfee SpamAssassin

McAfee® Security SpamKiller® for Microsoft® Exchange, “powered by McAfee SpamAssassin™”, brinda detección y rendimiento anti-spam inigualables y no tiene rival en la protección de servidores Microsoft Exchange. Ajustado para operar a alta velocidad, McAfee SpamKiller puede ayudarle a reducir los costos asociados al *spam*, realizando la exploración del e-mail entrante luego que llega al servidor Microsoft Exchange. Luego de la exploración, el e-mail de *spam* se puede poner en cuarentena en una carpeta de basura electrónica del servidor o del propio usuario. Detectando el *spam*, usted impide que sus usuarios tengan que manejar mensajes indeseables, ayudándoles a aumentar su productividad.

¿Qué es el Spam?

Definición de un problema creciente

Hay muchas formas distintas de describir el *spam*, y lo que es *spam* para una persona puede ser información útil para otra. Para simplificar el tema, McAfee Security clasifica el *spam* en tres grupos: *spam* malintencionado, *spam* de propaganda y *spam* amistoso. El *spam* malintencionado consiste en mensajes que pueden incluir contenido inadecuado o amenazas a la seguridad; el *spam* de propaganda consiste en mensajes de empresas legítimas que intentan vender productos o servicios; y el *spam* amistoso consiste en mensajes que contienen chistes o *links* para páginas Web de humor. Todos los estudios recientes del ramo sugieren que el volumen del *spam* está creciendo. Aproximadamente entre 25% y 50% de todos los e-mails que reciben las organizaciones son *spam*.

¿El spam es sólo una molestia? ¡No!

El spam es una amenaza devastadora

Se estima que los mensajes indeseados costaron a las empresas norteamericanas más de US\$ 10.000 millones en 2003, y un reciente estudio de la Comisión Europea nos muestra que el *spam* les cuesta a los usuarios europeos de Internet €10.000 millones al año. Existen cuatro áreas principales de molestias donde el correo *spam* le cuesta dinero a su organización.

Pérdida de productividad — La cantidad de tiempo que los usuarios gastan al leer y administrar mensajes indeseables. Se estima que la pérdida de productividad de los usuarios sea el mayor costo asociado al *spam* para las empresas.

Contenido inadecuado — Los mensajes que, de algún modo, se consideran ofensivos y, muy probablemente, violan la política de RH. Este tipo de mensaje puede ofender a personas o grupos (por

ejemplo, el mensaje puede tener contenido para adultos).

Consumo de recursos de IT — La cantidad de ancho de banda de la red ocupado por el *spam* que realmente logra alcanzar la red.

Spam como una amenaza a la seguridad — Los correos electrónicos *spam* pueden contener códigos malintencionados o ataques de DDoS; los e-mails infectados por virus pueden usar métodos de distribución semejantes al *spam* (por ejemplo: Sobig.F – Correos de envío Masivo, etc.) .

Exploración del Spam

Reducción de la amenaza

McAfee SpamKiller for Microsoft Exchange reduce los costos acarreados por el *spam*, explorando los mensajes entrantes que llegan al servidor Exchange. Tras la exploración, se puede poner el e-mail *spam* en cuarentena, en una carpeta de basura electrónica del servidor o del propio usuario. Detectando el *spam*, usted impide que sus usuarios tengan que manejar mensajes indeseables, ayudándoles a aumentar su productividad. Además, ayudará a impedir que sus empleados reciban contenidos inadecuados en e-mails, permitiendo una mejor aplicación de sus políticas de RH. Impedirá el desperdicio de ancho de banda — transferencia de archivos y almacenamiento en el *desktop* —pues el material ofensivo quedará almacenado de forma segura en una carpeta que reside en el servidor. Usted también reducirá los riesgos para la seguridad asociados a los e-mails *spam*.

Reglas predefinidas

Detección instantánea

La tecnología central de la familia de productos McAfee SpamKiller es el *engine* McAfee SpamAssassin™, que opera con un sistema de clasificación, atribuyendo puntuaciones a los mensajes según una serie de pruebas. Es altamente preciso en la identificación del *spam*, capturando hasta un 95% de todo el *spam*, además de brindar una tasa muy reducida de identificación de falsos positivos (menos de 0,05%). McAfee Security mantiene las reglas predefinidas que acompañan al producto. No se necesita ninguna configuración de reglas, pues McAfee SpamKiller es extremadamente eficaz en la detección del *spam*, sin ningún ajuste.

Sistema de puntuación

Puntuaciones distintas para mensajes distintos

SpamAssassin utiliza un sistema de puntuación basado en un amplio conjunto de reglas, para determinar si el mensaje de e-mail es *spam*. Cientos de reglas se aplican a cada e-mail y se asocia cada regla a una puntuación negativa o positiva. Reglas con puntuación negativa indican atributos de e-mails legítimos y reglas con puntuación positiva indican atributos de mensajes no solicitados. Combinadas, dichas puntuaciones individuales atribuyen a cada e-mail una “clasificación general de spam”. Un algoritmo genético optimiza la puntuación, utilizando un archivo de millones de mensajes de *spam* y que no son *spam* para determinar las puntuaciones de cada regla. Ahora que se utiliza el e-mail como una parte crítica de la infraestructura de negocios, es vital que todos los proveedores de anti-spam brinden protecciones contra mensajes incorrectamente identificados como *spam*. El uso de un sistema de puntuación es obligatorio hoy día, pues permite la detección de las áreas “nebulosas” del *spam*.

Edición de reglas

Ajuste de las reglas a través de la interfaz de usuario

Si el administrador quiere aumentar las reglas predefinidas, podrá hacerlo a través de la interfaz administrativa. Personalizar las reglas en cada organización permite que el administrador ajuste con precisión el sistema a sus necesidades.

Múltiples niveles de protección contra el *spam*

Cinco niveles que aseguran la detección

Utilizando el proceso subyacente de conjuntos de reglas predefinidas, McAfee SpamKiller verifica, a través de cinco métodos distintos de detección, cada e-mail que se recibe.

- **Análisis de integridad** — McAfee SpamKiller examina el encabezamiento, el *layout* y la organización de cada mensaje de e-mail para identificar las características comunes de *spam*. Un avanzado *engine* de comparación de patrones aplica simultáneamente cientos de algoritmos durante un único paso, determinando una clasificación de probabilidad que define si el mensaje es *spam* o no. Este es un método altamente preciso de detección de *spam*, que asegura una excelente detección de mensajes de *spam*.

- **Método de detección heurística**—Este método utiliza una serie de pruebas internas para determinar la probabilidad de que un mensaje sea *spam*. Cada prueba atribuye una puntuación para ayudar a reducir falsos positivos. Esto asegura que McAfee SpamKiller operará proactivamente para proteger su entorno contra el *spam*.

Filtración Bayesiana — McAfee SpamKiller cuenta con tecnología de filtración Bayesiana para permitir que los mensajes de *e-mail* sean evaluados de manera inteligente con base en criterios de lo que es y de lo que no es *spam*. La filtración Bayesiana ofrece cuenta con un banco de datos predefinido de filtros Bayesianos, además de una tecnología preventiva de aprendizaje automático de los tipos de mensajes que deben ser clasificados como *spam* y no-*spam*, en su empresa.

Filtrado de contenido — Se puede utilizar esta función para ayudar a identificar las palabras o giros claves que aparecen en un e-mail y que pueden indicar que el mensaje es *spam*. El administrador o el usuario (dependiendo del tipo de software que se está utilizando – servidor o cliente) puede incluir palabras o giros en una base de datos para definir el contenido inadecuado.

- **Blacklists y Whitelists** — El administrador es capaz de establecer los estándares en el nivel del servidor para determinar e-mails de *spam* para todos los integrantes de la organización, utilizando configuraciones globales de *whitelists* y de *blacklists*. Personalizar las *blacklists* y *whitelists* permite que los usuarios vean y editen sus propias listas. Esta poderosa función transfiere a sus usuarios finales la decisión final sobre qué es *spam* o no, liberando el tiempo del administrador de sistemas para otras tareas.

- **Autoajuste** — McAfee SpamAssassin es capaz de aprender las características de los e-mails que usted recibe. Es capaz de usar la información para ajustar la “clasificación general de *spam*” de nuevos mensajes enviados por un remitente conocido. El autoajuste ayuda a reducir la identificación de e-mails falsos positivos y aumentar la tasa de detección de *spam* sin que el administrador o el usuario necesiten configurarla. Por lo tanto, McAfee SpamAssassin es esencial en la batalla para reducir el costo total de propiedad.

Múltiples opciones de cuarentena

Cuando se detecta el *spam*, McAfee SpamKiller lo pone en cuarentena en el servidor e indica los mensajes como *spam* antes de transferirlos al buzón del usuario. Los administradores también tienen la opción de usar la utilidad incorporada o de transferir el *spam* para carpetas de basura electrónica especificadas en la red (por ejemplo, las

carpetas personales de basura electrónica del usuario y áreas de cuarentena del sistema).

Reportes detallados y administración centralizada

Analice la detección del *spam*

McAfee SpamKiller for Microsoft Exchange se integrará con McAfee ePolicy Orchestrator® para centralizar la administración y la emisión de reportes. Con ello, los administradores buscan y evalúan las vulnerabilidades del sistema, mantienen actualizada la protección, configuran y fiscalizan las políticas de protección y generan reportes gráficos detallados.

Compatibilidad total con McAfee GroupShield for Microsoft Exchange

McAfee SpamKiller for Microsoft Exchange es un complemento de la tecnología McAfee GroupShield® for Exchange existente, que brinda protección de primera clase contra el *spam* en entornos de computación colaborativa. Si instala en el mismo servidor McAfee SpamKiller y GroupShield for Microsoft Exchange, podrá compartir la consola de administración de ePolicy Orchestrator.

Anti-Phishing

McAfee SpamKiller incluye reglas específicas que ayudan a identificar ataques de phishing observando ciertas características específicas de phishing presentes en e-mail. Una vez aplicadas, Spamkiller atribuye una puntuación, que resulta en la mayoría de los casos en bloqueo. En conjunto con el Anti-Phishing Working Group (APWG), McAfee ha compilado un considerable Banco de Datos de ataques de phishing que utiliza para crear reglas efectivas de filtrado de estos ataques.

Requisitos de sistema

Es importante observar que se puede instalar McAfee SpamKiller en servidores Exchange que ya ejecutan software antivirus.

- **Plataforma de Correo** — Microsoft Exchange 2000 o 2003 Server o Advanced Server
- **Sistema operativo** — Microsoft Windows 2000 o 2003
- **Límite del buzón** — Ilimitado

McAfee System Protection Solutions

- **Espacio en disco** — 200MB de espacio libre en el disco duro o más
- **Memoria** — 512MB de memoria o más
- **Procesador** — Pentium II de 400MHz o superior

McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054, 408.988.3832 principal, www.mcafeesecurity.com

Los productos de Network Associates® evidencian años de experiencia y compromiso con la satisfacción de los clientes. El equipo PrimeSupport® de técnicos de soporte, atentos y altamente calificados, brinda soluciones a medida y asistencia técnica detallada para administrar el éxito de proyectos esenciales — todo con niveles de servicio que atienden a las necesidades de todas las organizaciones. McAfee® Research, líder mundial en sistemas y seguridad de la información, sigue en la vanguardia de la innovación en el desarrollo y el refinamiento de todas nuestras tecnologías.

