McAfee ePolicy Orchestrator

Inspirando y facultando al profesional de la seguridad

La administración de la seguridad implica complicadas combinaciones entre varias herramientas y una gran cantidad de datos. Esto ofrece una ventaja al adversario ya que le da más tiempo para aprovechar las deficiencias no detectadas entre herramientas, por lo que pueden hacer más daño. El equipo de ciberseguridad es limitado y necesita ser facultado para orquestar de forma sencilla entornos de ciberseguridad complejos.

Su empresa necesita responder rápidamente a las amenazas en cualquier tipo de dispositivos a fin de minimizar el daño, y el equipo directivo exige que se demuestre la eficacia de la seguridad. La plataforma de administración McAfee® ePolicy Orchestrator® (McAfee ePO™) —disponible in situ y desde la nube (con dos modelos: SaaS o IaaS)— ayuda a eliminar el esfuerzo y el tiempo dedicados a la administración de la seguridad, limita las posibilidades de cometer errores y ayuda a los responsables a responder más rápido y con más eficacia.

Seguridad fundamental

Empecemos por lo imprescindible. El núcleo de toda arquitectura de seguridad es la capacidad de supervisar y controlar el estado de los dispositivos y sistemas. Estándares del sector, como los controles y parámetros de seguridad y privacidad de los documentos CIS Controls y CIS Benchmarks y de la publicación especial 800-53 del NIST reivindican la necesidad de supervisar y controlar las infraestructuras de seguridad como requisito imperativo. La consola de McAfee ePO le permite conseguir visibilidad crítica, así como definir y aplicar automáticamente directivas para garantizar un adecuado estado de seguridad en toda su empresa. Elimina la complejidad de orquestar varios productos con administración e implementación de directivas para toda la empresa desde una sola consola. Esta función de administración de la seguridad esencial es fundamental para conseguir el cumplimiento relativo a la seguridad de TI.

Principales ventajas

- Administración centralizada aclamada por el sector con un panel único de visibilidad integrado que simplifica enormemente las tareas —disponible desde la nube o in situ.
- Flujos de trabajo automatizados para optimizar las tareas administrativas y conseguir una mayor eficacia.
- Plataforma abierta y completa que integra McAfee y más de 150 soluciones de terceros para ofrecer respuestas más rápidas y precisas.
- Administración común de la seguridad para el mayor número de dispositivos del mercado.
- Aprovecha y mejora los controles nativos integrados en los sistemas operativos, como Windows Defender.
- Ampliable a cientos de miles de dispositivos, con cobertura del dispositivo a la nube.

Síganos

Administración avanzada y demostrada de la seguridad, con total simplicidad

Más de 36 000 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 dispositivos, la redes y las operaciones de seguridad. Las grandes empresas confían en la arquitectura escalable de la consola de McAfee ePO, que les permite administrar cientos de miles de nodos desde una única consola. Este panel le ayuda a priorizar las tareas y le ofrece un resumen, en una vista gráfica, de su estado de seguridad en toda su topografía digital con un nuevo espacio de trabajo de protección. Además, hay una página Recursos de seguridad donde encontrará lo último en información e investigaciones sobre amenazas.

Los administradores pueden acceder a eventos específicos para obtener información más detallada. Esta vista de resumen reduce el tiempo necesario para crear y racionalizar los datos disponibles, y elimina la posibilidad de que se produzcan errores, incluso si fuera necesaria la intervención manual. 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), nuestra estructura de mensajería líder del sector, e integrar directivas de manera bidireccional con una amplia gama de productos. Estas mejoras en la eficiencia operativa reducen el exceso de procesos y datos compartidos, facilitando una respuesta más rápida y más precisa.

El objetivo del centro de soporte es facilitar el acceso a la información sobre los productos de McAfee y proporcionar una visión del estado del servidor de ePO en los entornos del cliente. Está disponible para ePO in situ y para ePO en AWS. Puede recibir soporte y notificaciones de productos de forma proactiva, buscar en repositorios de contenido de McAfee y acceder a recursos sobre mejores prácticas y procedimientos, desde la consola de ePO. Además, puede gestionar su infraestructura de ePO evaluando fácilmente su estado y recibiendo sugerencias sobre las medidas que deben tomarse para mejorarlo en caso necesario.

Eficacia de una plataforma abierta frente a la 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 aumenta la complejidad y multiplica las ventajas que ofrece un modelo de administración unificada, desde la instalación hasta la generación de informes. Más de la mitad de las empresas calculan que se consigue más de un 20 % de mejora gracias a la integración de herramientas de seguridad (Estudio de MSI, 2018). McAfee cubre estos requisitos gracias a una estrategia de administración de la seguridad de plataforma abierta 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 control del cumplimiento de directivas y de la administración de una amplia gama de productos de

Los analistas del sector afirman que el software McAfee ePO es la razón por la que los clientes eligen y permanecen con McAfee.

Ventajas de una plataforma integrada
Las empresas que disponen de plataformas integradas están mejor protegidas y consiguen tiempos de respuesta más rápidos que las que no disponen de este tipo de plataformas.

Empresas con plataformas integradas
- El 78 % sufrieron menos de cinco ataques el año pasado.
- El 80 % detectaron las amenazas en ocho horas.

Las empresas sin plataformas integradas
- Solo el 55 % sufrieron menos de cinco ataques el año pasado.
- Solo el 54 % detectaron las amenazas en ocho horas.

Fuente: 2016 Penn Schoen Berland

seguridad. Los analistas pueden 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.

Nuestra plataforma abierta ofrece una serie de enfoques de integración (scripting, API, sin API, y con el mínimo esfuerzo gracias a la estructura de mensajería DXL de código abierto), lo que le permite elegir el que mejor se ajuste a sus necesidades sin intensas personalizaciones ni servicios. A través del programa McAfee® Security Innovation Alliance, impulsamos el desarrollo de productos de seguridad interoperables, simplificamos la integración de esos productos en los entornos complejos de los clientes y ofrecemos un ecosistema de seguridad realmente integrado y conectado para maximizar el valor de las inversiones realizadas por los clientes. El programa McAfee Security Innovation Alliance cuenta con más de 150 integraciones con partners.

Además, la estructura de comunicación de Data Exchange Layer (DXL) conecta y optimiza las acciones de seguridad de productos de varios proveedores, así como de las soluciones de código abierto desarrolladas internamente. Gracias a la integración de Cisco pxGrid y DXL puede acceder a todos los datos de otras 50 tecnologías de seguridad. McAfee ePO es un componente fundamental para administrar nuestra robusta plataforma abierta.

Seguridad de los dispositivos ampliada con administración de las herramientas nativas

La plataforma ampliable de McAfee ePO administra una gran cantidad de dispositivos, incluidos los que tienen controles nativos. McAfee mejora y administra conjuntamente la seguridad ya integrada en Microsoft Windows 10 para ofrecer una protección optimizada, permitiendo a las empresas aprovechar la funciones nativas de los sistemas Microsoft. El software McAfee ePO administra McAfee® MVISION Endpoint, que combina funciones avanzadas de aprendizaje automático especialmente ajustadas para la seguridad nativa de los sistemas operativos Microsoft, y evita además la complejidad y el coste de una consola de administración adicional. Proporciona una experiencia de administración común con directivas compartidas para los dispositivos Microsoft Windows 10 y todos los dispositivos de la empresa para garantizar la coherencia y la simplicidad.

Coherencia a través de flujos de trabajo automatizados

El software McAfee ePO 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.
En 2018 y por encargado de McAfee, un estudio de MSI descubrió que las empresas esperan poder ahorrar aproximadamente un 25 % de tiempo al día mediante la automatización de tareas repetitivas. Con el software McAfee ePO, puede desplegar e implementar fácilmente las directivas de seguridad desde una consola única con tan solo realizar unos pasos lógicos. El panel

Ahorro de tiempo

Un reciente estudio de MSI de 2018 señala que los clientes piensan que ahorrarán hasta un 20 % de tiempo si sus herramientas de seguridad están integradas.

El valor de la integración

- Aumenta la eficacia de herramientas y procesos: 61 %
- Reduce la complejidad y los esfuerzos manuales, lo que permite a los profesionales de la seguridad centrarse en tareas que requieren atención crítica: 61 %
- Mejora la visibilidad al mostrar los datos en patrones y contexto: 58 %
- Optimiza los flujos de trabajo para una respuesta más rápida: 57 %

Fuente: Estudio de MSI, 2018

centralizado ofrece el contexto adecuado a medida que ejecuta las tareas y ve cada paso y su relación con otros. Esto elimina la complejidad y la posibilidad de que se produzcan errores. Puede definir la forma en 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. Sus interfaces web de programación de aplicaciones (API) reducen el esfuerzo manual. Tiene la opción de solicitar un proceso de aprobación antes de que se distribuya una directiva o tarea nueva o actualizada, lo que reduce el riesgo de errores y garantiza el control de calidad.

Ejemplos de uso comunes

- Ahorre tiempo y elimine tareas laboriosas y redundantes mediante la planificación de informes de cumplimiento de directivas de seguridad adaptados a 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, se integra con sistemas de fichas, aplicaciones web o portales de autoservicio.
- Mantenga su estado de seguridad mediante el despliegue de soluciones de seguridad con agentes o aprendizaje automático a medida que se incorporan nuevos dispositivos a su red corporativa. Para ello sincronice la consola de McAfee ePO con Microsoft Active Directory.

Rápida mitigación y corrección

La plataforma McAfee ePO dispone de funciones avanzadas integradas 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 de directivas. 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.

Ejemplos de uso 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.

"McAfee ePO es uno de los antepasados de la automatización y la organización integrada de la seguridad. ...los profesionales de la seguridad actuales necesitan las ventajas del ePO tradicional, pero a través de una experiencia simplificada, de manera que sean eficientes Y TAMBIÉN eficaces... como espacio de trabajo SaaS, MVISION combina análisis, administración de directivas y eventos de una forma adecuada para las medianas y grandes empresas".

—Frank Dickinson, Vicepresidente de investigación, Productos de seguridad, IDC

- 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.
- Poner en cuarentena la carga de trabajo o contenedor (cualquier dispositivo) con directivas más restrictivas.

Administración de la seguridad basada en la nube

Las empresas necesitan simplificar y acelerar el despliegue de soluciones de amenazas avanzadas. Muchas ven el valor de la administración de la seguridad basada en la nube al eliminar el coste y el mantenimiento de una infraestructura in situ. El software McAfee ePO se puede implementar en la nube desde cualquier lugar y en cualquier momento a través de dos opciones de despliegue: el software McAfee ePO en Amazon Web Services (AWS) o McAfee MVISION ePO. En ambos casos la implementación dura menos de una hora.

- El software McAfee ePO en AWS permite a las empresas aprovechar muchos servicios de AWS nativos, como el escalado automático y Amazon RDS, lo que elimina la necesidad de adquirir y administrar una base de datos distinta. De esta forma los administradores pueden centrarse en las tareas de seguridad críticas, no de la infraestructura. El software McAfee ePO en AWS gestiona McAfee® Endpoint Security, McAfee® Data Loss Prevention, McAfee® Cloud Workload Security, Data Exchange Layer y soluciones de terceros integradas en el software McAfee ePO.
- McAfee® MVISION ePO aprovecha las ventajas de la oferta de McAfee ePO como software como servicio (SaaS). Esto simplifica enormemente la administración de la plataforma y le permite ocuparse de otras tares de seguridad críticas. Las actualizaciones de la plataforma son transparentes, con un modelo de distribución continua. La seguridad de los dispositivos se despliega automáticamente en toda la empresa una vez desplegado su agente, lo que elimina tareas manuales para instalar o actualizar la seguridad para cada dispositivo, garantizando así una implementación reforzada contras las amenazas. Esto permite administrar McAfee MVISION Endpoint y Data Exchange Layer desde una única consola y desde cualquier lugar. McAfee MVISION ePO permite que sus dispositivos proporcionen información crítica a su solución de administración de información y eventos de seguridad (SIEM), lo que garantiza que esa información esté a disposición de sus analistas para mejorar las tareas de caza y corrección de amenazas.

"El software McAfee ePO destaca frente a otras soluciones. Se trata de una plataforma integral para la protección de nuestros 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

FICHA TÉCNICA

Productos de McAfee gestionados por McAfee ePO

Productos de McAfee*
McAfee® Endpoint Protection (Prevención de amenazas, firewall, control de la Web)
McAfee MVISION Endpoint complementa Windows Defender con protección contra amenazas avanzadas
McAfee® MVISION Mobile
McAfee® Drive Encryption
McAfee® File and Removable Media Protection
McAfee® Active Response
McAfee® Management for Optimized Virtual Environments (McAfee MOVE)
McAfee Data Loss Prevention (McAfee DLP)
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
Data Exchange Layer (DXL)

**Para McAfee ePO in situ*

Despliegues flexibles

Despliegue	Ventaja principal
McAfee ePO in situ	Control total de los datos y del conjunto de funciones
McAfee ePO en AWS	Elimina la necesidad de mantenimiento de hardware que requiere una solución in situ
McAfee MVISION ePO (software como servicio ePO)*	Oferta SaaS multiinquilino para eliminar todo el mantenimiento de la infraestructura y las ampliaciones

**No todas las funciones de ePO están disponibles en McAfee MVISION ePO*

Ejemplos de uso: Cómo hace posible la consola McAfee ePO la administración centralizada de la seguridad

Producto y tecnología	**Ejemplo de uso**	**Ventaja**
McAfee MVISION ePO McAfee MVISION Endpoint Microsoft Windows 10	El software McAfee MVISION ePO gestiona McAfee MVISION Endpoint, que mejora los controles nativos de Microsoft Windows 10 con protección avanzada. Puede descubrir y gestionar las amenazas avanzadas con una plataforma de administración común y directivas coherentes para Microsoft Windows y McAfee Endpoint Security.	Mejor protección para los controles nativos de Microsoft Windows y administración de eficacia demostrada
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 los endpoints infectados
McAfee ePO McAfee Data Loss Prevention 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 (mediante la consola de McAfee ePO). Cisco ISE puede aislar el host hasta que se considere aceptable.	Mayor protección proactiva
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 permite priorizar las acciones a fin de minimizar riesgos, todo 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 también se comparten con la comunidad DXL. El software blade Check Point Anti-Bot bloquea el tráfico de mando y control y alerta al software McAfee ePO y a otras soluciones de seguridad de terceros integradas sobre temas DXL comunes. Con esta información, inicia automáticamente un flujo de trabajo de corrección apropiado para los endpoints. Check Point y McAfee también detectan e impiden ataques de tipo zero-day y los convierten en ataques conocidos, independientemente de si proceden de la red o del endpoint. Gracias al intercambio de inteligencia crítica en tiempo real, la integración permite a nuestros respectivos productos detectar, bloquear corregir las amenazas de manera automatizada.	▪ Disminución del tiempo de detección ▪ Bloqueo y corrección de amenazas

McAfee
Together is power.

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