



McAfee System Protection Solutions

Soluciones de Administración Segura de Contenido

Índice

Resumen Ejecutivo	3
Panorama	3
Retos a la Administración Segura de Contenido	3
Soluciones flexibles de Administración de Contenido	4
Soluciones para el Punto de Contacto (<i>Gateway</i>) con Internet	5
Soluciones para el Servidor de Aplicaciones	6
Solución de Servicios Administrados	7
Seguridad en varios niveles	8
Conclusión	8
McAfee PrimeSupport	9

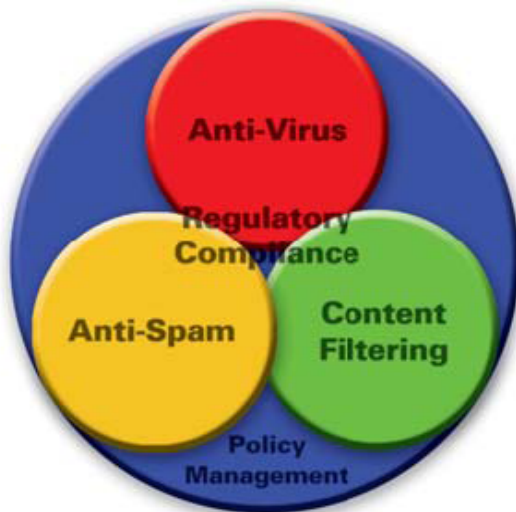
Resumen Ejecutivo

Proteger el contenido del tráfico que entra y sale de las empresas es esencial en los entornos de red actuales. Es esencial asegurar que su empresa cuente con una protección amplia contra contenidos inadecuados, malintencionados o virales, y que usted cumpla las políticas de seguridad de la empresa, cumpliendo, al mismo tiempo, las normas de privacidad definidas por el ramo y por la empresa.

Panorama

Las Soluciones de Administración Segura de Contenido de McAfee® ofrecen tecnología integrada y flexible para que las empresas pequeñas, medianas y grandes utilicen los recursos de la forma más eficaz, aumenten su productividad y eviten el comprometer las políticas definidas por el ramo y por la empresa. Con la mejor combinación de tecnologías antivirus, anti-spam y de protección de contenido, las Soluciones de Administración Segura de Contenido de McAfee están ligadas a lo mejor del mercado en términos de administración y fiscalización de políticas, asegurando que usted disponga de la flexibilidad de administración que tanto necesita.

Instaladas en el punto de contacto (*gateway*) con Internet o en servidores de aplicaciones colaborativas como el *e-mail*, las Soluciones de McAfee llevan la estrategia Protection-in-Depth™ a todas las aplicaciones principales asociadas, además de dispositivos de hardware y software integrados que permiten el control, la administración y la comprensión de su tráfico de Internet.



Funciones de administración necesarias para proteger el contenido de Internet y e-mail de una empresa.

Retos a la Administración Segura de Contenido

Antivirus

Vivimos en un mundo cada vez más comunicado por la red y las amenazas a esta evolucionaron en la última década a una velocidad alarmante. El impacto sobre las empresas aumentó a un ritmo increíble. Identificar las áreas de vulnerabilidad que ponen a su empresa y sus negocios en riesgo no es una tarea fácil en términos de conocimiento y recursos necesarios.

No sólo los incidentes de virus están aumentando, sino también la gravedad de dichos incidentes y el costo asociado a su recuperación también están en auge.

- Según la 8ª Encuesta Anual de Predominancia de Virus de Computadora, de ICSA Labs en 2002, se pidió que los encuestados identificaran los medios de infección de sus incidentes, desastres o encuentros más recientes y el 86% señaló al *e-mail* como la fuente principal
- Según Computer Economics, el virus Nimda les costó a las empresas US\$635 millones en limpieza y productividad perdida en 2001

Los virus y *worms* que se diseminan a través de *e-mail* pueden infectar toda su red en cuestión de minutos, interrumpiendo las comunicaciones con sus clientes y socios, además de interrumpir la comunicación y la colaboración dentro de la empresa. Dichos virus aprovechan los recursos automatizados de creación de *scripts* de las aplicaciones de *e-mail*, que son flexibles y ricos en recursos, para generar diluvios de mensajes de *e-mail* que ocupan los servidores y atascan los buzones de entrada.

Anti-Spam

La evolución sigue, y no sólo en términos de códigos malintencionados tales como virus, *worms* y troyanos. En el mundo de la mensajería de colaboración, las amenazas se están volviendo cada vez más diversificadas, intrusas y subversivas, y no siempre su objetivo es causar interrupciones directas en la productividad de los profesionales, aunque este sea, a menudo, el efecto.

- Según Gartner Research, los mensajes de *spam* les cuestan a las empresas norteamericanas US\$1000 millones al año en términos de productividad perdida
- Según el Aberdeen Group, se esperaba que el porcentaje de mensajes de *spam* que atascan las redes corporativas fuera del 25% en 2002 para el 50% en el pasado 2003

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054. 888.847.8766. www.mcafee.com

Los productos de McAfee® denotan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee PrimeSupport® de técnicos de soporte colaboradores y altamente cualificados brinda soluciones hechas a la medida, brindando asistencia técnica detallada para administrar el éxito de proyectos esenciales — todo eso con niveles de servicio que atienden a las necesidades de todas las empresas clientes. McAfee Research, líder mundial en sistemas de información e investigaciones de seguridad, sigue encabezando la innovación en el desarrollo y el refinamiento de todas nuestras tecnologías.

McAfee, Protection-in-Depth, WebShield, SpamKiller, SpamAssassin, SecurityShield, GroupShield, ePolicy Orchestrator, ePO, PortalShield y PrimeSupport son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo asociado a la seguridad es marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. © 2004 Network Associates Technology, Inc. Todos los derechos están reservados. 6-sps-scm-001-1004

Se utiliza cada vez más el *spam* como un nuevo mecanismo de distribución de troyanos y virus. Ya vimos la distribución de *backdoors* a través de *spam*, como ocurrió con el Adware-Surfbar en septiembre de 2003.

Con la creciente tendencia de los mensajes de *phishing*, el *spam* es creado para inducir al destinatario a revelar información personal como números de tarjeta de crédito, información bancaria, números de documentos personales, contraseñas y otra información sigilosa.

Anti-Phishing

McAfee SpamKiller® posee reglas específicas que ayudan a identificar ataques de *phishing*, buscando ciertas características peculiares de dicho tipo de ataque que puedan existir en los mensajes. Luego de su accionamiento, dichas reglas reciben automáticamente una puntuación general de *spam* del SpamKiller, resultando, en la mayoría de los casos, en el bloqueo de los mensajes. Junto con el Grupo de Trabajo Anti-Phishing (APWG), McAfee recopiló una detallada base de datos de ataques de *phishing*, utilizando el conocimiento sobre dichos ataques para crear reglas eficaces de filtrado.

Filtrado de Contenido

Muchas empresas están empezando a considerar al *spam* de contenido ofensivo como un problema jurídico, tras el precedente creado en Chevron. En 1996, Chevron Corporation se involucró en una contienda judicial con valor de US\$2,2 millones, pleiteada por empleadas que se sintieron ofendidas por un *e-mail* chistoso intitulado “25 motivos por los que la cerveza es mejor que la mujer”. Igualmente, un chiste racista que circuló en la red ofendió a algunos empleados y llevó a Morgan Stanley Dean Witter & Co. a enfrentar un pleito con el valor de US\$60 millones.

- Informes de IDC, en junio de 2001, señalan que el 48% de los empleadores que monitorean los empleados afirman que su intención es protegerse contra virus y contra la pérdida de información; el 21% monitorean los empleados como una forma de limitar la responsabilidad legal

Los empleadores siempre fueron responsables de las acciones de sus empleados en el entorno laboral. Sin embargo, si una empresa es capaz de demostrar el debido cuidado para reducir las actividades inaceptables de sus empleados, eso puede reducir la posibilidad de que la empresa sea responsabilizada.

- Según “The e-Policy Handbook”, de Nancy Flynn, el 27% de las empresas de la lista FORTUNE 500 ya necesitaron defenderse contra litigios de acoso sexual cuyo origen eran *e-mails* inadecuados

Administrar y proteger el contenido en un entorno de mensajería aumenta significativamente la productividad de los empleados.

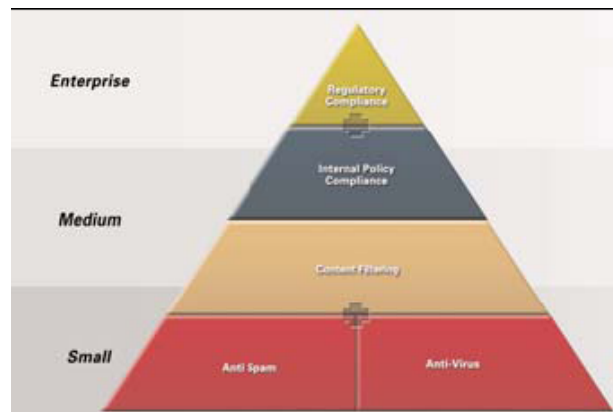
Cumplimiento de las Políticas Internas

Más que nunca, el trabajo del gerente de seguridad o de TI es un acto delicado de equilibrio. De un lado están las exigencias de los negocios — administrar una gama cada vez mayor de dispositivos y sitios y atender a las necesidades de un número cada vez mayor de usuarios móviles y empleados que trabajan fuera de la empresa. De otro lado están las exigencias de seguridad — mantener los sistemas actualizados y administrar los varios niveles de protección y las herramientas necesarias para combatir las amenazas de hoy que evolucionan constantemente.

Es esencial garantizar el cumplimiento de las políticas internas por su solución de Administración Segura de Contenido. La visibilidad y la fiscalización son fundamentales para asegurar que su protección esté actualizada y que realmente proteja su empresa.

Cumplimiento de Leyes y Normas

El cumplimiento de leyes de privacidad tales como HIPAA, GLBA y SEC siguen alimentando las preocupaciones de las empresas respecto a la seguridad de la mensajería. La tecnología de Administración Segura de Contenido permite no sólo proteger la mensajería en las empresas, sino también ayudan a impedir la fuga de información, permitiendo que las empresas establezcan políticas para protegerse contra responsabilidad legal. Los riesgos de la responsabilidad legal son cada vez mayores debido a empleados que descargan archivos MP3 y DVD integrales en los recursos de almacenamiento de la empresa. Dichas empresas tienen la obligación legal no sólo de asegurar que pueden cumplir las leyes y normas, sino también de protegerse desde el punto de vista legal.



McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054. 888.847.8766. www.mcafee.com

Los productos de McAfee® denotan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee PrimeSupport® de técnicos de soporte colaboradores y altamente cualificados brinda soluciones hechas a la medida, brindando asistencia técnica detallada para administrar el éxito de proyectos esenciales — todo eso con niveles de servicio que atienden a las necesidades de todas las empresas clientes. McAfee Research, líder mundial en sistemas de información e investigaciones de seguridad, sigue encabezando la innovación en el desarrollo y el refinamiento de todas nuestras tecnologías.

McAfee, Protection-in-Depth, WebShield, SpamKiller, SpamAssassin, SecurityShield, GroupShield, ePolicy Orchestrator, ePO, PortalShield y PrimeSupport son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo asociado a la seguridad es marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. © 2004 Network Associates Technology, Inc. Todos los derechos están reservados. 6-sps-scm-001-1004

Distribución de las funciones de administración segura de contenido entre los segmentos de empresas pequeñas, medianas y grandes.

Soluciones flexibles de Administración de Contenido

Las empresas pequeñas, medianas o grandes tienen necesidades básicas distintas respecto a una solución de administración segura de contenido (SCM), y cualquier solución que se considere en dicha área tendrá que ser capaz de seguir las necesidades de la empresa. Para una empresa pequeña, los elementos más comunes de la SCM — filtrado antivirus y anti-spam — son los más importantes, sin embargo también necesitan impedir la entrada de contenidos inadecuados. Empresas medianas tienen las mismas necesidades respecto a la tecnología antivirus y anti-spam, pero las necesidades respecto a dichas tecnologías, así como las necesidades con respecto al filtrado de contenido, se están volviendo cada vez más específicas y detalladas. Eso ocurre porque las empresas medianas poseen políticas de seguridad de mensajería de negocios que necesitan fiscalización y cumplimiento. Ejemplos de políticas de seguridad de mensajería: la necesidad de opciones específicas de cuarentena para individuos cuando la cuestión es de *spam*; permitir que sólo ciertos tipos de archivos entren en su empresa; o cubrir grupos específicos de personas. En suma, una empresa necesita ser capaz de establecer reglas de exploración para individuos o grupos de usuarios. Las necesidades de las grandes empresas respecto al cumplimiento de las políticas se están volviendo cada vez más detalladas debido a la necesidad de cumplir políticas detalladas de seguridad interna o leyes que vedan la salida de datos confidenciales de las empresas. Cualquier solución de SCM que se adquiera debe brindar a la empresa la mejor combinación de tecnologías en cada una de los principales áreas — antivirus, anti-spam y filtrado de contenido — además de ser capaz de proporcionar controles detallados de políticas para el tráfico entrante y saliente. Eso permite que la empresa cumpla todas las políticas de seguridad de mensajería. Otra ventaja de una solución integrada es que la empresa reducirá su TCO de administración, teniendo toda la tecnología central de mensajería disponible en una única solución.

Soluciones para la Puerta de Enlace (*Gateway*) con Internet

Appliances McAfee

Los Appliances McAfee son la piedra angular de las Soluciones de Administración de Contenido de McAfee para *Gateway*. Los Appliances McAfee 3100, 3200 y 3300 están disponibles en tres soluciones físicas altamente flexibles e instalables en *rack*. Utilizando tecnología de PC probada y aprobada de alta disponibilidad y un robusto sistema operacional Linux, los Appliances son una solución robusta y flexible para hospedar las Soluciones de Software para

Administración Segura de Contenido de McAfee. Los Appliances de McAfee ejecutan los programas McAfee WebShield® y McAfee SpamKiller individualmente o combinados en un único *appliance*.

Appliances McAfee WebShield

En los diferentes entornos de red de hoy, es esencial asegurar que el contenido que entra y sale de la empresa cumpla las políticas de seguridad de la empresa y las leyes que cuidan de la privacidad. Las Soluciones de Administración Segura de Contenido de McAfee utilizan una tecnología integrada y flexible que permite que empresas de cualquier tamaño optimicen sus recursos, aumenten la productividad e impidan el comprometimiento de sus políticas de seguridad. Con tecnologías de primera clase contra virus, *spam* y de protección de contenido, las Soluciones de Administración Segura de Contenido de McAfee permiten que usted controle, administre y comprenda su tráfico de Internet.

Los Appliances McAfee WebShield son una solución del tipo “configúrela y olvídense” para la puerta de enlace con Internet, explorando el tráfico de los protocolos SMTP, HTTP, FTP y POP3 que entra y que sale. Los Appliances son incomparables en términos de velocidad, detección, limpieza de virus y protección contra *e-mails* indeseables en la forma de *spam*, contenidos inoportunos. Estos *appliance* existen para empresas de cualquier tamaño.

Appliances McAfee SpamKiller

Los Appliances McAfee SpamKiller ofrecen protección anti-spam y filtrado de contenido, líderes del mercado en un único dispositivo que integra hardware y software. SpamKiller brinda una tasa de detección de *spam* del 95%, sin ningún ajuste. La tecnología central de los *appliances* SpamKiller es el mecanismo McAfee SpamAssassin™, que actúa a través de un sistema de puntuación, atribuyendo puntuaciones a los *e-mails* según una serie de pruebas. SpamAssassin utiliza un sistema de puntuación basado en un amplio conjunto de reglas, para determinar si un cierto *e-mail* es un *spam*. Cientos de reglas se aplican a cada *e-mail*, y cada regla lleva una puntuación negativa o positiva asociada a ella. Las reglas con puntuación negativa señalan atributos de mensajes legítimos, y las reglas con puntuación positiva indican atributos de mensajes no solicitados. Combinadas, dichas puntuaciones individuales les atribuyen a cada *e-mail* una puntuación general de *spam*. Utilizando el proceso subyacente de conjuntos de reglas predefinidas, los *appliances* SpamKiller verifican cada *e-mail* recibido, utilizando distintos métodos de detección.

- *Análisis de Integridad* — SpamKiller examina el encabezamiento, el *layout* y la organización de cada *e-mail*, identificando las características del *spam*

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054. 888.847.8766. www.mcafee.com

Los productos de McAfee® denotan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee PrimeSupport® de técnicos de soporte colaboradores y altamente cualificados brinda soluciones hechas a la medida, brindando asistencia técnica detallada para administrar el éxito de proyectos esenciales — todo eso con niveles de servicio que atienden a las necesidades de todas las empresas clientes. McAfee Research, líder mundial en sistemas de información e investigaciones de seguridad, sigue encabezando la innovación en el desarrollo y el refinamiento de todas nuestras tecnologías.

McAfee, Protection-in-Depth, WebShield, SpamKiller, SpamAssassin, SecurityShield, GroupShield, ePolicy Orchestrator, ePO, PortalShield y PrimeSupport son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo asociado a la seguridad es marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. © 2004 Network Associates Technology, Inc. Todos los derechos están reservados. 6-sps-scm-001-1004

- **Detección Heurística** — Usada para identificar mensajes como *spam* probable. La detección heurística utiliza una serie de pruebas internas para determinar la probabilidad de que un mensaje sea realmente un *spam*, y cada prueba atribuye una puntuación para ayudar a reducir los falsos positivos.
- **Filtrado de Contenido** — Esta función se puede usar para ayudar a identificar palabras claves o expresiones en un mensaje que puedan indicar que es un *spam*
- **Utilización de Blacklists y Whitelists** — “Listas negras” definidas por el administrador, que bloquean dominios conocidos por el administrador como remitentes de *spam*; además de “listas blancas” definidas por el administrador, que siempre permiten la entrada de mensajes desde dominios especificados por el administrador
- **Utilización de Listas de Bloqueo de DNS** — Los *appliances* WebShield permiten el uso de listas de bloqueo por DNS para la identificación de remitentes conocidos de *spam*
- **Filtrado Bayesiano** — Con la tecnología de filtrado bayesiano, la solución SpamKiller es capaz de enseñarse a sí misma qué es y qué no es *spam* para una empresa específica, proporcionando una detección de *spam* verdaderamente inteligente

Soluciones para el Servidor de Aplicaciones

McAfee SecurityShield for Microsoft ISA Server

Con funciones y velocidad incomparables de antivirus, anti-spam y filtrado de contenido, McAfee SecurityShield™ no tienen ningún rival en la protección del Microsoft® ISA Server 2000 y 2004.

Reconociendo originalmente los protocolos SMTP, HTTP y FTP, la protección de los principales protocolos de tráfico de *e-mail* de Web y de Internet está asegurada. Filtre el tráfico que entra y sale de la empresa o internamente si se usa Microsoft ISA Server entre departamentos o áreas de la empresa. Con McAfee SecurityShield, usted tiene lo mejor en tecnología antivirus, con el filtrado antivirus de primera clase de McAfee. SecurityShield puede reparar, bloquear o poner en cuarentena automáticamente el tráfico infectado, evitando que los códigos malintencionados entren o salgan de la empresa a través de los protocolos SMTP, HTTP y FTP.

Para las empresas que quieren la mejor defensa contra el *spam*, existe el SpamKiller for SecurityShield.

SpamKiller clasifica los *e-mails* según una serie de pruebas internas, proporcionando una detección extremadamente precisa, sin la necesidad de ningún otro ajuste. Brinda cinco niveles de protección contra *spam* anteriormente

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054. 888.847.8766. www.mcafee.com

Los productos de McAfee® denotan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee PrimeSupport® de técnicos de soporte colaboradores y altamente cualificados brinda soluciones hechas a la medida, brindando asistencia técnica detallada para administrar el éxito de proyectos esenciales — todo eso con niveles de servicio que atienden a las necesidades de todas las empresas clientes. McAfee Research, líder mundial en sistemas de información e investigaciones de seguridad, sigue encabezando la innovación en el desarrollo y el refinamiento de todas nuestras tecnologías.

McAfee, Protection-in-Depth, WebShield, SpamKiller, SpamAssassin, SecurityShield, GroupShield, ePolicy Orchestrator, ePO, PortalShield y PrimeSupport son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo asociado a la seguridad es marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. © 2004 Network Associates Technology, Inc. Todos los derechos están reservados.

mencionados: :¿ Análisis de Integridad , Detección Heurística,, Filtrado de Contenido, Utilización de Blacklists y Whitelists y Filtrado Bayesiano

McAfee GroupShield para Servidores de e-mail

McAfee GroupShield® para Servidores de e-mail es una protección amplia contra amenazas que llegan por *e-mail*, tales como virus y contenidos inadecuados, además de poseer un módulo complementario opcional anti-spam para servidores Microsoft Exchange 5.5, 2000, 2003 y Lotus Domino 5 o posteriores. Como un componente de las soluciones de administración segura de contenido para servidores de aplicaciones, GroupShield puede identificar e impedir la entrada y la circulación de mensajes o archivos hostiles en su entorno de servidor de *e-mail*. Sólo GroupShield se integra con el McAfee ePolicy Orchestrator® (ePO™) para permitir que los administradores administren las políticas y generen informes gráficos de forma centralizada. McAfee SpamKiller actúa como un complemento opcional de GroupShield, proporcionando recursos anti-spam inigualables como parte de una solución sencilla e integrada de seguridad de *e-mail*. Finalmente, McAfee Outbreak Manager brinda una defensa eficaz y preventiva contra el envío de *e-mails* en masa (que haría inútiles otras soluciones de seguridad).

Como todos los productos antivirus de McAfee, GroupShield utiliza el premiado mecanismo de exploración de McAfee. Siempre reconocido por organizaciones independientes de prueba como la tecnología líder mundial en detección y limpieza de virus, el mecanismo bloquea todos los tipos de virus y códigos malintencionados, incluso virus de macro, troyanos, *worms* de Internet, virus avanzados de 32 bits y objetos ActiveX y Java hostiles. McAfee tiene un envidiable historial en pruebas independientes por brindar detección y limpieza eficaces.

McAfee GroupShield cuenta con AutoUpdate, que permite la descarga automática de los más recientes archivos de definición de virus (DAT) a través de FTP o de unidades compartidas de la red. Dicha función automatizada en el lado del servidor asegura que usted estará siempre actualizado con los últimos archivos DAT de McAfee.

McAfee SpamKiller para Servidores de e-mail

McAfee SpamKiller para Servidores de e-mail ofrece protección amplia contra *spam* y contenidos inadecuados para servidores Microsoft Exchange 5.5, 2000, 2003 y para Lotus Domino 5 o posteriores. Disponible como un componente autónomo o combinado con McAfee GroupShield, SpamKiller para Servidores de e-mail brinda detección y velocidad incomparables contra el *spam* y no tiene ningún rival en la protección de servidores de *e-mail*. Diseñado para operar en alta velocidad, SpamKiller puede

ayudar a reducir los riesgos asociados al *spam*, explorando los mensajes luego de su llegada al servidor de *e-mail*. Tras ser sometido a la exploración, se puede poner al *spam* en cuarentena en una carpeta de basura electrónica en el servidor o en la carpeta de basura electrónica del usuario. Detectando el *spam*, usted impide que sus usuarios necesiten manejar mensajes indeseables, ayudándoles a aumentar su productividad. La tecnología central de los *appliances* SpamKiller es el mecanismo McAfee SpamAssassin. El mecanismo SpamAssassin opera a través de un sistema de puntuación que clasifica los *e-mails* según una serie de pruebas. SpamAssassin utiliza un sistema de puntuación basado en un amplio conjunto de reglas para determinar si un mensaje es *spam* o no. Se aplican cientos de reglas a cada mensaje y cada regla lleva una puntuación negativa o positiva asociada a ella. Las reglas con puntuación negativa señalan atributos de mensajes legítimos y las reglas con puntuación positiva indican atributos de mensajes no solicitados. Combinadas, dichas puntuaciones individuales les atribuyen a cada *e-mail* una puntuación general de *spam*.

Utilizando el proceso subyacente de conjuntos de reglas predefinidas, los *appliances* SpamKiller verifican cada *e-mail* recibido, utilizando los distintos métodos de detección anteriormente mencionados: *Análisis de Integridad*, *Detección Heurística*, *Filtrado de Contenido*, *Utilización de Blacklists y Whitelists* y *Filtrado Bayesiano*

McAfee PortalShield for Microsoft SharePoint Server

McAfee PortalShield™ for Microsoft SharePoint brinda seguridad de contenido a todos los documentos, archivos, contenidos de la Web y repositorios de documentos. Con PortalShield, los usuarios de Microsoft SharePoint pueden acceder, encontrar y compartir con seguridad la información que necesitan para que sean productivos profesionalmente, independientemente de la ubicación física de la información en la red. Los recursos de PortalShield van más allá de las soluciones tradicionales de seguridad antivirus y de contenido para proteger los servidores Microsoft SharePoint, detectando, limpiando y eliminando virus, además de buscar contenidos prohibidos dentro de los documentos almacenados en los espacios de trabajo de SharePoint.

Con un único paquete de software que brinda amplia exploración antivirus de todos los documentos, archivos, contenidos de la Web y repositorios de documentos en máquinas que ejecutan SharePoint Portal Server, PortalShield atiende la necesidad de las empresas pequeñas, medianas y grandes respecto a la implementación de tecnologías antivirus amplias que sean flexibles y administrables, ayudándolas a reducir su vulnerabilidad a ataques a contenidos y datos confidenciales.

Solución de Servicios Administrados

McAfee Managed Mail Protection

McAfee Managed Mail Protection brinda protección amplia de *e-mail* contra *spam*, virus, además de filtrado de contenido, todo eso como un servicio administrado. Managed Mail Protection explora los *e-mails* SMTP entrantes y salientes, que son encaminados a McAfee para detección y limpieza previas de *spam* y virus antes que entren o salgan del *gateway*, sin los altos costos y las molestias normalmente asociados a la seguridad de *e-mail* instalada físicamente en la red de su empresa. Junto con la amplia exploración de *e-mails* “en la nube”, McAfee Managed Mail Protection también ofrece — gratuitamente — acceso a un portal seguro en la Web para exhibir informes de visibilidad de *status* de *e-mail* y estadísticas de velocidad, además de personalizar las políticas de *e-mail*, aumentando la flexibilidad de su seguridad de *e-mail*. Transfiera su administración de seguridad de *e-mail* a McAfee para tener una protección automática siempre activa — y para que, así, usted pueda concentrarse otra vez sólo en sus negocios.

Compatible con todas las plataformas de *e-mail* (Exchange, Outlook, Lotus), Managed Mail Protection no exige la contratación de más profesionales ni la compra de más hardware y software para administrar las operaciones diarias de *e-mail*, reduciendo el costo total de propiedad de la seguridad de *e-mail*. Managed Mail Protection es un servicio administrado de seguridad que no es instalado ni se queda residente en la PC. Basta que un registro de Intercambio de E-Mail (MX) de una empresa sea redirigido a través de los servidores de McAfee para que el tráfico pase rápidamente por la exploración, con facilidad — antes que entre o salga de su red — con un retraso de menos de un segundo en el tránsito. Managed Mail Protection ayuda las empresas a protegerse contra los mensajes que consumen tiempo o contra contenidos inadecuados, sin aumentar la carga de trabajo del ya sobrecargado personal de TI o de la red existente.

Como parte de las Soluciones de Administración Segura de Contenido de McAfee, Managed Mail Protection brinda una tecnología integrada y flexible, asegurando que las comunicaciones de una empresa por *e-mail* se queden limpias y protegidas. La fiscalización de políticas seguras de contenido con Managed Mail Protection protege automáticamente sus comunicaciones esenciales y, al mismo tiempo, optimiza los recursos, aumenta la productividad e impide el comprometimiento de las políticas internas. Con Managed Mail Protection, un único servicio de seguridad brinda varios niveles de protección administrada con la confiable tecnología de McAfee.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054. 888.847.8766. www.mcafee.com

Los productos de McAfee® denotan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee PrimeSupport® de técnicos de soporte colaboradores y altamente cualificados brinda soluciones hechas a la medida, brindando asistencia técnica detallada para administrar el éxito de proyectos esenciales — todo eso con niveles de servicio que atienden a las necesidades de todas las empresas clientes. McAfee Research, líder mundial en sistemas de información e investigaciones de seguridad, sigue encabezando la innovación en el desarrollo y el refinamiento de todas nuestras tecnologías.

McAfee, Protection-in-Depth, WebShield, SpamKiller, SpamAssassin, SecurityShield, GroupShield, ePolicy Orchestrator, ePO, PortalShield y PrimeSupport son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo asociado a la seguridad es marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. © 2004 Network Associates Technology, Inc. Todos los derechos están reservados. 6-sps-scm-001-1004

Seguridad en varios niveles

Debido a que el perímetro se está convirtiendo en un área cada vez más incierta, las empresas ya no pueden presuponer que los servidores que se quedan detrás de las defensas de *gateway* están totalmente protegidos. Con un número cada vez mayor de servidores de aplicaciones, tales como portales de Web o servidores de intercambio de mensajes, expuestos a Internet, nos olvidamos, a menudo, que la posibilidad de fuga de información o de ataques es grande aún. Las Soluciones de Administración Segura de Contenido de McAfee son diseñadas para adecuarse a todos los niveles de la red, en el *gateway* y en sus principales servidores de aplicaciones.

La práctica recomendada para cualquier empresa es aplicar una protección amplia y con amplitud de protección. Su empresa necesita protección amplia para defenderse contra amenazas tales como virus, *worms*, *spam* y contenidos inadecuados y, al mismo tiempo, cumplir exigencias legales y fiscalizar las políticas internas. Además, las empresas necesitan de protección en el *gateway* y en los servidores de *e-mail* y de aplicaciones.

Las únicas soluciones que probadamente ofrecen protección amplia en varios niveles y combinan varios métodos de detección con protección en todos los niveles del entorno perimetral son las Soluciones de Administración Segura de Contenido de McAfee.

¿Por qué proteger el Puerta de Enlace (Gateway) con Internet?

Siendo el primer punto de entrada, el puerta de enlace (*gateway*) con Internet lleva la ventaja de ser un punto único de protección para toda la estructura de la empresa. Los *appliances* McAfee instalados en el puerta de enlace con Internet protegen el *e-mail* contra códigos malintencionados tales como virus, además de contenidos inadecuados en mensajes y *spam*. El tráfico de la Web es protegido contra códigos malintencionados, incluso usuarios con cuentas de Webmail personales. Cuidando del *spam* en el *gateway*, se ahorran el espacio de almacenamiento en la red y el ancho de banda a través del bloqueo de los mensajes antes que entren en el entorno de *e-mail* de la empresa.

Con menos dispositivos para administrar y mantener, los *appliances* de McAfee ejecutando WebShield y SpamKiller reducen el costo total de propiedad y aumentan la capacidad de reacción a brotes, con la capacidad de actualización rápida. Con un 'embudo' principal de seguridad para el relato de incidentes de seguridad en la red, es fácil lograr una visión amplia de la actividad en el puerta de enlace con Internet. Ya que McAfee WebShield y SpamKiller residen en los *appliances* diseñados con un sistema operativo robusto basado en Linux, los *appliances* reducen el riesgo de inactividad de la red debida al mantenimiento de los parches de seguridad, normalmente

asociada a los entornos operativos más ampliamente utilizados.

¿Por qué proteger los Servidores de Aplicaciones?

Los servidores de aplicaciones, incluso los servidores de *e-mail* y de colaboración (Microsoft Exchange, Lotus Domino), y los portales de Web (Microsoft SharePoint) representan dificultades únicas para la protección. Siempre que se envía o recibe un mensaje, lo que se escribe (una nueva solicitud de calendario u otro artículo, como un archivo o documento), el mensaje se queda almacenado en una base de datos o en otro repositorio de información. Si el mensaje contiene una amenaza, ésta se quedará almacenada y estará lista para infectar o propagarse tan pronto otro usuario la lea. Ni las soluciones antivirus para PC ni las soluciones antivirus para el *gateway* son capaces, sin auxilio, de explorar dichos tipos de repositorios o dichas bases de datos; por lo tanto, se convierten en puertos seguros desde donde se pueden lanzar futuras infecciones contra la empresa hospedera o sus clientes y socios. Además, se pueden encaminar los mensajes desde el servidor de mensajería a otro destinatario sin que los mensajes siquiera sean sometidos a la exploración en el cliente o pasen por el puerta de enlace con Internet. Los mensajes pueden ser transmitidos internamente sin que salgan de la red a través del puerta de enlace con Internet.

La protección en el nivel del servidor de aplicaciones permite un nivel más alto de personalización de políticas para usuarios/grupos, además de permitir que los administradores protejan el tráfico interno de *e-mail*, además del tráfico externo (que incluye el envío de materiales inadecuados dentro de la empresa).

Conclusión

Las soluciones de administración segura de contenido residen en dos "puestos avanzados" en el perímetro — el puerta de enlace con Internet (*gateway*) y el servidor de aplicaciones (área de *e-mail* o de mensajería de colaboración).

Manejar las actuales amenazas, el cumplimiento de las políticas internas y las exigencias legales significa asegurar que todas las áreas de su empresa están cubiertas. El puerta de enlace con Internet, como el primer punto de entrada en la estructura de la empresa, permite la implementación de soluciones que se pueden distribuir por toda la red de forma fácil y rápida. Sin embargo, debido a su amplio alcance, las soluciones de *gateway* no son capaces de penetrar en los servidores de *e-mail* y de colaboración debido a la naturaleza de su operación. Los entornos de *e-mail* o de colaboración presentan dificultades ligeramente distintas cuando la cuestión es proteger el entorno. Dichos servidores son vulnerables a los ataques tradicionales de red y transportados por *e-mail*, permitiendo el hospedaje de amenazas por largos períodos, contribuyendo, a menudo, con la reinfección de la red. Si se

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054. 888.847.8766. www.mcafee.com

Los productos de McAfee® denotan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee PrimeSupport® de técnicos de soporte colaboradores y altamente cualificados brinda soluciones hechas a la medida, brindando asistencia técnica detallada para administrar el éxito de proyectos esenciales — todo eso con niveles de servicio que atienden a las necesidades de todas las empresas clientes. McAfee Research, líder mundial en sistemas de información e investigaciones de seguridad, sigue encabezando la innovación en el desarrollo y el refinamiento de todas nuestras tecnologías.

McAfee, Protection-in-Depth, WebShield, SpamKiller, SpamAssassin, SecurityShield, GroupShield, ePolicy Orchestrator, ePO, PortalShield y PrimeSupport son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo asociado a la seguridad es marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. © 2004 Network Associates Technology, Inc. Todos los derechos están reservados. 6-sps-scm-001-1004

dejan los servidores sin verificación, también hospedarán una gran parte de las comunicaciones internas que no pasan por la puerta de enlace con Internet. Para proteger dichos entornos, las soluciones de administración segura de contenido necesitan residir en la plataforma del entorno de *e-mail* o de colaboración.

En términos sencillos, para proteger realmente el tráfico de mensajes entrantes y salientes de su empresa, es obligatoria la instalación de soluciones de administración segura de contenido en el puerto de enlace con Internet, en los servidores de *e-mail* y en todos los servidores de aplicaciones. Elegir una solución de administración segura de contenido de un proveedor como McAfee, que puede ofrecer una tecnología integrada de primera clase, ayudará mucho, con una interfaz única de administración para controlar las políticas en diversas áreas de operación, además de informes unificados de varios recursos de la administración segura de contenido. McAfee también es capaz de proveer una amplia gama de soluciones para cubrir toda su red, permitiendo que usted posea los mismos componentes tecnológicos premiados instalados en distintos puntos de entrada en la red – lo que es esencial para atender a las necesidades de una defensa de mensajes en varios niveles.

McAfee PrimeSupport

McAfee adoptó la estrategia de proveer tecnología de primera clase para cada tipo de aplicación de administración de rendimiento — pero la Estrategia Protection-in-Depth es más que sólo distribuir e implementar las mejores soluciones, hoy. La prevención es, seguramente, la prioridad número uno, pero, inevitablemente, ¡usted tendrá que reaccionar a uno y otro problema!

El programa McAfee PrimeSupport® es esencial para sacar el máximo provecho de su inversión en las Soluciones de Protección de Sistemas y Redes de McAfee. El equipo PrimeSupport de McAfee posee todos los recursos correctos y está lista para brindarle la solución de servicios que usted necesita. Entre los recursos del PrimeSupport están: autorización de acceso a todas las versiones de mantenimiento y actualizaciones de productos disponibles, acceso a una amplia gama de otros recursos de autoatención remota, soporte telefónico en vivo al que se puede acceder 24/7/365, gerentes de cuenta de soporte asignados disponibles, además de una amplia gama de soluciones de soporte de software y hardware que se pueden adaptar a sus necesidades.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054. 888.847.8766. www.mcafee.com

Los productos de McAfee® denotan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee PrimeSupport® de técnicos de soporte colaboradores y altamente cualificados brinda soluciones hechas a la medida, brindando asistencia técnica detallada para administrar el éxito de proyectos esenciales — todo eso con niveles de servicio que atienden a las necesidades de todas las empresas clientes. McAfee Research, líder mundial en sistemas de información e investigaciones de seguridad, sigue encabezando la innovación en el desarrollo y el refinamiento de todas nuestras tecnologías.

McAfee, Protection-in-Depth, WebShield, SpamKiller, SpamAssassin, SecurityShield, GroupShield, ePolicy Orchestrator, ePO, PortalShield y PrimeSupport son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo asociado a la seguridad es marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. © 2004 Network Associates Technology, Inc. Todos los derechos están reservados. 6-sps-scm-001-1004