

McAfee ePolicy Orchestrator

Consiga, visualice, comparta información sobre seguridad y actúe de forma centralizada

La administración de la seguridad implica complicadas combinaciones entre herramientas y datos. Esto ofrece una ventaja al adversario ya que le da más tiempo para aprovechar los vacíos no detectados entre herramientas y hacer daño. Además, el equipo de ciberseguridad es limitado y necesita ser facultado para hacer frente a la complejidad de la ciberseguridad. La plataforma de McAfee® ePolicy Orchestrator® (McAfee ePO™) elimina esfuerzos que llevan tiempo y que pueden dar lugar a errores humanos y estimula a los responsables para administrar la seguridad de forma más rápida y con mayor eficacia.

Seguridad fundamental

Empiece por lo básico. El núcleo de toda arquitectura de seguridad es la capacidad de supervisar y controlar el estado de los endpoints y sistemas. Estándares del sector, como los controles de seguridad y privacidad del Center for Internet Security (CIS) Controls y el National Institute of Standards Technology (NIST) SP 800-53 lo consideran imperativo. La consola de McAfee ePO le permite conseguir visibilidad crítica y definir y aplicar automáticamente directivas para garantizar un adecuado estado de seguridad en toda su empresa. La administración y aplicación de directivas en todos los productos de seguridad del conjunto de la empresa se lleva a cabo desde una única consola, lo que elimina la complejidad de administrar varios productos. Esta seguridad esencial es fundamental para conseguir el cumplimiento relativo a la seguridad de TI.

Administración de la seguridad avanzada demostrada

Más de 30 000 empresas y organizaciones confían en la consola de McAfee ePO para administrar la seguridad, simplificar y automatizar los procesos de cumplimiento de directivas y aumentar la visibilidad general de los endpoints, la red y las operaciones de seguridad. Las grandes empresas confían en la arquitectura escalable de la consola de McAfee ePO, que les permite administrar cientos e incluso de nodos desde una única consola. La consola de McAfee ePO pone a disposición de los administradores de seguridad de las grandes empresas la oportunidad de simplificar el mantenimiento de directivas, incorporar inteligencia sobre amenazas de terceros que aprovecha el uso de Data Exchange Layer (DXL), e integrar directivas de manera bidireccional con una amplia gama de productos. Estas mejoras en

Síguenos



FICHA TÉCNICA

la eficiencia operativa reducen el exceso de procesos y datos compartidos, facilitando una respuesta más rápida y más precisa.

Eficacia frente a dispersión

Un **estudio de ESG** demuestra que el 40 % de las empresas utiliza entre 10 y 25 herramientas, mientras que el 30 % utiliza entre 26 y 50, para administrar miles de millones de amenazas y dispositivos. Esta diversidad de uso de productos genera complejidad y multiplica las ventajas que ofrece de un modelo de administración unificada, desde la instalación hasta la generación de informes. McAfee cubre estos requisitos gracias a un enfoque de la seguridad del tipo "La unión hace la fuerza" (Together is power), que le permite consolidar esta dispersión protegiendo al mismo tiempo la totalidad de sus activos, favoreciendo la inteligencia sobre amenazas, gestionando los datos de código abierto e integrando productos de terceros. McAfee proporciona un centro de mando y control del cumplimiento de directivas y de administración de todos los productos de seguridad. Puede cambiar rápidamente de productos para encontrar los datos críticos y aplicar la directiva necesaria. La consola de McAfee ePO también le permite invertir en tecnologías de próxima generación e integrarlas con los activos existentes dentro de una única plataforma.

Ejemplos de productos gestionados por McAfee ePO

Productos de McAfee	Productos de terceros
McAfee Endpoint Protection Prevención de amenazas, firewall, control de la Web	Guidance Software: enCase Enterprise
McAfee Drive Encryption	Avecto: Privilege Guard
McAfee File and Removable Media Protection	AccessData: AccesData Enterprise
McAfee Active Response	Autonomic Software: Power Manager, Patch Manager
McAfee Management for Optimized Virtual Environments (McAfee MOVE)	Xerox MFP
McAfee Data Loss Prevention (McAfee DLP)	DXL
McAfee Policy Auditor	
McAfee Enterprise Security Manager	
McAfee Threat Intelligence Exchange	
McAfee Application Control	
McAfee Cloud Workload Security	
McAfee Advanced Threat Defense	
McAfee Content Security Reporter	
McAfee Database Activity Monitoring	

FICHA TÉCNICA

Ejemplos de casos prácticos: Cómo centraliza la consola de McAfee ePO la administración de los productos de seguridad

Producto y tecnología	Caso práctico de administración centralizada	Ventaja
McAfee ePO McAfee Endpoint Security	McAfee Endpoint Security detecta un archivo malicioso conocido en un endpoint. La consola de McAfee ePO define una directiva estricta en el endpoint para ponerlo en cuarentena. Esto se realiza en una interfaz de administración común.	Contención rápida de un endpoint no conforme
McAfee ePO McAfee DLP McAfee Enterprise Security Manager	McAfee Enterprise Security Manager detecta una importante filtración de datos en un endpoint y lo etiqueta en la consola de McAfee ePO. La consola de McAfee ePO aplica directivas de protección contra la pérdida de datos para bloquear los datos y advertir al usuario de que el endpoint no cumple la directiva.	Aplicación automática de la directiva contra la pérdida de datos

Ejemplos de integración

Producto y tecnología	Caso práctico de integración	Ventaja
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Security marca un host sospechoso. La consola de McAfee ePO puede activar análisis adicionales. Esta situación se comunica a Cisco ISE a través de PxGrid y el intercambio de DXL (la consola de McAfee ePO). Cisco ISE puede aislar el host hasta que se considere aceptable.	Mayor protección proactiva
Avecto Defendpoint McAfee ePO DXL McAfee Threat Intelligence Exchange	Despliegue y gestione la solución de administración de privilegios líder del sector, Avecto Defendpoint, desde McAfee ePO. Los cambios en la configuración de Avecto Defendpoint se basan en los datos de reputación de aplicaciones de McAfee Threat Intelligence Exchange.	Reducción de la complejidad Sin necesidad de infraestructura adicional, lo que reduce el coste total de propiedad Cambios en el acceso con privilegios basado en inteligencia sobre amenazas
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO comparte la lista de activos con Nexpose. Esto le permite conocer el estado de riesgo desde su consola de McAfee ePO y le permite definir la directiva en consecuencia. Se comparten datos de vulnerabilidades con la comunidad DXL de proveedores.	Reducción de la complejidad Consigue una visión completa y fiable y prioriza las acciones para minimizar riesgos desde un solo panel
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	Esta integración facilita el intercambio de inteligencia bidireccional y en tiempo real entre la red y los endpoints. Los eventos se comparten con la comunidad DXL.	Disminución del tiempo de detección Bloqueo y corrección de amenazas

FICHA TÉCNICA

Las empresas que disponen de plataformas integradas están mejor protegidas para conseguir tiempos de respuesta más rápidos que las que no disponen de este tipo de plataformas.

	Organizaciones integradas	Organizaciones no integradas
Sufrieron menos de cinco ataques el año pasado	78 %	55 %
Detectaron las amenazas en ocho horas	80 %	54 %

2016 Penn Schoen Berland

Los flujos de trabajo ampliables simplifican los procesos

La base de datos de McAfee ofrece funciones de administración flexibles y automatizadas que le permiten identificar, gestionar y responder rápidamente a las vulnerabilidades, cambios en los estados de seguridad y amenazas conocidas desde una sola consola. Como usuario, define la forma en la que la consola de McAfee ePO debe dirigir las alertas y las respuestas de seguridad en función del tipo y gravedad de los eventos de seguridad para su entorno y de sus directivas y herramientas. Para facilitar las operaciones de desarrollo y de seguridad, la plataforma McAfee ePO le permite crear flujos de trabajo automatizados entre sus sistemas de operaciones de seguridad y de TI para corregir rápidamente los problemas. Utilice la consola de McAfee ePO para activar las acciones de corrección de sus sistemas de operaciones de TI, como asignar directivas más estrictas. Utilizar sus interfaces web de programación de aplicaciones (API) reduce el esfuerzo manual.

Casos prácticos comunes

- Ahorre tiempo y elimine esfuerzos laboriosos innecesarios mediante la planificación de informes de cumplimiento de directivas para satisfacer las necesidades de todas las partes interesadas.
- Integre fácilmente la consola de McAfee ePO en sus procesos y funciones empresariales actuales aprovechando su sólido conjunto de interfaces API para conseguir más información y acelerar los flujos de trabajo (por ejemplo, con la integración con sistemas de fichas, aplicaciones web o portales de autoservicio).
- Mantenga su postura de seguridad mediante el despliegue de soluciones de agentes y de seguridad a medida que se incorporan nuevas máquinas a su red corporativa. Para ello sincronice la consola de McAfee ePO con Active Directory.

"La plataforma de administración de endpoints más potente disponible actualmente, McAfee ePolicy Orchestrator, es la herramienta de administración básica para todos los productos de seguridad de la empresa, y ofrece el poder y la flexibilidad que las grandes empresas desean. Las funciones de seguridad se integran de manera generalizada y sólida a través de un motor de directivas común y un flujo inteligente".

—Forrester Wave: Endpoint Security Suites (Suites de seguridad de endpoints) 2016

FICHA TÉCNICA

Rápida mitigación y corrección

La plataforma McAfee ePO dispone de funciones integradas avanzadas para aumentar la eficacia del personal de las operaciones de seguridad en su esfuerzo por mitigar una amenaza o realizar un cambio para restaurar el cumplimiento. La respuesta automática de McAfee ePO puede activar una acción en función de un evento que se haya producido. Las acciones pueden ser simples notificaciones o correcciones aprobadas.

Casos prácticos para respuesta automática

- Notificar a los administradores las nuevas amenazas, errores de actualización o errores de alta prioridad a través del correo electrónico o SMS en función de umbrales predeterminados.
- Aplicar directivas basadas en acciones de clientes o amenazas; por ejemplo, para impedir comunicaciones externas cuando un host pueda estar comprometido (esto denegaría actividades de mando y control) o bloquear la filtración de datos/transferencias salientes hasta que el administrador restablezca la directiva.
- Etiquetar sistemas y ejecutar otras tareas de corrección, como análisis de memoria bajo demanda cuando se detectan amenazas.
- Activar ejecutables registrados para ejecutar secuencias de comandos y scripts externos, como generar una ficha en el servicio de asistencia o integrar en otros procesos empresariales.
- Automatizar la puesta en cuarentena del endpoint con directivas más restrictivas.



Figura 1. Administración centralizada de la seguridad mediante la consola de McAfee ePO.

Proteja toda su organización con la consola de McAfee ePO

Administración centralizada de la seguridad

- Una consola única diferenciada para disponer de una administración y visibilidad centralizadas hasta de cientos de miles de nodos en toda la empresa.
- Plataforma abierta para una completa administración de la seguridad de sistemas protegida por McAfee y soluciones de terceros.
- Plataforma ampliable que se integra en su infraestructura de TI existente y la aprovecha para reducir el impacto operativo.

Aceleración de los tiempos de respuesta con confianza

- Vista e información completa para abordar de manera proactiva problemas de seguridad internos y externos.
- Rápido despliegue centralizado de las actualizaciones y definiciones de seguridad para garantizar la protección de los endpoints frente a las últimas amenazas.
- Tiempos de respuesta acelerados a través de paneles procesables y funciones de consultas e informes avanzadas.

Reducción de la complejidad y simplificación de los procesos

- Capacidad para comenzar rápidamente gracias a una configuración guiada, flujos de trabajo de administración de directivas automatizados y paneles predefinidos.
- Asignación de directivas basada en etiquetas para aplicar de forma precisa los perfiles de seguridad definidos a grupos de sistemas o sistemas individuales en función de sus papeles en la empresa o su estado de riesgo.
- El catálogo de tareas y las funciones de administración automatizadas racionalizan los procesos administrativos y reducen la carga de trabajo.
- Agente único para administrar varios productos para endpoints, lo que reduce el riesgo de conflictos de endpoints.

Adaptabilidad a despliegues en grandes empresas

- Arquitectura de nivel empresarial, capaz de administrar cientos de miles de dispositivos desde un solo servidor.
- Compatible y demostrada con entornos de TI complejos y heterogéneos.
- Generación de informes de nivel empresarial que agrupa una vista completa de su estado de seguridad y cumplimiento.

"El software McAfee ePO destaca frente a otras soluciones. Se trata de una plataforma única para nuestra protección para endpoints. Puedo ver todo lo que necesito de todos nuestros productos de McAfee desde una sola consola. Sus paneles fáciles de utilizar y funciones integradas lo hacen todo —visibilidad, generación de informes, despliegue, actualización, mantenimiento, toma de decisiones— mucho más fácil."

—Christopher Sacharok, Ingeniero de seguridad de la información, Computer Sciences Corporation



Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es

McAfee y el logotipo de McAfee, ePolicy Orchestrator y McAfee ePO son marcas comerciales o marcas comerciales registradas de McAfee, LLC o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros.
Copyright © 2017 McAfee, LLC. 3718_0118
ENERO DE 2018