



McAfee System Protection Solutions

Administración eficaz de Soluciones Antivirus y de Seguridad para Pequeñas Empresas

Índice

Introducción — ¿Es importante el tamaño?	3
¿Por qué es importante administrar una política de seguridad?	3
¿Qué significa “administrar”?	3
Si no es fácil de usar, no será usado	3
Mantener la actualización — El criterio más importante de la seguridad exitosa	4
Niveles de protección	4
La estrategia Protection-in-Depth de McAfee	4
Capacidad de planificar una reacción de seguridad	5
Capacidad de reacción	5
Disposición para invertir	5
El panorama de administración de McAfee — tres formas de administrar	5
Opciones de administración de seguridad de McAfee	6
McAfee PrimeSupport	8
Resumen	8

Introducción — ¿Es importante el tamaño?

Cuando la cuestión es defender las redes contra virus, *hackers* y otras amenazas, existen sólo dos categorías de usuarios — los que poseen una política de seguridad de TI definida, implementada y administrada, y los que no la poseen.

Existen algunas razones por las cuales muchas empresas no poseen una política de seguridad de TI. Cuentan con mano de obra de seguridad de TI limitada y los recursos que poseen se dedican a conducir sus operaciones comerciales. En su mayoría, son empresas pequeñas y medianas y necesitan auxilio para luchar eficazmente contra el aplastante número de amenazas que atacan sus redes. La mayoría de las grandes empresas ciertamente cuenta con equipos de TI y expertos en seguridad. La mayoría de las empresas menores no cuenta con dichos recursos.

Pero, en vez de concentrarse en el tamaño de la empresa, es más útil preguntarse sobre la capacidad del usuario de reaccionar a una amenaza a la seguridad. Entonces, otra forma de considerar la necesidad de soluciones de seguridad es examinar la medida en que el cliente es capaz de definir, implementar y distribuir una política de seguridad. Ser experto o analfabeto en seguridad. ¿Existen o no profesionales expertos en seguridad?

Se buscan — Profesionales de TI

Buscamos un superhombre para manejar instantáneamente 50 000 amenazas a la seguridad o más. Usted se ocupará de aplicaciones esenciales en todas las PC y los servidores. Entorno bajo constante ataque de terroristas cibernéticos. La protección necesita actualización semanal, mensual o inmediata. Debe ser capaz de trabajar con presupuestos restringidos. Los informes diarios al CIO necesitan presentar un 95% o más de usuarios en conformidad con la política. Elimine la amenaza y entre los beneficios estarán fines de semana libres. Pizza gratis en los domingos.

Paremos inmediatamente y preguntemos: *¿Qué es una política de seguridad?* Lo más sencillo es definir cuáles parámetros de configuración se deben aplicar al mecanismo de actualización del *firewall* o del antivirus para asegurar que, en general, el usuario esté protegido y actualizado. Lo más complejo es un conjunto de reglas sistemáticas divulgadas que valgan para todos los aspectos del sistema de TI y de la distribución de datos, definir aplicaciones aprobadas por la empresa, control de acceso y autenticación en la red, proveedores aprobados, grupos o dominios de usuarios, las configuraciones de cualquier número de distintos niveles de seguridad, etc.

Si una empresa necesita parar y preguntarse "*¿Qué es una política de seguridad?*", no importa el tamaño de dicha empresa: no logrará implementar exitosamente una solución de seguridad que exija definiciones de administración de políticas de seguridad de TI plenamente desarrolladas.

¿Por qué es importante administrar una política de seguridad?

Una de las dificultades que enfrenta cualquier empresa para administrar la seguridad de sus sistemas y asegurar protección completa es que, para fiscalizar el cumplimiento de las políticas, el administrador tiene que saber si hay algún problema con la conformidad de los sistemas de la empresa antes de que se pueda ponerlos en conformidad.

Una única computadora sin una protección adecuadamente administrada puede ser una amenaza para toda la red. Eso significa que conocer todos los sistemas conectados a la red es esencial para proteger exitosamente a la empresa.

Por lo tanto, tener una política de seguridad es bueno. Ser capaz de administrarla es mejor aún.

Nuevas amenazas afectan a empresas de todos los tamaños. Los proveedores tienen el deber de llevar herramientas de administración fáciles de usar a las empresas menores para que puedan reaccionar a las amenazas tan eficazmente como lo hacen las empresas mayores.

¿Qué significa "administrar"?

En el contexto de la seguridad de TI, el término "administración" se refiere a la capacidad de fiscalizar la conformidad de los usuarios, distribuir actualizaciones, generar informes de *status* y de excepciones, además de mantener a la red en buenas condiciones de seguridad — desde una ubicación central — controlada por una o más personas autorizadas.

Muchas soluciones de seguridad cuentan con un cierto nivel de autonomía administrativa incorporado. Todas las buenas aplicaciones antivirus cuentan con un proceso automatizado de actualización de archivos de detección de virus. Pero, aunque sea en redes pequeñas, eso es lento y, en última instancia, es imposible asegurar el cumplimiento uniforme de las políticas si cada sistema posee su propio mecanismo independiente de actualización, sin ningún mecanismo centralizado de control. Basta que un único usuario fuera de control altere las configuraciones de una única PC de la red para exponer toda la red a ataques.

Por lo tanto, administrar significa tener el control centralizado de la información y de las acciones para controlar el uso de grupos de PC en toda la red.

Si no es fácil de usar, no será usado

Para los empresarios extremadamente presionados y gerentes de TI no especializados en empresas menores, la facilidad de uso es un factor importante, así como la exigencia de adaptación en un escenario de amenazas que cambia constantemente.

El dilema de los proveedores es cómo poner las funciones necesarias en una solución de seguridad, equilibrando la facilidad de instalación, distribución y mantenimiento diario de dichas funciones. La capacidad de cambiar, adaptar o actualizar es fundamental para cualquier solución de seguridad, y es exactamente eso que distingue dichas soluciones de otras soluciones de oficina ampliamente utilizadas. Por su propia naturaleza, el escenario de seguridad es siempre cambiante. Por lo tanto, la facilidad de uso no debe significar “fácil de instalar, pero reprobado en la prueba de cambios”.

En el ramo de la seguridad de TI, donde las nuevas amenazas exigen que las soluciones de seguridad cambien constantemente, existe un aspecto fundamental en la conducción exitosa de una política de seguridad — la capacidad de cambiar — la capacidad de las empresas de definir sus políticas de seguridad y de implementar una solución que ejecute dichas políticas y permita que la reacción de las amenazas se adapte a lo largo del tiempo.

El cambio es un evento de proceso difícil para la mayoría de los usuarios. Las grandes empresas definen estándares de Entorno Operativo Común (COE) para intentar posibilitar la administración previsible de su infraestructura de TI. Pero definir un COE que haga imposible la implementación ágil de las actualizaciones de aplicaciones de seguridad en el actual escenario de amenazas mutantes es la receta del fracaso.

Para las pequeñas empresas, el concepto de cambio es difícil por razones distintas. Primeramente, no se comprende, a menudo, la necesidad del cambio. Todos saben que los virus son malos, pero ¿en qué momento de la semana media de trabajo del gerente de una pequeña empresa tiene la oportunidad de examinar la situación actual de las amenazas y de efectuar cambios en la política de seguridad de la red? ¿Cómo puede descubrir cuál puerto se debe bloquear para impedir que un nuevo *worm* se disemine? ¿Qué significa cuando Microsoft® divulga una nueva vulnerabilidad?

Nuevas amenazas explotan vulnerabilidades en la extremidad y en la margen, donde la defensa estándar implementada es, probablemente, la peor preparada para manejar la amenaza. ¿Cómo es posible defenderse contra una amenaza que todavía no fue descubierta? Aunque se descubra una nueva amenaza, ¿cómo es posible saber qué hacer para combatirla?

La seguridad de TI es un entorno en constante evolución, donde las amenazas tales como códigos malintencionados (virus, *worms*, programas espías) y explotaciones de vulnerabilidades (ataques de denegación de servicio, *hacking*, robo de datos) siempre desafían a los proveedores de seguridad a crear herramientas cada vez más sofisticadas para detectarlas, impedir las y alejarlas.

Mantener la actualización — El criterio más importante de la seguridad exitosa

Muchas empresas se dedican principalmente al mecanismo de actualización de su software antivirus. Este es un aspecto esencial del mantenimiento de una actitud defensiva sólida, pero

no basta por sí mismo. Una actitud defensiva sólida exige varios niveles de defensa, además de la capacidad de controlar la implementación, el ritmo, la distribución y la información de dichos niveles de defensa. En suma, la capacidad de administrar el software elegido para la protección contra virus es esencial.

Niveles de protección

Para que podamos definir un abordaje en varios niveles, se puede dividir la mayoría de las redes en las siguientes categorías:

- PC, servidores de archivos y otros dispositivos clientes
- Servidores de aplicaciones, tales como servidores de correo o servidores de portal
- Puntos de contacto (*gateways*) externos con Internet

En cada una de dichas categorías, McAfee posee varias soluciones específicas antivirus y de seguridad, con el intuito de brindarle al cliente lo mejor en soluciones para el nivel de las aplicaciones. Eso no es diferente del objetivo de otros fabricantes, y el cliente se beneficia de la naturaleza altamente competitiva del ramo y de los retos echados por los autores de programas malintencionados, en términos de innovación y perfeccionamiento constante de recursos para cada aplicación.

La estrategia Protection-in-Depth de McAfee

McAfee® posee una estrategia de reunir todas sus soluciones en una estructura única, que se llama “Estrategia Protection-in-Depth™”. Dicha estrategia permite que los clientes accedan a una amplia gama de productos de seguridad en varios niveles y para varias plataformas y que puedan impedir exitosamente las intrusiones, limitar el impacto de los ataques y reducir el costo de las operaciones de limpieza.

La implementación exitosa de un sistema de defensa de seguridad pasa esencialmente por la administración de políticas y de la conformidad de las aplicaciones. En el mundo de las pequeñas empresas, eso significa administrar el antivirus.



Estrategia Protection-in-Depth de McAfee.

Capacidad de planificar una reacción de seguridad

Virus, worms y otras formas de programas malintencionados no hacen distinción. Infectan o se proliferan dondequiera exista una oportunidad, a través de vulnerabilidades comunes de ingeniería social (usuarios) o de defensa de sistemas (profesionales de TI).

Las personas y empresas más afectadas son aquellas cuyas defensas son las más débiles. El hecho de que los virus son una amenaza está claro para empresas de todos los tamaños y segmentos, pero los medios para hacer algo por la defensa contra los virus con algo que vaya más allá de aplicaciones básicas antivirus varían enormemente según las características de la empresa o del usuario.

Las pequeñas empresas tienden a contar con menos profesionales especializados de TI y están menos preparadas para establecer una defensa exitosa contra programas malintencionados o intrusiones. Pueden contar con la capacidad técnica de implementar una política de seguridad de TI, pero no cuentan con los profesionales expertos para eso.

A menudo, los fabricantes del ramo de TI caracterizan sus clientes refiriéndose a su tamaño como empresas, normalmente dividido en pequeño, mediano o grande. Eso no es muy útil, especialmente cuando se intenta correlacionar las soluciones de seguridad con los clientes. En verdad, sólo hay dos tipos de clientes en términos de seguridad — los que cuentan con profesionales o recursos de TI y los que no cuentan — es decir, expertos en TI y analfabetos en TI.

Capacidad de reacción

¿Están protegidos todos mis usuarios?

¿Están actualizados todos mis usuarios?

Si la respuesta a cualquiera de las preguntas de arriba es “yo no sé”, entonces tenemos un problema de administración. Existe un fallo en el proceso de administración que significa, muy probablemente, que un ataque o una epidemia de virus podrán lograr éxito.

La cuestión se resume a la administración de los recursos. La incapacidad de administrar la conformidad de los usuarios, el proceso de actualización o el proceso de *backup* abren las puertas para que el cliente sufra daños a través de infecciones o intrusiones.

Algunos clientes simplemente no son capaces de reaccionar. Eso no significa que sean malos clientes, sino que simplemente necesitan auxilio para reaccionar. A menudo, simplemente no saben que necesitan reaccionar.

Disposición para invertir

De una forma o de otra, todo se resume a la inversión — así como todas las decisiones administrativas — si se invierte en recursos o si se transfiere la tarea a un proveedor externo. Las inversiones de este tipo siempre necesitarán adecuarse a restricciones, pero es posible lograr grandes ganancias aunque

sea con inversiones modestas.

En el ramo de la seguridad de TI, todos los clientes tienen en su favor un escenario extremadamente competitivo de proveedores, pues dichos proveedores luchan para hacer lo mejor por sus clientes y, naturalmente, conquistar los clientes de los otros proveedores.

No es sólo el precio lo que beneficia al cliente. La riqueza de funciones, la facilidad de uso y la calidad del soporte también son aspectos esenciales de una solución, y cada nueva versión brinda alguna novedad al usuario.

El panorama de administración de McAfee — tres formas de administrar

La gama de opciones de administración de McAfee permite que las empresas decidan si invertirán en herramientas que se puedan administrar sin intervención — más adecuadas a las empresas que cuentan con algunos o muchos expertos en TI — o si es mejor transferir la molestia a las soluciones administradas de servicios especialmente reunidas por McAfee y dedicar su tiempo a administrar los negocios mientras McAfee administra la política de seguridad.

1. Proceso de administración subcontratado
2. Simplificado, administración sin intervención
3. Grande, administración sin intervención

El objetivo es asegurar, independientemente de la abundancia o de la escasez de profesionales o recursos de seguridad de TI del cliente, que él esté seguro de que sus defensas estarán en el estado de prontitud ideal.

La principal diferencia entre lo sencillo y lo sofisticado es la gama de otras opciones de administración disponibles. El parámetro básico es la capacidad de mantener al menos un conjunto válido de configuraciones de seguridad (política), para que la aplicación antivirus, el *firewall* y la solución de prevención de intrusiones estén siempre funcionando para todos los usuarios a cualquier momento.

En un mundo ideal, se pueden administrar todas las amenazas con una única solución, de una forma adecuada a todos los tipos de usuarios. Pero no vivimos en un mundo ideal. La experiencia de McAfee con empresas que utilizan ePolicy Orchestrator® para administrar una gran infraestructura es que no existe un “tamaño único”. Las empresas menores necesitan un conjunto distinto de parámetros para alcanzar el 98% de las mismas metas, pero con una estructura simplificada de políticas. Hace varios años, McAfee viene operando sus soluciones administradas antivirus y de *firewall* para auxiliar a las empresas menores a alcanzar dicha meta y, hace poco tiempo, lanzó una consola de administración dedicada para empresas pequeñas y medianas, el McAfee ProtectionPilot™, para empresas que prefieren administrar por sí mismas sus instalaciones antivirus.

Opciones de administración de seguridad de McAfee

Transfiera el proceso de administración

- **Servicios Administrados de McAfee** — Los Servicios Administrados de McAfee brindan soluciones antivirus automáticas y siempre activas que son administradas 24 horas por día por los expertos de McAfee.
- **Público Objetivo** — Empresas que no poseen los profesionales o no quieren administrar sus configuraciones de antivirus o de *firewall*; probablemente, entre 2 y más de 100 usuarios.
- **Necesidades del cliente**
 - o Simplicidad de instalación
 - o Actualizaciones automáticas
 - o Generación sencilla de informes por un tablero de control
 - o Política única de seguridad

La mayor ventaja de implementar uno de los servicios administrados de McAfee es la transferencia de las decisiones de administración a un grupo de expertos. Para muchas empresas menores, el servicio McAfee Managed VirusScan® es una solución antivirus imperceptible y eficaz que se actualiza automáticamente al menos una vez por semana, o con mayor frecuencia, según lo exija la situación. El usuario no necesita tomar ninguna decisión sobre el nivel de riesgo de una amenaza. McAfee cuida de todas las decisiones sobre actualización. Sin embargo, el usuario es capaz de ver la situación de conformidad de todos los usuarios a través de la interfaz gráfica del tablero de control.



Informe del McAfee Managed VirusScan.

- **Simplificada, administración sin intervención (con McAfee ProtectionPilot)**
- **Público Objetivo** — Empresas pequeñas y medianas que quieren administrar sus propias defensas antivirus, pero que cuentan con pocos profesionales expertos especializados en seguridad de TI o que poseen una política sencilla de

seguridad de TI; normalmente, son empresas que poseen entre 25 y 250 usuarios

- **Necesidades del cliente**
 - o Simplicidad de implementación
 - o Configuración y administración de tareas con orientación
 - o Aplicación automática de actualizaciones
 - o Generación simple de informes por un tablero de control
 - o Capacidad de controlar y personalizar la política de seguridad

ProtectionPilot es una herramienta de administración centralizada de seguridad que permite un abordaje sencillo y preventivo de la implementación y de la administración continua de la protección antivirus, para administradores de red que administran hasta 500 computadoras. El asistente de instalación asegura la sencillez y la claridad del camino hacia la protección, y las actualizaciones automáticas empiezan inmediatamente.

Para las empresas que cuentan con algunos profesionales expertos en TI, ProtectionPilot presenta opciones de tareas que son intuitivas y orientadas por asistentes, que permiten que los administradores implementen y administren una política de seguridad fiscalizada automáticamente para sus usuarios. Dicha forma de defensa administrada sin intervención es viable y eficaz para empresas con pocos profesionales expertos en TI porque todo el *ethos* de facilidad de uso del diseño del ProtectionPilot cuenta con el respaldo de años de experiencia en ofrecer facilidad de administración para grandes empresas. El resultado es una amplia gama de funciones de control e información de antivirus que atiende a las necesidades de los clientes, sin comprometer el rigor de la conformidad en toda la red.

Donde otros proveedores esperan que el usuario se arrastre por interminables informes, McAfee facilita la visión de problemas de conformidad a través del tablero de control de informes. Cuando se incluyen nuevas computadoras, McAfee facilita el trabajo, permitiendo que se los arrastre hacia dentro del dominio administrado. Cuando los usuarios fuera de control o los colegas bienintencionados quieren ajustar las opciones de exploración antivirus, ProtectionPilot impone automáticamente la configuración correcta otra vez al sistema del usuario. Cuando McAfee publica un conjunto actualizado de archivos de características de detección de virus (DAT), ProtectionPilot les accede automáticamente y actualiza todos los usuarios de la red.

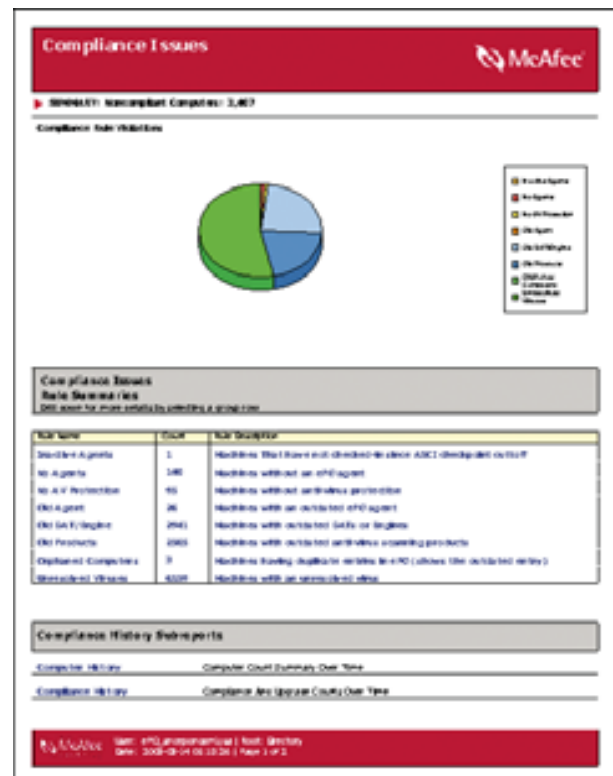


McAfee ProtectionPilot dashboard.

- **Grandes empresas, administración sin intervención (con ePolicy Orchestrator)**
 - **Público Objetivo** — Empresas medianas y grandes empresas que desean implementar una consola amplia y flexible de administración de políticas de seguridad y antivirus; adecuado para las empresas medianas y grandes empresas.
 - **Necesidades del cliente**
 - o Capacidad de centralización de la distribución
 - o Transmisiones de paquetes con ahorro de ancho de banda
 - o Repositorios distribuidos
 - o Estructuras jerárquicas de generación de informes
 - o Varios dominios administrados
 - o Detección de sistemas fuera de control
 - o Establecimiento del perfil de conformidad de los sistemas
 - o Informes personalizables de conformidad e infección
 - o Varios idiomas permitidos en un único dominio
 - o Acepta aplicaciones de varios fabricantes

ePolicy Orchestrator es la solución líder de mercado en administración de seguridad de sistemas, que brinda a la empresa una defensa coordinada y preventiva contra amenazas. Permitiendo una administración amplia e incomparable de la seguridad de los sistemas al menor costo de propiedad, asegura la conformidad con la política de seguridad de sistemas y la eficacia de la protección de las computadoras, evitando las dispendiosas interrupciones de negocios que causan las infecciones por programas malintencionados y otros ataques. Con el eje central de las Soluciones de Protección de Sistemas de McAfee, los administradores pueden tomar la iniciativa de reducir el riesgo de los sistemas fuera de control y no conformes, mantener la protección actualizada, configurar y fiscalizar las políticas de protección, además de monitorear la situación de seguridad, 24 horas por día, con una única consola centralizada y verdaderamente flexible para acompañar cualquier tamaño de infraestructura.

Hace más de cuatro años, ePolicy Orchestrator se estableció como la consola líder en conformidad de sistemas y administración de seguridad en el ramo de seguridad de TI. Muchos fabricantes poseen recursos de registro de eventos o generación de informes, pero pocos permiten que se tomen medidas para ejecutar acciones correctivas en una gama tan amplia de aplicaciones, afectando muy poco a la velocidad de la red y proporcionando tanta flexibilidad.



Informe del McAfee ePolicy Orchestrator.

El abordaje por tablero de control de ProtectionPilot es reemplazado por un entorno gráfico completo, comandado por menús, de generación de informes. Los usuarios fuera de control son identificados, mientras que distintas políticas de seguridad se pueden definir y aplicar a una amplia gama de grupos de usuarios y dominios. ePolicy Orchestrator pone al responsable de la seguridad de TI en el control de la implementación de la política de seguridad de la empresa, permitiendo que se alcance una conformidad demostrable.

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.

Resumen

Una política sencilla de seguridad que sea fácil de administrar será siempre más eficaz que una política sofisticada que sea imposible de administrar. Quizás el hecho más importante sea que una política de seguridad sencilla es mucho mejor que ninguna. Los clientes pueden contar con McAfee para encontrar soluciones de administración de políticas en ambos extremos del espectro, según su capacidad de administración o las necesidades de su infraestructura de TI. Las opciones de administración de seguridad de McAfee permiten que los clientes implementen las políticas de seguridad de TI más eficaces y apropiadas. Eso significa que pueden mantener el control de la seguridad de sus redes, sin forzar su personal de TI más allá del límite. McAfee significa opciones de administración.

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, ePolicy Orchestrator, ProtectionPilot, VirusScan, 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-mgt-001-1104