

McAfee ePolicy Orchestrator 3.5

Administre centralizadamente la seguridad de sus sistemas

Los sistemas conectados en red necesitan una constante vigilancia contra amenazas y ataques — que andan siempre por ahí, probando las defensas y sondeando las debilidades. Por eso, el trabajo del administrador es un delicado acto de equilibrio. Por un lado están las exigencias de los negocios — administrar una gama cada vez mayor de dispositivos y atender a las necesidades de un número cada vez mayor de usuarios móviles. Por otro lado están las exigencias de seguridad — mantener sus sistemas en conformidad y administrar los diversos niveles de protección de última generación así como las herramientas necesarias para el combate a las amenazas de hoy, que siguen evolucionando.

Es esencial que se pueda visualizar completamente la seguridad de su sistema y fiscalizar lo que ya está implementado. En última instancia, cada una de dichas exigencias es constante e igual. Basta un error y todo su universo puede caer en completo desequilibrio.

McAfee® ePolicy Orchestrator® 3.5 (ePO™) es la solución de administración de seguridad de sistemas líder de mercado — que brinda una defensa preventiva coordinada contra amenazas y ataques a la empresa. Con ese robusto núcleo de las soluciones de Protección de Sistemas de McAfee, los administradores pueden reducir el riesgo de los sistemas desprotegidos y no acordes, mantener la protección actualizada, configurar y fiscalizar políticas de protección y monitorear el 'status' de la seguridad, 24/7, desde una única consola centralizada que realmente se puede extender a toda la empresa.

Reduzca el riesgo de los sistemas desprotegidos y no acordes

La reducción de debilidades que se puedan atacar debe ser una de las principales prioridades de todos los equipos de seguridad. Un único sistema desconocido que no cuente con la protección administrada adecuada representa una considerable amenaza para toda la red — constante reinfección por amenazas conocidas, la introducción de nuevas vulnerabilidades, blancos potenciales de amenazas, o puntos de propagación, todo esto son los síntomas y los riesgos de tener sistemas desprotegidos. Por lo tanto, el conocimiento de todos los sistemas que se conectan a la red es esencial para la protección exitosa de la empresa.

El problema de los sistemas desprotegidos se agrava aún más debido a que, en la mayoría de las redes, el único requisito de entrada es el acceso físico. Contratistas, empleados terceros, visitantes de salas de conferencia, o simplemente sistemas olvidados, todos tienen la misma oportunidad de conectarse a la red corporativa y representar, aun cuando sea sin intención, una amenaza considerable a la integridad y a la disponibilidad de la red.

ePO 3.5 tiene un exclusivo abordaje de reducción de los riesgos de sistemas desprotegidos y no conformes. Utilizando sensores distribuidos, ePO 3.5 monitorea pasivamente la red en busca de cualquier conexión de LAN, determinando rápidamente si ePO 3.5 las está administrando y reaccionando, según diversas políticas, a sistemas desprotegidos que no están administrados por ePO 3.5. A través de la identificación ágil de los sistemas no administrados, los administradores pueden mejorar considerablemente los niveles de conformidad de seguridad, de los sistemas y reducir la debilidad que representan los sistemas desprotegidos y no acordes.

Monitoree la seguridad del sistema 24/7

Los servicios integrados de notificación y los informes gráficos del ePO 3.5 brindan la visibilidad continua necesaria para un monitoreo eficaz de la seguridad del sistema, a la evaluación del 'status' de su política y al descubrimiento de las debilidades de su red.

Información instantánea y preventiva es fundamental para un profesional de seguridad, especialmente en el monitoreo de conformidad y de actividad de las amenazas. ePO 3.5 cuenta con alertas y notificación integrados respecto a la conformidad, la actividad de amenazas y los sistemas desprotegidos. Los límites, definidos por el administrador, permiten el envío de alertas críticas a personas específicas a través de *e-mail*, SMS, *pager* alfanumérico o capturas de SNMP. Los alertas avisan sobre actividades de amenazas, niveles de conformidad del antivirus y detección de sistemas desprotegidos.

Además, encontrar sistemas no-acordes, rastrear un brote hasta su fuente, o determinar la eficacia de las políticas de seguridad no requieren ningún esfuerzo, con la amplia gama de más de 40 informes predefinidos del ePO 3.5. Desde resúmenes ejecutivos de seguridad en una página hasta información detallada sobre la política antivirus y la actividad de virus, sobre la política de Desktop *firewall*, las vulnerabilidades del sistema y las políticas anti-spam y de filtrado de contenido, toda la información está en sus manos. La personalización de los informes según sus necesidades específicas también es muy fácil. Los administradores pueden elegir entre varios tipos de gráficos imprimibles y exportables, incluso gráficos tridimensionales de barra, "torta", de línea y tablas. ePO 3.5 se integra con la tecnología Crystal Reports de Business Objects® y al servidor Microsoft® MSDE/SQL para equilibrar sencillez y riqueza de recursos, atendiendo a las necesidades de empresas de cualquier tamaño.

Fiscalice la conformidad de la protección y las actualizaciones

Uno de los aspectos más difíciles de la administración preventiva de una política de seguridad es mantener todos los sistemas con las protecciones más recientes. ePO 3.5 asegura la conformidad de toda la empresa a través de la fiscalización automática de las políticas, impidiendo que los sistemas dejen de ser conformes y que los usuarios finales cambien configuraciones o desactiven protecciones esenciales.

ePO 3.5 es fundamental para la administración eficaz del proceso de actualización. Los administradores pueden programar las actualizaciones para que sean realizadas a intervalos regulares, y se puede establecer por sistema o por grupo, además de otros métodos definidos por el administrador. Utiliza un diseño inteligente de repositorios distribuidos que libera totalmente el servidor de la responsabilidad de las actualizaciones, distribuyendo las actualizaciones por toda la red, manteniendo el tráfico de la red en niveles bajos y la velocidad en niveles altos. Además, es amplio, capaz de distribuir actualizaciones de todos los DAT, *engines*, todos los DAT, *engines*, *service packs*, *hotfixes* y parches de McAfee

Evalúe preventivamente la actualización de los parches de Microsoft

Con ePO 3.5, tomar medidas preventivas para la reducción de las vulnerabilidades del sistema y medir la eficacia de la distribución de sus parches son tareas sencillas y directas. System Compliance Profiler (SCP) es un componente que acompaña ePO 3.5, y permite que los profesionales de seguridad evalúen rápidamente la conformidad de los sistemas de toda la empresa, incluso la presencia de parches de seguridad esenciales de Microsoft. El establecimiento de perfiles está basado en reglas, las cuales el administrador puede personalizar, en modelos descargados desde McAfee, investigando un archivo, un servicio, una clave de registro o una referencia a un cierto parche de Microsoft. La *toma de huellas digitales* de Microsoft (que utiliza códigos de *hash* MD5) también está disponible para asegurar la absoluta integridad de los parches de seguridad de Microsoft y para impedir la falsificación de los parches. El administrador establece la criticidad de la conformidad, que se puede monitorear fácilmente bajo la forma de informes gráficos detallados de conformidad.

Reaccione rápidamente a brotes

Para reaccionar con eficacia a los brotes, ePO 3.5 es fundamental, brindando a los administradores los medios para adecuar una reacción a una amenaza específica. En emergencias donde usted necesita actualización inmediata en todas sus máquinas, el servidor puede exigir que todos los agentes *actualicen ya* y aplicar la alteración en toda la red. Por otro lado, el brote puede exigir que se altere la política en el *firewall* del sistema, tanto como exigir sólo una actualización de política en el *gateway*. Con ePO 3.5, su reacción será inmediata y centrada en la tarea.

La Actualización Global Expresa garantiza una actualización rápida en toda la empresa — hasta 50.000 sistemas en una hora a lo sumo — todos verificados con los poderosos recursos de generación de informes del ePO 3.5. La distribución por la red global asegura el uso eficaz del ancho de banda, aumentando mucho la capacidad de reaccionar ante amenazas nuevas y que surgieron recientemente.

Proteja a los usuarios móviles

Con ePO 3.5, un *empleado móvil* no necesita ser una preocupación para el equipo de seguridad. Al fiscalizar las políticas aunque la portátil no esté conectada a la red y al aplicar las actualizaciones siempre que se detecte una conexión a Internet, ePO 3.5 administra de manera eficaz su infraestructura “inadministrable”. Y como los usuarios móviles y remotos exigen más flexibilidad, ePO 3.5 les distribuye automáticamente las actualizaciones desde el repositorio más cercano y que consume menos ancho de banda, permitiendo, además, actualizaciones aplazables y reanudables. En última instancia, ePO 3.5 garantiza que sus usuarios remotos y móviles estén tan bien protegidos y sean tan fáciles de administrar como los que se conectan a través de la red local.

Facilidad de administración de toda la empresa

ePO 3.5 fue diseñado teniendo en cuenta la flexibilidad para la empresa, administrando hasta 250.000 usuarios por servidor, y se lo puede operar fácilmente en cualquier lugar, a través de una consola remota, ahorrando a su empresa los costos de más hardware y administración. Las políticas que cubren todos los niveles de protección contra amenazas — desde la frecuencia de actualizaciones hasta las configuraciones del *firewall* personal, la evaluación de parches, los tipos de archivos que se deben someter al *scan*, las configuraciones de *scan* heurístico — pueden ser definidas centralmente por máquina o por grupo, y son totalmente personalizables por el administrador. Todas son fiscalizadas automáticamente para garantizar una protección sólida.

¿Necesita administrar la protección en más de un idioma? ¡Sin problemas! ¿Quiere administrar los productos antivirus que ya posee así como las actuales aplicaciones de seguridad? ¡Es fácil! ¿Necesita que administradores distintos administren partes distintas de su red? ¡Hecho! ¿Posee servidores de archivos Windows®, Linux y NetWare? ¡Tranquilo! ¿Quiere la integración con Microsoft Active Directory? ¡Sin problemas! ¿Quiere incluir *firewalls* de sistema y prevención de intrusiones? ¡Sencillo! ePO 3.5 cuida de todo esto con facilidad.

Integración con inversiones esenciales en infraestructura

Por haber sido diseñado teniendo en cuenta la eficacia administrativa, ePO 3.5 se concentra en el aprovechamiento de las inversiones esenciales en Microsoft Active Directory (AD), asegurando la simplicidad del control de modificaciones y la uniformidad de directorios en toda la empresa. La integración con Microsoft AD permite la importación programada de sistemas desde AD al directorio del ePO 3.5, además de permitir, si procede, reflejar las agrupaciones del AD en el directorio del ePO 3.5.

Reduzca los costos de operación e infraestructura

ePO 3.5 le ayuda a consolidar sus proveedores de seguridad, se integra con su infraestructura de red y seguridad y reduce los costos de operación y capital, a través de un abordaje único y centralizado de administración de la seguridad de sistemas.

Dos preguntas importantes

En la lucha contra los códigos malintencionados, hay muchas preguntas que usted puede hacer, pero sólo dos son importantes. La primera: *¿Estamos protegidos?* La segunda: *¿Estamos infectados?* ePO 3.5 puede contestar ambas — asegurando que su protección esté lista, con la verificación y exhibición de sus puntos de conexión.

Requisitos del sistema

Para obtener información sobre los requisitos del sistema, consulte la *data sheet* de Requisitos del Sistema.

Los productos de McAfee® denotan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee 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 cada uno de nuestros clientes. McAfee Research, líder mundial en investigación de sistemas de información y seguridad, sigue en la vanguardia de la innovación en el desarrollo y refinamiento de todas nuestras tecnologías.

McAfee, ePolicy Orchestrator, ePO, 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 usado para identificar la seguridad es un rasgo distintivo 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 dueños. © 2004 Network Associates Technology, Inc. Todos los derechos están reservados.

1-sps-e35-001-0704