RESUMEN DE LA SOLUCIÓN

Un planteamiento más sencillo de la seguridad de los endpoints

Desarrollo de una defensa unificada para proteger todos los endpoints, desde el dispositivo a la nube

La ciberseguridad se encuentra en una calle sin salida: mientras siguen aumentando el número, el nivel de sofisticación y el impacto económico de las fugas de datos, cada vez hay menos analistas experimentados disponibles.

Ahora hay una forma de resolver los complejos problemas de seguridad a los que se enfrenta su empresa haciendo más en menos tiempo y con menos recursos. La cartera de soluciones de protección para endpoints de McAfee® emplea el análisis y el aprendizaje automático para lograr una eficacia líder del sector y además ofrece la flexibilidad de conectar nuestras soluciones a productos de más de 150 proveedores. Trabajando por unificar la protección de datos y las defensas contra amenazas desde el dispositivo hasta la nube, estamos creando un futuro en el que la seguridad es un sistema integrado, un sistema más sencillo, inteligente y amplio que cualquiera de sus predecesores.

Principales ventajas

- Defienda sus endpoints con prevención de exploits, firewall, control de la Web y aprendizaje automático.
- Proteja los dispositivos iOS y Android frente al phishing, los ataques de tipo zero-day y las pérdidas de datos en tiempo real, incluso offline.
- Detecte, investigue y responda a las amenazas de forma eficiente, todo ello simplificado con investigaciones guiadas por inteligencia artificial.
- Añada a las funciones de seguridad básicas del sistema operativo el aprendizaje automático, la protección frente al robo de credenciales y la reversión del sistema.
- Simplifique y acelere la eficiencia de la protección, gracias al uso de un panel centralizado para su administración.
- Elija la administración basada en SaaS con MVISION ePO o la administración in situ con McAfee® ePO™.

Síganos

Con el aumento del número, el tipo y la complejidad de los endpoints, las empresas se encuentran en una encrucijada. ¿Deben seguir confiando únicamente en las soluciones antivirus tradicionales, sabiendo que al hacerlo quedan expuestas a las amenazas modernas, como el ransomware y las redes de bots? ¿O es mejor amalgamar productos de varios proveedores para crear una "solución" que les ofrezca una mejor protección contra amenazas, pero también ralentice los procesos, reduzca el desempeño de las máquinas y genere un considerable tiempo de inactividad? Por suerte, con la cartera de protección para endpoints de McAfee, las empresas ya no tienen que elegir entre protección contra amenazas y agilidad operativa.

McAfee Endpoint Security

Administración centralizada, análisis compartido

Esta plataforma de administración centralizada para la protección de los endpoints utiliza un solo agente para varias tecnologías, como protección contra amenazas, firewall, control de la Web, prevención adaptable contra amenazas y muchas otras, todas diseñadas para simplificar entornos complejos.

A diferencia del software antivirus tradicional, McAfee Endpoint Security aprovecha las conexiones entre los endpoints locales y McAfee® Global Threat Intelligence en la nube para detectar amenazas de tipo zero-day casi en tiempo real. En cuanto se identifica una amenaza en un lugar, puede detectarse en cualquier otro sitio. La combinación de información y análisis compartido con funciones avanzadas de protección frente a exploits permite a McAfee Endpoint Security lograr un 25 % más de protección que McAfee® VirusScan® Enterprise frente a las amenazas de tipo zero-day. En pruebas independientes, McAfee Endpoint Security alcanzó en total un índice de eficacia del 99,98 % sin falsos positivos.

Mantenimiento automatizado, corrección eficiente

Con McAfee Endpoint Security, puede aprovechar las funciones ampliadas de automatización y aprendizaje automático. La clasificación de comportamientos a través del aprendizaje automático detecta las amenazas zero-day casi en tiempo real y genera información procesable sobre ellas. Además, va evolucionando automáticamente a lo largo del tiempo, para identificar nuevos comportamientos y añadir reglas con el fin de reconocer ataques futuros.

Durante un ataque, los administradores pueden ver rápidamente dónde se está produciendo la infección y cuánto tiempo estuvieron expuestos los endpoints, lo que les permite comprender la amenaza y reaccionar con mayor prontitud. La función Real Protect puede devolver los endpoints afectados al último estado correcto conocido para prevenir inmediatamente la infección y reducir la carga del administrador. La Contención dinámica de aplicaciones le defiende del ransomware y el greyware porque le permite proteger el "paciente cero".

La combinación de la plataforma McAfee ePO con McAfee Endpoint Security ofrece más visibilidad, favorece la productividad de TI, simplifica las operaciones, unifica la seguridad y reduce los costos. Estas y otras mejoras de eficiencia han permitido a los equipos de ciberseguridad que migraron a McAfee Endpoint Security ahorrar hasta 40 horas de administración a la semana.

Principales ventajas de McAfee Endpoint Security

- Detecta las amenazas de tipo zero-day casi en tiempo real.
- Actualiza continuamente el motor antimalware.
- Permite la comunicación entre diferentes soluciones antivirus, prevención de exploits, firewall y control de la Web.
- Devuelve el endpoint al último estado correcto conocido.
- Contiene las aplicaciones y los procesos maliciosos en los endpoints incluso cuando están offline.
- Prioriza las alertas según la "reproducción" de eventos del ataque.
- Integra la caza y la respuesta ante incidentes en una función fácil de usar.
- Facilita la respuesta ante incidentes hasta reducirla a un solo clic.

También se preserva la productividad de los empleados: los análisis solo demoran unos segundos, se producen únicamente cuando el dispositivo está inactivo y se reanudan imperceptiblemente tras un reinicio o cierre. Y lo mejor de todo es que McAfee Endpoint Security es ligero y no necesita conexión a la nube, con lo que los usuarios están protegidos incluso offline.

McAfee MVISION EDR

Un departamento típico de TI administra miles de endpoints, desde computadoras de escritorio y servidores hasta celulares, relojes inteligentes y dispositivos IoT. Las soluciones EDR actuales vuelcan demasiada información sobre unos equipos de seguridad que ya están al límite de su capacidad y que dependen de analistas veteranos para investigar las amenazas. Esta estrategia ha demostrado ser poco eficiente y adaptable, especialmente cuando se le suman las limitaciones actuales de ancho de banda y la escasez de expertos.

MVISION EDR empieza donde acaban las tecnologías antivirus y las soluciones EDR tradicionales. Esta solución integrada de seguridad para endpoints permite administrar un gran volumen de alertas al supervisar los endpoints, recopilar los datos de actividad que pueden indicar una amenaza y proporcionar la visibilidad y el contexto necesarios. Mediante el análisis de los datos que identifican patrones de amenazas, las funciones automatizadas de análisis y respuesta por IA pueden eliminar o contener las amenazas automáticamente e informar al personal de seguridad, mientras que las herramientas de análisis forense investigan las amenazas identificadas y buscan actividades sospechosas.

Mejore su seguridad con la investigación guiada por inteligencia artificial (IA)

Tradicionalmente, las soluciones EDR "hacen posible" la investigación proporcionando datos sin procesar, contexto y otras funciones de búsqueda, pero siguen necesitando la intervención de analistas competentes para realizar la investigación y el análisis. Sin embargo, MVISION EDR guía la investigación, lo que reduce la experiencia y el esfuerzo necesarios para realizar investigaciones. También permite que los analistas determinen el nivel de riesgo del incidente y su causa principal con más rapidez.

La investigación guiada por IA reúne y procesa automáticamente enormes cantidades de datos de fuentes diferentes y averigua la fuente, el objetivo y el patrón del ataque. A continuación, tal como haría cualquier analista veterano para guiar con sus preguntas a uno más inexperto, plantea automáticamente una o varias hipótesis sobre alertas y reúne, resume y presenta las pruebas de varias fuentes a medida que avanzan las investigaciones. Basándose en estas pruebas, MVISION EDR utiliza las hipótesis para formular y buscar respuestas a preguntas pertinentes que dirijan la investigación, mientras los analistas trabajan para decidir si continúan planteando preguntas y recopilando datos, retiran el problema o lo elevan a instancias superiores.

Todo ello les permite aumentar su nivel de experiencia y ganar competencia para administrar un gran volumen de alertas, lo que reduce el tiempo que se tarda en iniciar una investigación y mejora su exactitud. Como hasta los analistas noveles son capaces de analizar amenazas, los más veteranos pueden dedicar sus conocimientos a la caza y a agilizar el tiempo de respuesta.

Principales ventajas de McAfee MVISION EDR

- Detección de amenazas procesable de alta calidad sin datos irrelevantes.
- Análisis más rápido para armar una defensa más resistente.
- Investigaciones guiadas mediante inteligencia artificial, que proporciona información del ataque generada automáticamente.
- Capacidad para maximizar los resultados de los equipos actuales.
- Solución en la nube que requiere muy poco mantenimiento.
- Administración de la seguridad con una sola consola aclamada por el sector: MVISION ePO (basado en SaaS) o McAfee ePO (in situ o basado en IaaS).
- Dedicación de los analistas a la respuesta estratégica ante el incidente sin las complicadas cargas administrativas.

A más rapidez de identificación, más agilidad de respuesta

Los analistas también pueden utilizar las potentes funciones de búsqueda y de recopilación continua de datos para ampliar las pesquisas y examinar en profundidad todos los sistemas. MVISION EDR captura una instantánea de los procesos activos, las conexiones de red, los servicios y las entradas de ejecución automática de un endpoint para permitir su inspección inmediata, búsquedas en tiempo real y búsquedas históricas. Estos datos también se transmiten a la nube, lo que permite que se adopten rápidamente nuevos motores y técnicas de análisis, mientras que se cotejan los resultados de la detección basada en el comportamiento con el marco MITRE ATTACK, con el fin de obtener un proceso más coherente para determinar la fase y el riesgo de una amenaza y priorizar la respuesta.

Las funciones de investigación e información de MVISION EDR se amplían aún más mediante la integración con soluciones de administración de información y eventos de seguridad (SIEM), como McAfee® Enterprise Security Manager o productos de terceros. Esto permite la correlación de artefactos de endpoints con información de red y otros datos recopilados por el sistema SIEM.

McAfee MVISION Endpoint

MVISION Endpoint ofrece funciones mejoradas de detección y corrección a los clientes que desean reforzar la protección de sus endpoints. Diseñado específicamente para aumentar las defensas nativas del sistema operativo (SO), amplía el firewall antivirus y la prevención contra exploits nativa de los entornos Windows 10 y Server 2016 y 2019 al detectar las amenazas sofisticadas que Microsoft Defender pasa por alto.

Una estrategia para endpoints más inteligente

A diferencia de otras alternativas que se limitan a una sola forma de análisis basado en el aprendizaje automático, MVISION Endpoint puede realizar análisis del malware estático, conductual y sin archivos, para reforzar la protección contra amenazas y reducir los falsos positivos. Utiliza el aprendizaje automático basado en el comportamiento para identificar las amenazas por su conducta real y aísla los archivos que comparten características con otros archivos de malware. También incluye funciones avanzadas de reversión, lo que permite devolver un sistema afectado por ransomware a su último estado correcto conocido.

Protección basada en la nube con una sola consola

Y lo mejor de todo es que MVISION Endpoint proporciona una experiencia de administración unificada. En lugar de duplicar la administración de directivas, permite administrar de forma centralizada el antivirus de Windows Defender, Exploit Guard, la configuración de Windows Firewall y las directivas de McAfee. Al desplegar McAfee MVISION Endpoint junto con McAfee ePO o MVISION ePO, se obtiene una protección verdaderamente integrada con un solo panel. McAfee ePO y MVISION ePO también ofrecen funciones de integración con terceros, lo que aporta contramedidas adicionales a la consola para reforzar y personalizar aún más su seguridad.

Principales ventajas de McAfee MVISION Endpoint

- Administración centralizada para Windows 10 y Windows Server 2016 y 2019.
- Defensas avanzadas, con y sin archivos, y con aprendizaje automático basado en el comportamiento.
- Menor costo total de propiedad y racionalización de flujos de trabajo.
- Protección frente al robo de credenciales y reversión del sistema.
- Administración de las tecnologías de defensa de McAfee y Microsoft con una sola consola y una directiva única.

Principales ventajas de McAfee MVISION Mobile

- Ofrece protección en el dispositivo y en tiempo real.
- Detecta las amenazas contra dispositivos móviles y protege contra ataques de tipo zero-day.

Este agente, extremadamente ligero, es más rápido, sencillo y robusto que las herramientas de seguridad tradicionales. Las actualizaciones se suministran automáticamente al cliente, por lo que nunca tendrá que preocuparse de mantenerse al día, y, al tener dispositivos de menor tamaño y menos preocupaciones de desempeño, el impacto sobre el usuario sigue siendo mínimo para respetar su productividad.

McAfee MVISION Mobile

McAfee MVISION Mobile detecta las amenazas y las vulnerabilidades en dispositivos Apple iOS o Android, las redes a las que se conectan y las aplicaciones que descargan los usuarios. Su integración con nuestra plataforma insignia de administración centralizada, el software McAfee ePO, le permite administrar dispositivos móviles de la misma forma que cualquier otro endpoint. Como componente integrado en McAfee® Device Security, MVISION Mobile amplía la visibilidad y el control de sus activos móviles utilizando la misma consola centralizada que administra todos sus demás dispositivos gestionados por McAfee.

Más inteligente, más vigilante

A diferencia de las soluciones de seguridad para dispositivos móviles basadas en la nube que dependen del uso de entornos aislados para las aplicaciones o la tunelización del tráfico, MVISION Mobile se instala directamente en los dispositivos móviles para proporcionar protección continua contra amenazas sea cual sea el modo de conexión del dispositivo: a la red corporativa, a través de un punto de acceso público o una operadora de telefonía móvil, o incluso si está desconectado.

MVISION Mobile utiliza algoritmos de aprendizaje automático con información de miles de millones de puntos de datos procedentes de millones de dispositivos con el fin de identificar las amenazas y los ataques en curso o inminentes. Estos algoritmos analizan las desviaciones en el comportamiento del dispositivo y llegan a conclusiones sobre los indicadores de peligro para identificar con precisión los ataques avanzados contra dispositivos, aplicaciones y la red, incluidos los que nunca se habían visto antes. La inteligencia integral de las aplicaciones mitiga los riesgos para la seguridad y la privacidad, lo que reduce las posibilidades de pérdida de datos. Y las notificaciones de protección de la red, diseñadas para permitirle a usted y a sus empleados saber si el dispositivo se va a conectar a una red poco segura o peligrosa, se centran en detener los ataques antes de que comiencen.

McAfee MVISION ePO

McAfee MVISION ePO, una solución aclamada por el sector, está diseñada para administrar las soluciones de McAfee y mejorar los controles de seguridad nativos de los sistemas operativos. Esta versión SaaS global multiinquilino para empresas de McAfee ePO, un software único de eficiencia demostrada, le permite administrar la seguridad, definir y aplicar automáticamente directivas, simplificar y automatizar procesos de cumplimiento de normativas y aumentar la visibilidad. Ofrece escalabilidad a cientos de miles de dispositivos, incluidos los que tienen controles nativos, con cobertura desde el dispositivo hasta la nube, y todo ello sin la complejidad de mantener una arquitectura in situ.

- Destaca los riesgos para la privacidad con el fin de informar a los usuarios de los peligros asociados con cada aplicación.
- Agiliza la respuesta con información práctica sobre las amenazas contra dispositivos móviles aplicable en toda la empresa.
- Permite a los empleados trabajar en cualquier lugar, en cualquier momento y con cualquier dispositivo gracias a los controles de cumplimiento de normativas.
- Detecta enlaces peligrosos en mensajes de texto, aplicaciones de redes sociales y mensajes de correo electrónico mediante la protección contra phishing.
- Se integra en soluciones empresariales de administración de la movilidad (EMM), pero también funciona con dispositivos personales (BYOD).
- Permite a los equipos de respuesta ante incidentes aprovechar los datos forenses de amenazas para analizarlos y tomar medidas destinadas a prevenir que un dispositivo comprometido pueda generar un brote.

Seguridad... y además simplicidad

La plataforma ampliable MVISION ePO proporciona una experiencia de administración común con directivas compartidas para todos los dispositivos en toda la empresa, incluidos los dispositivos Microsoft Windows 10, para garantizar la coherencia y la simplicidad. MVISION ePO ofrece visibilidad con un panel único, lo que le permite eliminar la complejidad de coordinar múltiples productos. Con funciones de administración dinámicas y automatizadas, los usuarios pueden identificar, administrar y responder rápidamente a las vulnerabilidades, los cambios en el estado de seguridad y las amenazas conocidas... desde cualquier lugar y a través de su navegador. Sobre esa base, es posible desplegar y aplicar las directivas de seguridad en toda la empresa en unos cuantos pasos.

El espacio de trabajo de protección ofrece, en una sola vista gráfica, un resumen de su estado de seguridad en toda su topografía digital, lo que permite a los administradores priorizar los riesgos y acceder a eventos específicos para obtener información más detallada. Esta vista de resumen reduce el tiempo necesario para crear informes y racionalizar los datos disponibles, y elimina la posibilidad de que se produzcan errores si es necesaria la intervención manual. Al aunar la administración de riesgos y el análisis de incidentes, permite que sus dispositivos proporcionen información crítica a su solución SIEM, lo que garantiza que esa información esté a disposición de sus analistas para mejorar las tareas de caza y corrección de amenazas.

Mayor eficiencia

Según el Magic Quadrant de Gartner en la categoría de protección para endpoints, el software McAfee ePO es la razón por la que muchas organizaciones compran soluciones de McAfee y son fieles a la empresa. Y ahora que esta tecnología de eficiencia probada está disponible en formato SaaS, las empresas pueden beneficiarse aún más al permitir que sus profesionales de seguridad se centren exclusivamente en supervisar y controlar todos los dispositivos. Además de eliminar la configuración y el mantenimiento que exige una infraestructura de seguridad in situ, MVISION ePO también automatiza el despliegue de la seguridad de los dispositivos en toda la empresa y proporciona actualizaciones continuas y transparentes, lo que ofrece estabilidad y ahorra tiempo. Y, con funciones avanzadas para aumentar la eficiencia del personal de operaciones de seguridad en su esfuerzo por mitigar una amenaza o realizar un cambio para restaurar el cumplimiento de directivas, se puede ahorrar todavía más tiempo.

Para comprobar que MVISION ePO es la solución adecuada para su negocio, haga clic aquí y realice una prueba gratuita.

Principales ventajas de McAfee MVISION ePO

- Administración centralizada aclamada por el sector.
- Punto de visibilidad y control único y sencillo desde cualquier lugar.
- Eliminación de la complejidad asociada al mantenimiento de las plataformas de seguridad in situ.
- Vista unificada que aúna la administración de riesgos y el análisis de incidentes.
- Plataforma completa que administra los productos de McAfee y los controles nativos de los sistemas operativos.
- Flujos de trabajo automatizados para tareas administrativas eficientes.
- Investigación/corrección de incidentes optimizadas.
- Administración común de la seguridad para el mayor número de dispositivos del mercado.
- Escalabilidad de cientos a miles de dispositivos.
- Cobertura desde el dispositivo hasta la nube.

CASOS REALES

MGM Resorts International
20 000 nodos en 20 complejos turísticos en todo el mundo

- **Desafíos:** mitigar los riesgos y bloquear los ataques de tipo zero-day; comprender los patrones de ataque complejos y garantizar un tiempo de actividad constante para las aplicaciones fundamentales; reducir los gastos de las operaciones de seguridad y mantenerse actualizados.
- **Soluciones:** McAfee® Enterprise Security Manager, McAfee® Investigator, MVISION EDR, McAfee® Web Gateway, McAfee Endpoint Security, McAfee Data Loss Prevention, DXL y McAfee® Professional Services.
- **Resultados:** redujeron el tiempo para contener, investigar y corregir las amenazas y mejoraron la competencia del equipo de operaciones de seguridad.

Atrius Health
Más de 65 000 usuarios con 9000 endpoints en más de 29 centros

- **Desafíos:** protegerse del ransomware y el phishing; reducir el tiempo para detectar y responder; mantener a la organización segura sin entorpecer su crecimiento.
- **Soluciones:** McAfee Enterprise Security Manager y McAfee Endpoint Security.
- **Resultados:** ahorro operativo; evitaron contratar a varios empleados a jornada completa; redujeron el tiempo de detección y respuesta; mejoraron la seguridad del entorno virtual.

Florida International University
55 000 estudiantes y 15 000 empleados en dos campus principales y varios campus secundarios internacionales

- **Desafíos:** dar libertad a los BYOD, pero proteger el entorno frente a las amenazas; evitar que los estudiantes introdujeran malware inadvertidamente en el entorno; mantener una visibilidad generalizada.
- **Soluciones:** McAfee Enterprise Security Manager y McAfee Endpoint Security.
- **Resultados:** lograron contener los ataques o archivos sospechosos con mayor rapidez; fortalecieron su nivel de seguridad general sin tener que aumentar la plantilla; consiguieron una protección más robusta de los endpoints con un mínimo impacto en los usuarios; facilitaron la administración y la visibilidad en toda la empresa.

Banco Delta
400 endpoints

- **Desafíos:** reducir la carga de la administración de seguridad; crear una defensa fuerte para protegerse de ataques sofisticados; planificar una estrategia de seguridad para el futuro, incluida la migración a la nube.
- **Soluciones:** plataforma McAfee ePO, McAfee Enterprise Security Manager y McAfee Endpoint Security.
- **Resultados:** redujeron de forma tangible las infecciones y los comportamientos potencialmente peligrosos de los usuarios.

Compañía de seguros de EE. UU.
6000 computadoras de escritorio y 2000 servidores en 12 centros

- **Desafíos:** proteger los datos confidenciales de los clientes; proporcionar seguridad máxima sin empeorar la experiencia de los clientes.
- **Soluciones:** McAfee Endpoint Security, McAfee Data Loss Prevention y McAfee Web Gateway.
- **Resultados:** redujeron los picos de uso de la CPU del 95 % al 30/35 % y los análisis de días a horas; ahorraron numerosas horas semanales en técnicos de ciberseguridad; incrementaron la productividad tanto de los usuarios finales como de las operaciones de seguridad; mejoraron su nivel de seguridad.

Gran banco multinacional (EMEA)
45 000 endpoints en más de 40 países y dos centros de datos

- **Desafíos:** proteger la organización del ransomware y los ataques zero-day y bloquear las amenazas causadas por el comportamiento de los usuarios; mejorar la eficiencia de la administración de seguridad.
- **Soluciones:** McAfee Endpoint Security, plataforma McAfee ePO y McAfee Web Gateway.
- **Resultados:** mejoraron la protección de los endpoints al detectar más malware y defenderse mejor frente a las amenazas de tipo zero-day; redujeron el tiempo que demoraban en conseguir protección con soluciones de seguridad integradas que comparten la información de amenazas casi en tiempo real; ahorraron tiempo operativo con una administración de seguridad más fácil y con menos incidentes.

Grandes victorias

McAfee Endpoint Security

- Medalla de plata en 2019 en los premios Cybersecurity Excellence Award, categoría de seguridad para endpoints
- Aprobado como producto empresarial en las comparativas de antivirus "AV-Comparatives"
- AV-TEST: McAfee obtuvo la puntuación de usabilidad perfecta

MVISION Endpoint

- Medalla de plata en 2019 en los premios Cybersecurity Excellence Award, categoría de seguridad para endpoints
- Premio 2018 a la innovación tecnológica en seguridad para endpoints

MVISION Mobile

- Medalla de plata en 2019 en los premios Cybersecurity Excellence Award, categoría de seguridad móvil

Presencia de McAfee Endpoint

- 622 millones de endpoints en total
- 97 millones de endpoints de empresa
- 525 millones de endpoints de particulares
- 69 000 clientes empresariales
- 7000 empleados
- 189 países
- El 80 % de las empresas del Fortune 100
- El 75 % de las empresas del Fortune 500
- El 64 % de las empresas del Global 2000
- El 87 % de los mayores bancos del mundo
- El 54 % de los 50 principales minoristas
- Más de 1550 de patentes de seguridad mundiales

"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 [McAfee] 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

McAfee
Together is power.

Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
+52-55-50890250
www.mcafee.com/mx

4329_0819
AGOSTO DE 2019