

# McAfee GroupShield for Microsoft Exchange Server

Los entornos de computación abierta que permiten el reparto de información, puede dejar a las empresas vulnerables a ataques. Muy frecuentemente, contenidos inadecuados u ofensivos son enviados, recibidos o circulan en una empresa, exponiendo a las organizaciones a responsabilidades legales. Además, debido a que los gusanos, los virus y otras amenazas de Internet muy a menudo entran y se diseminan a través de adjuntos de e-mail, y a que los archivos de datos se comparten rutinariamente a través de bases de datos internas, los sistemas de e-mail y groupware requieren soluciones especializadas que protejan contra las amenazas que invaden el entorno Microsoft® Exchange, sin que importe si la amenaza es un virus, contenido inadecuado o *spam*. Si no existe una protección contra amenazas tales como gusanos, virus y atacantes, el resultado puede ser tiempo de inactividad, pérdida de ingresos, reducción de la productividad y hurto de datos.

McAfee® GroupShield® brinda una amplia seguridad de contenido para los servidores Microsoft Exchange. Con su avanzada administración de contenido, el eXtended Policy Support, McAfee Outbreak Manager, Microsoft Virus Scanning API, anti-spam integrado con McAfee Security SpamKiller® "powered by McAfee SpamAssassin™" y McAfee ePolicy Orchestrator®, McAfee GroupShield permite protección completa de contenido para ambientes computacionales compartidos. McAfee GroupShield, como parte de la estrategia McAfee Protection-in-Depth™, protege los sistemas contra ataques perjudiciales y datos inadecuados que puedan causar estragos a los servidores de la empresa y comprometer sistemas y redes corporativos.

## McAfee SpamKiller for Microsoft Exchange

Al instalar McAfee GroupShield con McAfee SpamKiller for Microsoft Exchange, los usuarios reciben un reforzado anti-spam en una única solución optimizada. Con incomparable detección y rendimiento anti-spam, McAfee SpamKiller no tiene rival en la protección de Microsoft Exchange. McAfee SpamKiller brinda detección anti-spam líder del mercado basada en reglas, además de cinco niveles de protección contra *spam*, proporcionando hasta un 95% de precisión, con baja detección de falsos negativos y falsos positivos, sin necesidad de adaptaciones.

## Integración con McAfee ePolicy Orchestrator

### Mayor facilidad de administración y mejores reportes gráficos

McAfee GroupShield se integra con McAfee ePolicy Orchestrator, proporcionando una estricta conformidad antivirus, reportes y administración a nivel corporativo —

brindándole una visión completa de su política de seguridad antivirus. McAfee GroupShield se integra con ePolicy Orchestrator, una de las únicas herramientas de administración de políticas de seguridad verdaderamente flexibles, para administración de políticas, emisión de reportes gráficos detallados y distribución de software. ePolicy Orchestrator ofrece una consola única para administrar sus implementaciones de McAfee GroupShield y McAfee SpamKiller for Microsoft Exchange, además de todas las soluciones de McAfee Security en todo su entorno. ePolicy Orchestrator permite que los administradores aseguren la protección de sus redes, por medio de una de las principales soluciones de seguridad de contenido para Microsoft Exchange existentes hoy día en el mercado.

Determinar la eficacia de su McAfee GroupShield en su política de seguridad no requiere ningún esfuerzo con ePolicy Orchestrator y su amplia gama de reportes predefinidos, información sobre la distribución de actualizaciones y actividad de virus. Debido a que el aspecto más difícil de la implementación y administración proactiva de la política de seguridad, es obtener la visibilidad necesaria para evaluar la eficacia de su política y descubrir las debilidades de su red, además es fácil personalizar los reportes según sus necesidades específicas.

## Administración de brotes

### Bloquea los brotes antes que empiecen

McAfee Outbreak Manager utiliza una innovadora tecnología antivirus que bloquea automáticamente los brotes antes que empiecen. Tener Outbreak Manager es como tener un administrador veinticuatro horas al día en el sitio, listo para actuar en caso de brotes de virus o actividades inusuales, añadiendo una nueva dimensión a la estrategia de defensa de su red. Utilizando reglas definidas por el administrador, busca nuevos ataques al observar actividades típicas de nuevos brotes de virus. Se puede instruir a Outbreak Manager para que opere en los modos automático o manual. En el modo manual, cuando se detecta un brote de virus, Outbreak Manager lo reporta al administrador de e-mail que, entonces, determinará la acción necesaria para contener el brote. Además, Outbreak Manager puede operar en el modo automático. En este caso, si se detecta un brote, realiza algunas tareas predeterminadas para proteger el entorno de e-mail contra posibles infecciones, sin necesidad de ninguna intervención manual, como, por ejemplo, aumentar los parámetros de exploración o bloquear ciertos tipos de adjuntos de correo, según diversos criterios.

## Administración avanzada de contenido

Muy frecuentemente, contenidos inadecuados u ofensivos son enviados, recibidos o circulan en una empresa, exponiendo la organización a responsabilidades legales. McAfee GroupShield bloquea contenidos inadecuados que puedan ser ofensivos a los empleados, con una avanzada administración de contenido. McAfee GroupShield puede analizar el contenido del cuerpo de los mensajes de e-mail y muchos cientos de adjuntos de e-mail en busca de palabras o frases inadecuadas. Además, McAfee GroupShield puede registrar e-mails y ponerlos en cuarentena para ayudar a las organizaciones a cumplir las leyes respecto a mensajes de e-mail inadecuadas, según:

- El verdadero tipo del archivo adjunto
- Nombres de archivos adjuntos
- Tamaños de los archivos adjuntos
- Contenido de la línea de asunto del mensaje
- Contenido del cuerpo del mensaje
- Contenido del adjunto del mensaje

Para reducir aún más la responsabilidad legal, McAfee GroupShield puede añadir mensajes de exención de responsabilidad al encabezamiento o al pie de los e-mails.

## eXtended Policy Support

McAfee GroupShield permite que los administradores apliquen políticas de contenido a usuarios o departamentos. Las políticas de grupos se pueden aplicar como una excepción a las políticas globales de *scan* de contenido de McAfee GroupShield. Ahora, los administradores pueden aplicar políticas departamentales más detalladas, tales como mensajes de exención de responsabilidad departamental o filtrado de archivos adjuntos, brindando una seguridad más estrecha donde se necesita. McAfee GroupShield viene con diez políticas de grupos de usuarios. McAfee eXtended Policy Support permite un número ilimitado de políticas para usuarios, aumentando el número de controles detallados de seguridad de contenido para usuarios o departamentos. Las empresas que utilizan el McAfee SpamKiller for Exchange también reciben el eXtended Policy Support.

## Reglas inteligentes de contenido

La dificultad de intentar bloquear el contenido inadecuado es diferenciar qué es inadecuado y, por lo tanto, debe tener su entrada, salida o circulación prohibidas en la organización. McAfee GroupShield posee reglas inteligentes de contenido que se pueden aplicar a los cuerpos o adjuntos de los mensajes de e-mail, incluso reglas basadas en palabras, para bloquear contenidos inadecuados (por ejemplo, lenguaje inadecuado, drogas, sexo, desnudez, racismo e intolerancia). El administrador puede personalizar dichas reglas. Cada grupo de muestras de reglas posee tres niveles de severidad: alto, medio y bajo, dependiendo de la severidad de las palabras utilizadas. Las reglas inteligentes de contenido también

proporcionan criterios de uso para impedir la identificación de palabras falsas-positivas, tan común a muchas palabras o frases. Además, las reglas inteligentes de contenido son localizadas para brindar soporte adicional a cada país en organizaciones globales.

## Engine de Detección y Limpieza de McAfee

### Insuperables detección y limpieza de virus

Como todos los productos antivirus de McAfee, McAfee GroupShield está basado en el premiado *scan engine* de McAfee. Siempre reconocido por organizaciones de pruebas independientes como la tecnología líder mundial en detección y limpieza de virus, el *engine* bloquea todos los tipos de amenazas de virus y códigos malintencionados, incluso virus de macro, troyanos, gusanos de Internet, virus avanzados de 32 bits, hasta objetos ActiveX y Java hostiles. McAfee tiene un envidiable historial en pruebas independientes, brindando detección y limpieza eficaces.

### Siempre actualizado

McAfee GroupShield posee el AutoUpdate, que permite la descarga automática de los más recientes archivos de definición de virus (DAT) a través de FTP o reparto de archivos en la red. Esta función automatizada del lado del servidor asegura que usted siempre tendrá los archivos DAT más recientes de McAfee.

### API de exploración de virus

Utilizando la API de exploración de virus de Microsoft, GroupShield brinda la forma más segura de realizar la exploración del "Information Store" de Microsoft Exchange. GroupShield mantiene su compatibilidad inversa con la Virus Scanning API 2.0, admitiendo el nuevo recurso avanzado del VS-API 2.5 para Microsoft Exchange 2003. GroupShield realiza la exploración del cuerpos y adjuntos de todos los mensajes enviados o recibidos desde el cliente de acceso a Web de Outlook (OWA), clientes basados en Internet (POP3/IMAP), o el cliente Outlook (MAPI), además de realizar la exploración a nivel de Transporte de SMTP, impidiendo, así, que los e-mails sean guardados en el Information Store y brindando protección en entornos configurados con servidores *bridgehead*.

### Exploración del Tráfico SMTP

McAfee GroupShield permite el análisis de tráfico SMTP antes que entre al Information Store de Exchange. McAfee GroupShield permite la exploración del Tráfico SMTP de mensajes encaminados — mensajes que no han sido dirigidas al servidor local — además de bloquear la entrega de mensajes. La exploración del tráfico SMTP puede ser aplicado a Microsoft Exchange 2003 con la VS-API 2.5 para los usuarios de Exchange 2000. La exploración del tráfico SMTP viene junto con el GroupShield. Por lo tanto, los servidores Exchange 2000 pueden contar con la misma seguridad que disfrutaban los servidores Exchange 2003.

## Desechado de mensajes

McAfee GroupShield informa al remitente, al destinatario y al administrador con un mensaje de alerta siempre que se detecta un virus en un mensaje de e-mail. En caso de virus de envío masivo de e-mails, tales como Melissa o Bubbleboy, que se propagan con una velocidad alarmante, esos útiles mensajes de alerta pueden convertirse en una molestia. McAfee GroupShield puede manejar de forma distinta los alertas de virus de envío masivo de e-mails, además de impedir la recepción del exceso de mensajes de alerta.

## Fácil instalación y distribución

Los administradores de e-mail necesitan comprender su entorno de Microsoft Exchange y necesitan saber si el proceso de instalación será tranquilo y sin molestias. McAfee GroupShield for Microsoft Exchange brinda una instalación más fiable aún y una distribución más fácil que nunca. Además, McAfee GroupShield se puede distribuir remotamente a través de McAfee ePolicy Orchestrator, proporcionando distribuciones globales más fáciles aún.

## Administración por la Web

Los usuarios de McAfee GroupShield también pueden usar una interfaz de administración por la Web para facilitar el uso, aprovechar recursos de administración remota y obtener auxilio remoto dinámico para la configuración.

## Administrador de alertas

McAfee GroupShield brinda una excelente visibilidad de la seguridad perimetral antivirus, permitiendo que los administradores reciban alertas detalladas. Además, McAfee GroupShield permite que los administradores configuren una amplia gama de alertas de sistema que se pueden accionar, filtrar y priorizar selectivamente. McAfee GroupShield también se integra con McAfee Alert Manager, permitiendo que usted cree fácilmente sofisticadas políticas de notificación que alerten a múltiples funciones administrativas. Se pueden enviar los alertas a través de e-mail, *pager*, mediante el registrador de eventos de Microsoft y mensajes de red.

## Requisitos de sistema

### Requisitos mínimos para instalación en Microsoft Exchange 2000

- Procesador Intel Pentium o compatible de 133MHz
- 128MB de RAM (se recomiendan 256MB)
- 740MB de espacio libre en el disco duro
- Microsoft Windows 2000 Server con Service Pack 4
- Microsoft Exchange 2000 Server con Service Pack 3
- Internet Explorer 5.5 o más reciente

### Requisitos mínimos para instalación en Microsoft Exchange 2003

- Procesador Intel Pentium o compatible de 133MHz
- 128MB de RAM (se recomiendan 512MB)
- 740MB de espacio libre en el disco duro
- Microsoft Windows 2000 Server con Service Pack 4
- Microsoft Windows 2000 Advanced Server con Service Pack 4
- Microsoft Windows Server 2003 Standard Edition (32 bits)
- Microsoft Windows Server 2003 Enterprise Edition (32 bits)
- Internet Explorer 5.5 o más reciente

**McAfee Security** 3965 Freedom Circle, Santa Clara, CA 95054, 408.988.3832 principal, [www.mcafeesecurity.com](http://www.mcafeesecurity.com)

Los productos de Network Associates® llevan años de experiencia y compromiso con la satisfacción del cliente. 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.

Network Associates, McAfee, GroupShield, SpamKiller, powered by SpamAssassin, ePolicy Orchestrator, Protection-in-Depth, and PrimeSupport son marcas comerciales, registradas o no, de Network Associates, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. Los productos que llevan la marca Sniffer® son hechos sólo por Network Associates, Inc. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. ©2003 Network Associates Technology, Inc. Todos los derechos están reservados. 1-sps-gse-001-1203