McAfee Endpoint Security

Seguridad diseñada expresamente para ofrecer administración proactiva de amenazas y controles de seguridad de eficacia probada

Seguridad para endpoints: ¿cuáles son sus prioridades?

En las empresas actuales la seguridad puede ser responsabilidad de uno o de varios equipos. En el caso de las grandes corporaciones, esta responsabilidad se comparte entre varios equipos, como administración de TI y operaciones de seguridad. Sea cual sea el carácter de la función que desempeña usted en la empresa, sus prioridades particulares le llevarán a preocuparse más por un grupo de funciones y objetivos concretos en lo que respecta a su plataforma de protección de endpoints.

La solución para endpoints que elija debe estar en línea con sus principales prioridades. Independientemente de su función, McAfee® Endpoint Security es perfecta para sus necesidades críticas concretas; desde prevenir las amenazas y detectarlas, hasta adaptar los controles de seguridad. Con las funciones de McAfee® MVISION Insights, se ofrecen prioridades de amenazas específicas en las que trabajar antes de que se produzca el ataque. La solución le permite garantizar el tiempo de actividad de los sistemas para los usuarios, encontrar más oportunidades para la automatización y simplificar flujos de trabajo complejos.

Tiempo de funcionamiento y visibilidad

McAfee Endpoint Security permite a los clientes responder y gestionar el ciclo de vida de protección frente a amenazas con defensas proactivas y herramientas de corrección. La reversión automática de los sistemas los devuelve a un momento anterior en el que estaban en buen estado, para garantizar la productividad de los usuarios y administradores, y ahorrar tiempo que se dedicaría a esperar hasta que se corrigiera el sistema, se efectuara la recuperación o se copiara una imagen de la máquina infectada. La información global sobre amenazas y la inteligencia sobre eventos locales en tiempo real se comparten entre los endpoints y McAfee® MVISION EDR para recopilar los detalles de los eventos de amenazas, detectar y prevenir amenazas que intentan evadir la detección, y se asignan al marco MITRE ATT&CK para llevar a cabo una investigación más profunda. Una consola de administración centralizada, con opciones de despliegue en entornos locales, SaaS o virtuales, facilita la administración. MVISION Insights ofrece visibilidad y control únicos de las amenazas potenciales que requieren prioridad con alta propensión a atacar, además de determinar si el estado de seguridad de una empresa será capaz de proteger contra la amenaza. Esto garantiza un nivel de protección contra una amenaza crítica y derrota al agresor antes de que ataque.

Ventajas principales

- **Defensas avanzadas para amenazas avanzadas:** el aprendizaje automático, la reversión de los sistemas y la protección frente a robo de credenciales complementan las funciones de seguridad básicas de sistemas de sobremesa y servidores de Windows.
- **Sin más complejidades:** administración de las tecnologías de McAfee, las directivas antivirus de Windows Defender, Defender Exploit Guard y la configuración de Windows Firewall, con una sola directiva y a través de una única consola.

Síganos

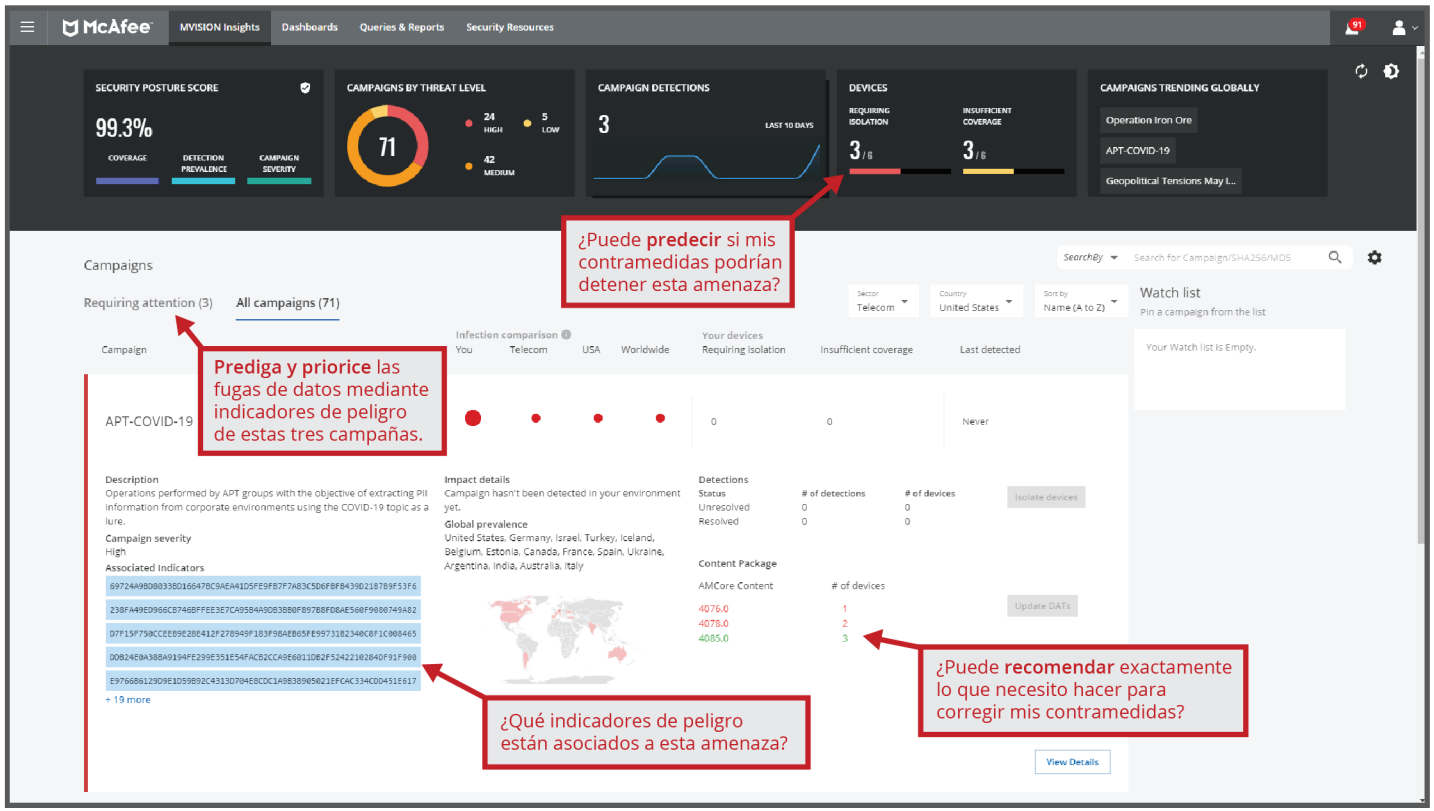

Figura 1. Panel de MVISION Insights. (MVISION Insights requiere telemetría de McAfee Endpoint Security (con autorización del usuario) para funcionar correctamente.)

Gracias a MVISION Insights, las empresas disponen de alertas y notificaciones sobre amenazas potenciales con muchas probabilidades de golpear en función del sector y la región. Además, MVISION Insights ofrece una evaluación local del nivel de seguridad y si puede proteger contra esa amenaza. También identifica los endpoints que son vulnerables a la amenaza y ofrece orientación sobre lo que hay que cambiar. Esto aumenta los esfuerzos proactivos para ir por delante de adversarios con muchas probabilidades de atacar.

McAfee Endpoint Security recopila información de amenazas a partir de varias capas de interacción, utilizando un solo agente de software para eliminar las redundancias que provoca el empleo de varios productos individuales.

Ventajas principales (continuación)

- **MVISION Insights:** responda inmediatamente a campañas activas potenciales que se priorizan en función de si atacan su sector o región con una solución de inteligencia sobre seguridad procesable disponible hoy. MVISION Insights predecirá a qué endpoints les falta protección contra las campañas y ofrecerá orientación sobre lo que hay que hacer para mejorar la detección. Se trata de la única protección de seguridad para endpoints para priorizar, predecir y recomendar medidas de forma simultánea.

El resultado es un enfoque integrado de la seguridad que elimina la correlación manual de amenazas. Los detalles de la amenaza que requieren una investigación en profundidad se trasladan automáticamente a los responsables de la respuesta a incidentes. Los datos de eventos de amenazas se presentan en un formato simple y fácil de consultar a través de Story Graph, que visualiza los detalles de la amenaza y permite a los administradores profundizar fácilmente e investigar los orígenes de los ciberdelincuentes.

Las defensas de amenazas avanzadas e integradas automatizan y agilizan la respuesta

McAfee Endpoint Security también ofrece otras defensas de amenazas avanzadas, como la contención dinámica de aplicaciones, con el fin de ayudar a las empresas a defenderse de las últimas amenazas avanzadas[1].

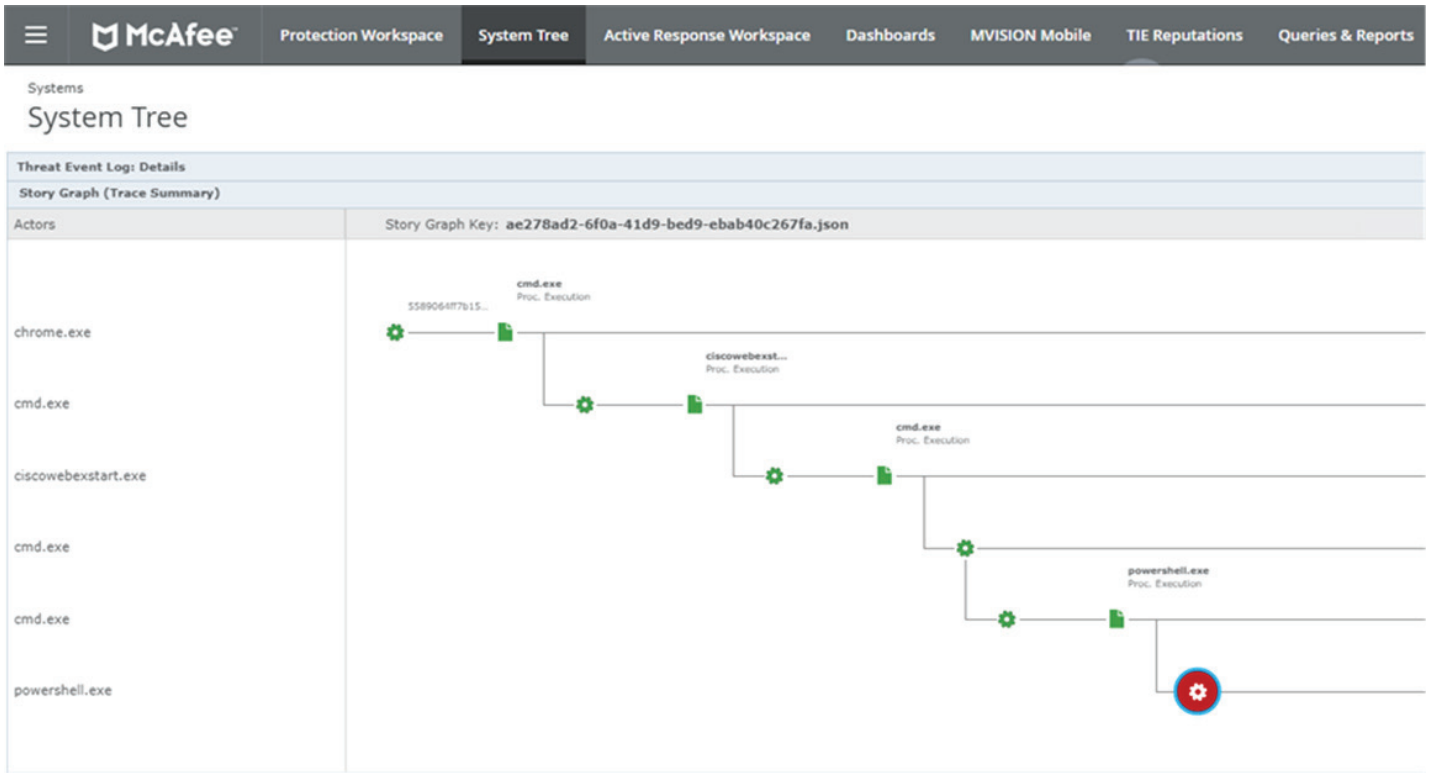

Figura 2. Story Graph.

Por ejemplo, DAC analiza y toma medidas ante el greyware y demás malware emergente, y frena estos ataques para evitar la infección.

Otra tecnología para las amenazas avanzadas es Real Protect, que emplea clasificación de comportamientos mediante aprendizaje automático para detectar malware de tipo zero-day y mejorar la detección. La clasificación sin firmas se realiza en la nube y ocupa muy poco espacio en el software cliente al tiempo que proporciona una detección casi en tiempo real. Además, se proporciona información práctica que puede utilizarse para crear indicadores de peligro (IoC) e indicadores de ataque (IoA). Esto resulta especialmente útil para la detección de desplazamiento lateral, el descubrimiento de pacientes cero, la atribución de responsabilidad de la amenaza, la investigación forense y la corrección. Además, con Real Protect los análisis futuros son más rápidos, ya que la clasificación de comportamientos evoluciona automáticamente e identifica comportamientos y añade reglas para identificar futuros ataques que son similares, utilizando tanto funciones estáticas como de tiempo de ejecución.

Por último, para impedir inmediatamente la infección y reducir el tiempo que necesitan los administradores de seguridad de TI, el cliente repara el endpoint, después de la confirmación, y lo devuelve al último estado correcto conocido.

La protección inteligente de los endpoints permite saber qué están haciendo los agresores

Con más inteligencia, mejoran los resultados. McAfee Endpoint Security comparte sus observaciones en tiempo real con las distintas tecnologías de defensa para endpoints conectadas a su plataforma, con el fin de agilizar la identificación de conductas sospechosas, favorecer la coordinación de las defensas y mejorar la protección frente a ataques selectivos y amenazas de tipo zero-day. Localiza y comparte hash de archivos, direcciones URL del origen, y eventos de AMSI y PowerShell no solo con otras defensas, sino también con la interfaz cliente y de administración, para ayudar a los usuarios a comprender los ataques y proporcionar a los administradores análisis forenses útiles de las amenazas.

Además, la tecnología de McAfee® Threat Intelligence Exchange permite que las defensas adaptables colaboren con otras soluciones de McAfee, como gateways, entornos aislados y nuestra solución de administración de información y eventos de seguridad (SIEM). Recopilar y distribuir inteligencia de seguridad local, comunitaria y mundial acorta el intervalo entre el ataque, la detección y la contención de semanas o meses a milisegundos.

Cuando se combina con McAfee® Global Threat Intelligence (McAfee® GTI), la plataforma McAfee Endpoint Security se nutre de la nube para supervisar y actuar frente a todo el espectro de amenazas nuevas y emergentes en tiempo real y en todos los vectores, es decir, archivos, Web, mensajería y redes. El sistema existente de administración y datos de endpoints mejora con la información local y mundial sobre amenazas para combatir al instante el malware desconocido y selectivo. Las medidas automáticas contra aplicaciones y procesos sospechosos aplican respuestas adaptadas rápidamente a las formas de ataque nuevas y emergentes, y, al mismo tiempo, informan a las demás defensas y a la comunidad mundial.

Los clientes que utilizan DAC y Real Protect obtienen información de amenazas más avanzadas, así como de los comportamientos que muestran. Por ejemplo, DAC proporciona información sobre las aplicaciones contenidas y el tipo de acceso que intentan conseguir, como por ejemplo, al registro o la memoria.

Para las organizaciones interesadas en obtener información acerca de las amenazas para los endpoints con el fin de detectar malware y equipar a los encargados de la respuesta a incidentes, Real Protect proporciona información de los comportamientos que se han considerado maliciosos y clasifica las amenazas. Esta información puede resultar particularmente útil para descubrir los intentos de malware basado en archivos de eludir la detección a través de técnicas como el empaquetamiento, el cifrado o el uso malintencionado de aplicaciones legítimas.

Un rendimiento sólido y eficaz ayuda a responder a tiempo

Las defensas inteligentes pierden su valor si entorpecen a los usuarios con análisis lentos, largas instalaciones o complicadas operaciones de administración. McAfee Endpoint Security protege la productividad de los usuarios con una capa común de servicios y nuestro nuevo motor antimalware que ayuda a reducir la cantidad de recursos y la potencia que necesita el sistema de un usuario. Los análisis de los endpoints no afectan a la productividad del usuario porque solo se realizan cuando el dispositivo está inactivo y se reanudan automáticamente tras el reinicio o el cierre del sistema.

El proceso de análisis adaptable también contribuye a reducir la demanda de la CPU, ya que aprende qué procesos y fuentes son de confianza, para centrar los recursos únicamente en los que parecen sospechosos o proceden de fuentes desconocidas. McAfee Endpoint Security posee un firewall integrado que utiliza McAfee GTI para proteger los endpoints frente a redes de bots, ataques distribuidos de denegación de servicio (DDoS), amenazas persistentes avanzadas y conexiones web peligrosas.

Alivie la presión con menos complejidad y más sostenibilidad

Para muchas personas, debido al rápido aumento de los productos de seguridad con funciones que se solapan y a la variedad de consolas de administración, ahora es más difícil obtener una imagen clara de los ataques potenciales. McAfee Endpoint Security ofrece una sólida protección a largo plazo, gracias a su plataforma abierta y ampliable, que actúa como base para centralizar las soluciones para endpoints actuales y futuras. Esta plataforma hace uso de Data Exchange Layer para permitir la colaboración de varias tecnologías con la inversión actual en seguridad. La arquitectura integrada encaja a la perfección con otros productos de McAfee, lo que reduce aún más las brechas de seguridad, las tecnologías aisladas y las redundancias, a la vez que mejora la productividad al recortar los costos operativos y la complejidad de administración.

McAfee® ePolicy Orchestrator® (McAfee ePO™) puede disminuir todavía más la complejidad, ya que proporciona un solo panel de visualización para supervisar, desplegar y administrar los endpoints. Las vistas personalizables y los prácticos flujos de trabajo en lenguaje comprensible brindan las herramientas necesarias para evaluar rápidamente el nivel de seguridad, localizar las infecciones y reducir el impacto de las amenazas poniendo los sistemas en cuarentena, deteniendo los procesos maliciosos o bloqueando la filtración de datos. La solución también ofrece un único punto para administrar todos los endpoints, otras funciones de McAfee y más de 130 soluciones de seguridad de otros proveedores.

FICHA TÉCNICA

Función	Por qué la necesita
Detección y respuesta a amenazas proactiva (MVISION Insights)	▪ Detecta de manera predictiva y preventiva amenazas potenciales en función de su sector y región. ▪ Evalúa locamente su nivel de seguridad contra las amenazas potenciales y ofrece orientación sobre cómo mejorarlo. ▪ Adelántese a los adversarios configurando protecciones antes de que se produzca un ataque.
Real Protect	▪ Clasificación de comportamientos a través del aprendizaje automático que detecta las amenazas zero-day casi en tiempo real y genera información procesable sobre ellas. ▪ Además, va modificando la clasificación de comportamientos para identificar comportamientos y añadir reglas con el fin de reconocer ataques futuros.
Protección para endpoints frente a ataques selectivos	▪ La protección de endpoints reduce el intervalo desde la detección hasta la contención del ataque de días a milisegundos. ▪ McAfee Threat Intelligence Exchange recopila información de múltiples fuentes, lo que permite a los componentes de seguridad comunicarse entre sí al instante cuando se producen ataques avanzados emergentes y de varias fases. ▪ El registro de eventos de AMSI y PowerShell permiten descubrir los ataques sin archivos y basados en scripts y contribuye a protegerse frente a ellos.
Análisis inteligentes y adaptables	▪ Mejoran el rendimiento y la productividad, ya que omiten el examen de los procesos de confianza y dan prioridad a los procesos y las aplicaciones sospechosos. ▪ El análisis de comportamientos adaptable adecua la supervisión, selección y alcance a la actividad sospechosa.
Reversión de los cambios	▪ Revierte automáticamente los cambios realizados por el malware, devuelve los sistemas a su último estado correcto conocido y mantiene la productividad de los usuarios.
Seguridad en la Web proactiva	▪ Seguridad web proactiva para que la navegación sea segura con protección web y filtrado para endpoints.
Contención dinámica de aplicaciones	▪ Defiende frente al ransomware y greyware, y protege al "paciente cero"[2].
Bloquea los ataques hostiles a la red	▪ El firewall integrado utiliza puntuaciones de reputación basadas en McAfee GTI para proteger los endpoints frente a redes de bots, ataques DDoS, ataques persistentes avanzados y conexiones web sospechosas. ▪ Durante el arranque del sistema la protección con firewall autoriza solamente tráfico saliente, lo que protege los endpoints cuando no están en la red corporativa.
Story Graph	▪ Los administradores ven rápidamente dónde están las infecciones, por qué se están produciendo y la duración de la exposición de manera que pueden comprender la amenaza y reaccionar con más prontitud.
Administración centralizada (plataforma McAfee ePO) con múltiples opciones de despliegue	▪ La administración verdaderamente centralizada ofrece mayor visibilidad, simplifica las operaciones, aumenta la productividad de TI, unifica la seguridad y reduce costos.
Plataforma abierta y ampliable de seguridad para endpoints	▪ La arquitectura integrada permite que las defensas para endpoints colaboren y se comuniquen entre sí para reforzar la protección. ▪ Reduce los costos operativos al eliminar redundancias y optimizar procesos. ▪ Se integra a la perfección con otros productos de McAfee y otros proveedores para reducir los intervalos de desprotección.

Tabla 1. Funciones principales y por qué las necesita.

Saque ventaja a las ciberamenazas

McAfee Endpoint Security ofrece lo que necesitan los profesionales de la seguridad actuales para contrarrestar las ventajas de los agresores: defensas inteligentes y colaborativas y un marco que simplifique los entornos complejos. Con un rendimiento sólido y eficiente, y una eficacia de detección de amenazas demostrada en pruebas de terceros, las organizaciones pueden proteger a sus usuarios, aumentar su productividad y garantizar su tranquilidad.

McAfee, líder del mercado en seguridad para endpoints, ofrece una amplia gama de soluciones que protegen en profundidad y de manera proactiva mediante la combinación de potentes defensas con una administración eficaz que permiten a los equipos de seguridad resolver más amenazas en menos tiempo y con menos recursos.

Migrar es fácil

Los entornos que utilizan versiones actuales del software McAfee ePO, McAfee VirusScan® Enterprise y McAfee® Agent pueden disfrutar de nuestra herramienta de migración automática para migrar sus directivas existentes a McAfee Endpoint Security en cuestión de 20 minutos o menos[3].

Estas son las ventajas que disfrutará también con McAfee Endpoint Security:

- Análisis que no afectan en absoluto a los usuarios para garantizar una mayor productividad.
- Datos forense más completos que se asignan al gráfico histórico (Story Graph) para ofrecer información fácil de consultar e investigaciones simplificadas para ayudarle a fortalecer sus directivas.
- Corrección que permite revertir los cambios del malware y mantener los sistemas en su estado de funcionamiento correcto.
- Información proactiva sobre amenazas potenciales con prioridad y orientación sobre cómo ajustar las contramedidas contra las amenazas con MVISION Insights.
- Menos agentes que administrar, junto con la capacidad de evitar el análisis, para reducir la introducción manual.
- Defensas colaborativas que trabajan conjuntamente para derrotar a las amenazas avanzadas.
- Marco de próxima generación preparado para incorporarlo a nuestras otras soluciones de detección y respuesta frente a amenazas avanzadas y para endpoints.

Más información

Para obtener más información sobre McAfee Endpoint Security, visítenos aquí.

Para obtener más información sobre cómo complementa McAfee Endpoint Security la cartera de productos de McAfee, visite:

- MVISION Endpoint
- Familia de productos de MVISION
- McAfee Threat Intelligence Exchange
- MVISION EDR
- McAfee ePolicy Orchestrator
- MVISION Insights

1. Disponible con la mayoría de las suites para endpoints de McAfee. Solicite los detalles a su agente comercial.
2. Ibid.
3. El tiempo de migración depende de las directivas existentes y del entorno actual.

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