

McAfee ePolicy Orchestrator 3.5

Gestione de Forma Centralizada la Seguridad de sus Sistemas

Los sistemas en red requieren una constante vigilancia contra amenazas y ataques maliciosos: éstos están siempre ahí, poniendo a prueba las defensas en busca de puntos débiles. Esto convierte el trabajo del administrador en un delicado ejercicio de equilibrio. Por una parte están las exigencias de la empresa: gestionar una cantidad cada vez mayor de dispositivos y responder a las necesidades de un número creciente de usuarios móviles. Por otra parte están las necesidades de seguridad: mantener actualizados los sistemas y gestionar los múltiples niveles de protección y herramientas necesarias para responder a las amenazas de hoy en día, en constante evolución.

Es esencial contar con una visibilidad completa de la seguridad de su sistema, así como con la aplicación efectiva de las soluciones ya instaladas. A la larga, cada una de estas exigencias son constantes y de igual importancia. Si una de ellas se tambalea, su universo empresarial puede verse completamente desequilibrado.

ePolicy Orchestrator® 3.5 (ePO™) de McAfee® es la solución de gestión de la seguridad de sistemas líder del sector, que proporciona una defensa coordinada y proactiva de la empresa frente a ataques y a amenazas maliciosas. Como eje central de las soluciones McAfee para la Protección de Sistemas, los administradores pueden reducir el riesgo de los sistemas no autorizados y que no cumplen las normativas, mantener actualizada la protección, configurar y cumplir las políticas de protección, y controlar el estado de la seguridad, 24/7, desde una consola centralizada, verdaderamente escalable en la empresa.

Reducir el Riesgo de los Sistemas no Autorizados y que no Cumplen las Normativas

Reducir los puntos débiles que pueden ser objeto de ataque debe ser una prioridad esencial para todos los equipos de seguridad. Un sistema único y desconocido, que no disponga de una protección debidamente gestionada, representa una amenaza significativa para toda la red: constante reinfección por amenazas conocidas, aparición de nuevas vulnerabilidades, objetivos potenciales de ataque o puntos de propagación, he aquí los síntomas y riesgos de estos sistemas no autorizados. Por consiguiente, el conocimiento de todos los sistemas conectados a la red es crítico para proteger con éxito a la empresa.

El problema de los sistemas no autorizados se complica aún más por el hecho de que en la mayoría de las redes, el único requisito de entrada es el acceso físico. Contratistas, colaboradores externos, asistentes a conferencias o simplemente sistemas olvidados tienen todos ellos la misma posibilidad

de conectarse a la red corporativa y representan una amenaza involuntaria para la integridad y la disponibilidad de la misma.

ePO 3.5 adopta un acercamiento único para reducir el riesgo de los sistemas no autorizados y que no cumplen las normativas. Utilizando sensores distribuidos, ePO 3.5 monitoriza la red de forma pasiva para controlar todas las conexiones basadas en LAN, determinando rápidamente si están siendo gestionadas en la actualidad por ePO 3.5 y proporcionando una serie de respuestas basadas en políticas a los sistemas no autorizados que no están gestionados por ePO 3.5. Al identificar con toda rapidez los sistemas no gestionados, los administradores pueden mejorar de forma significativa el cumplimiento de las políticas de seguridad por parte de los sistemas, así como reducir la debilidad derivada de los sistemas no autorizados y que no cumplen las normativas.

Monitorización de la Seguridad del Sistema 24/7

Los servicios integrados de notificación y de informes gráficos de ePO 3.5 proporcionan la visibilidad necesaria 24/7 para vigilar eficazmente la seguridad del sistema, evaluar el estado de sus políticas y encontrar los puntos débiles de su red.

La información instantánea y proactiva es esencial para un profesional de la seguridad, especialmente cuando supervisa el cumplimiento de las normativas y las amenazas que acechan al sistema. ePO 3.5 presta un servicio integrado de alertas y notificación sobre el cumplimiento de las normas, las amenazas y los sistemas no autorizados. Unos umbrales que define el propio administrador permiten enviar alertas críticas a determinadas personas vía correo electrónico, mensajes SMS, textos en buscaperonas o interrupciones SNMP de programa. Las alertas se ocupan de vigilar las amenazas, los niveles de cumplimiento con políticas antivirus y los sistemas no autorizados.

Además, identificar los sistemas que no cumplen las normativas, rastrear una infección hasta su origen o determinar la eficacia de las políticas de seguridad no requiere esfuerzo alguno con la amplia selección de informes predefinidos (más de cuarenta) de ePO 3.5. Desde resúmenes ejecutivos de una sola página hasta datos detallados sobre políticas y actividades antivirus, política de firewalls en ordenadores personales, vulnerabilidades del sistema, antispam y políticas de filtrado de contenidos: toda la información está al alcance de la mano. La personalización de los informes para adaptarlos a sus necesidades específicas es igual de sencillo. Los administradores pueden elegir entre diversos tipos de gráficos imprimibles y exportables, que incluyen diagramas de barras tridimensionales, diagramas circulares, lineales y

tablas. ePO 3.5 está integrado con la tecnología Business Objects® Crystal Reports y con el servidor Microsoft® MSDE/SQL para conseguir un equilibrio entre sencillez y potencia que se adapte a empresas de cualquier tamaño.

Aplicación del Cumplimiento y las Actualizaciones de las Políticas de Protección

Uno de los aspectos más difíciles de gestionar de forma proactiva una política de seguridad es conseguir que todos los sistemas cumplan con la protección más avanzada. ePO 3.5 garantiza dicho cumplimiento en toda la empresa mediante la aplicación automática de la política de seguridad, que evita que los sistemas dejen de cumplir las normas e impide que los usuarios finales cambien configuraciones o desactiven protecciones esenciales.

ePO 3.5 es un factor clave para gestionar eficazmente el proceso de actualización. Los administradores pueden programar las actualizaciones a intervalos determinados, y pueden establecerlas por sistema, por grupos o por otro método de su elección. Utiliza un diseño inteligente de puntos de actualización distribuidos que libera al servidor de toda la carga de este proceso y reparte la actualización por toda la red, en la que mantiene un bajo nivel de tráfico y un alto rendimiento. Además se caracteriza por su exhaustividad, con la capacidad de instalar actualizaciones para todos los archivos DAT, procesadores, paquetes de servicios, *hotfixes* o soluciones de emergencia y parches de McAfee.

Evaluación Proactiva del Cumplimiento de los Parches de Microsoft

La adopción de medidas proactivas para reducir las vulnerabilidades del sistema y la medición de la eficacia de la instalación de los parches de su empresa son tareas sencillas y sin complicaciones con ePO 3.5. El System Compliance Profiler (SCP) es un componente integral de ePO 3.5 que permite a los profesionales de la seguridad evaluar rápidamente el cumplimiento de las normas por parte del sistema en toda la empresa, incluida la presencia de parches vitales de seguridad de Microsoft. El establecimiento de perfiles se basa en reglas personalizadas por el administrador o en plantillas descargadas de McAfee, para buscar un archivo, servicio, clave de registro o referencia concreta de parche de Microsoft. Para garantizar la absoluta integridad de los parches de seguridad de Microsoft y evitar el falseamiento de los mismos hay también *firmas digitales* disponibles (utilizando códigos de encriptación MD5). El administrador establece la importancia del cumplimiento, que se vigila fácilmente mediante informes gráficos detallados.

Respuesta Rápida a los Brotes Infecciosos

Si desea dar una respuesta eficaz a los brotes infecciosos, ePO 3.5 es fundamental para proporcionar a los administradores los medios de elaborar una respuesta personalizada y específica a la amenaza. En emergencias en las que es necesario que todas las máquinas se actualicen

inmediatamente, el servidor puede pedir que todos los agentes se actualicen en el momento, extendiendo este cambio a toda la red. También es posible que la infección requiera cambios en la política del firewall del sistema, o que sólo se necesite una actualización o un cambio de política en el gateway. Con ePO 3.5, su respuesta será inmediata y se centrará con precisión milimétrica en la tarea en curso.

Express Global Updating garantiza una rápida actualización de la empresa (hasta 50.000 sistemas en una hora o menos), todos ellos verificados en el potente sistema de informes de ePO 3.5. La distribución por toda la red garantiza la eficiencia del ancho de banda y aumenta en gran medida la capacidad de respuesta ante nuevas amenazas que vayan apareciendo.

Protección de Usuarios Móviles

Con ePO 3.5, la expresión *empleado móvil* no tiene por qué ser temible para el equipo de seguridad. Al aplicarse la política aun cuando el portátil no está conectado a la red y efectuarse la actualización en cuanto se detecta una conexión a Internet, ePO 3.5 administra con eficacia la infraestructura, por *inadministrable* que ésta sea. Y, puesto que los usuarios móviles y remotos demandan mayor flexibilidad, ePO 3.5 les proporciona automáticamente actualizaciones desde el punto más cercano y más económico en términos de ancho de banda, además de permitirles aplazar y reanudar la actualización. Por último, ePO 3.5 garantiza que sus usuarios lejanos y móviles estén tan bien protegidos y tan fácilmente administrados como los que están conectados por medio de LAN.

La Gestión en Todo el Ámbito de la Empresa se Convierte en una Tarea Fácil

ePO 3.5 ha sido diseñado pensando en la escalabilidad en la empresa: gestiona hasta 250.000 usuarios por servidor y funciona fácilmente desde cualquier sitio mediante una consola remota, ahorrando a la empresa los costes de equipos y gestión adicionales. Las políticas que se ocupan de los distintos niveles de protección contra amenazas malintencionadas—desde la frecuencia de actualización hasta las configuraciones de firewall personales, la evaluación de parches, los tipos de archivos que deben explorarse o las configuraciones de análisis heurístico—pueden establecerse de forma centralizada por equipo o por grupo, y son totalmente personalizables por parte del administrador. Todas ellas se aplican automáticamente para garantizar una protección sólida.

¿Necesita administrar la protección en más de un idioma? No hay ningún problema. ¿Desea gestionar productos antivirus instalados con anterioridad, además de las actuales aplicaciones de seguridad? Es fácil. ¿Necesita que diferentes administradores gestionen partes distintas de su red? ¡Eso está hecho! ¿Tiene servidores de archivos Windows®, Linux y NetWare? No se preocupe. ¿Desea integración con

Microsoft Active Directory? Tampoco hay problema. ¿Quiere añadir firewalls de sistema y prevención de intrusiones? No puede ser más fácil. ePO 3.5 se ocupa de todas estas cuestiones con facilidad.

Integración con Inversiones Clave en Infraestructura

Diseñada pensando en la eficiencia de administración, la solución ePO 3.5 se centra en el aprovechamiento de las inversiones clave en Microsoft Active Directory (AD), garantizando un control de cambios más fácil y la coherencia de los directorios en toda la empresa. La integración con Microsoft AD permite la importación programada de sistemas desde AD al directorio de ePO 3.5 y también, cuando proceda, ofrece la posibilidad de hacer una réplica idéntica de los grupos AD en el directorio de ePO 3.5.

Menores Costes Operativos y de Infraestructura

ePO 3.5 le ayudará en la consolidación de sus proveedores de seguridad, en integración con su red e infraestructura de seguridad y en la reducción de las inversiones de capital y los costes operativos mediante un enfoque único y centralizado de la gestión de la seguridad del sistema.

Dos Preguntas Importantes

En la lucha contra los programas malintencionados, hay muchas preguntas que cabe hacerse, aunque sólo dos, en realidad, son importantes. La primera: ¿estamos protegidos? La segunda: ¿estamos infectados? McAfee ePO 3.5 puede responder a ambas: garantizando que la protección está activa mediante la verificación y visualización de sus puntos débiles.

Requisitos del Sistema

Si desea información acerca de los requisitos del sistema, consulte la hoja de datos de Requisitos del Sistema.

McAfee PrimeSupport

McAfee ha seguido una estrategia que consiste en ofrecer la mejor tecnología para cada tipo de aplicación de gestión del rendimiento y la seguridad; ahora bien, la estrategia Protection-in-Depth™ va más allá de la instalación y aplicación de las mejores soluciones actuales. La prevención es sin duda nuestra prioridad principal, pero es inevitable que tenga usted que reaccionar ante un problema.

El programa PrimeSupport® de McAfee es fundamental para aprovechar al máximo su inversión en las soluciones de protección de redes y sistemas de McAfee. El equipo PrimeSupport de McAfee cuenta con todos los recursos adecuados y puede ofrecerle en todo momento la solución de servicio que necesita. Entre los recursos de PrimeSupport se encuentran: autorización para acceder a todas las nuevas versiones de mantenimiento y actualizaciones de producto disponibles; acceso a una serie completa de funciones adicionales de autoasistencia on line; asistencia telefónica en vivo accesible las 24 horas del día, los 7 días de la semana y los 365 días del año; disponibilidad de directores de cuenta asignados para prestar asistencia, y toda una serie de soluciones de asistencia para el software y el hardware que pueden adaptarse a sus necesidades.