McAfee Advanced Threat Defense para IPS de red

Protección más amplia contra el malware oculto

Ventajas principales

- Busca, bloquea y soluciona de forma automática el malware avanzado y los ataques ocultos en el tráfico de red.
- Añade a la seguridad web análisis de código estático verdadero y entornos aislados específicos para el objetivo, sin incrementar la carga de trabajo en el sistema de prevención de intrusiones (IPS).
- Bloquea las amenazas plug-and-play sin retrasos debidos a necesidades de intervención humana.

El sistema de prevención de intrusiones (IPS) basado en la red es uno de los pilares de las arquitecturas de seguridad de las empresas. Desplegado en banda junto al gateway y a la seguridad basada en host, el sistema IPS supervisa el tráfico de red y el comportamiento de los endpoints mediante el empleo de una serie de técnicas que permiten detectar los ataques y activar las respuestas defensivas.

Sin embargo, hoy día, cada vez más amenazas desconocidas, zero-day, consiguen evadir las defensas tradicionales. Estos sofisticados ataques, ocultos, bien camuflados, con capacidad de adaptación inteligente y con objetivos muy selectivos, constituyen una parte del panorama de las amenazas en evolución que, aunque pequeña, es desproporcionadamente peligrosa y costosa.

Como respuesta, algunas organizaciones incorporan el análisis dinámico a sus infraestructuras de IPS, normalmente mediante dispositivos de entorno aislado fuera de banda. El entorno aislado ejecuta los archivos ejecutables sospechosos en un entorno virtual seguro y supervisa en tiempo real los comportamientos con el fin de detectar intenciones maliciosas. Sin embargo, con demasiada frecuencia, esta aparente ventaja en precisión de la detección se pierde rápidamente debido a una integración deficiente y al empleo de procesos de respuesta manuales.

Por ejemplo, la mayoría de los dispositivos de entorno aislado de otros distribuidores solo pueden alertar a un analista de seguridad humano cuando se encuentra un nuevo ataque. El analista debe crear de forma manual nuevas reglas de bloqueo para el IPS y el firewall y, a continuación, comenzar la tarea de identificar y reparar los endpoints que han sufrido el ataque durante al análisis del entorno aislado fuera de banda. Entre otras limitaciones que presentan las soluciones actuales se pueden citar:

- La necesidad de contar con un dispositivo de entorno aislado por sensor de IPS, lo que infla los costes.
- La dependencia de un entorno de ejecución virtual genérico que puede pasar por alto comportamientos de ataques dirigidos a objetivos específicos.
- La dependencia del análisis dinámico en exclusiva, lo que deja al entorno aislado vulnerable ante varias estrategias de malware para detectar entornos seguros y retrasar la ejecución del comportamiento que se va a revelar.

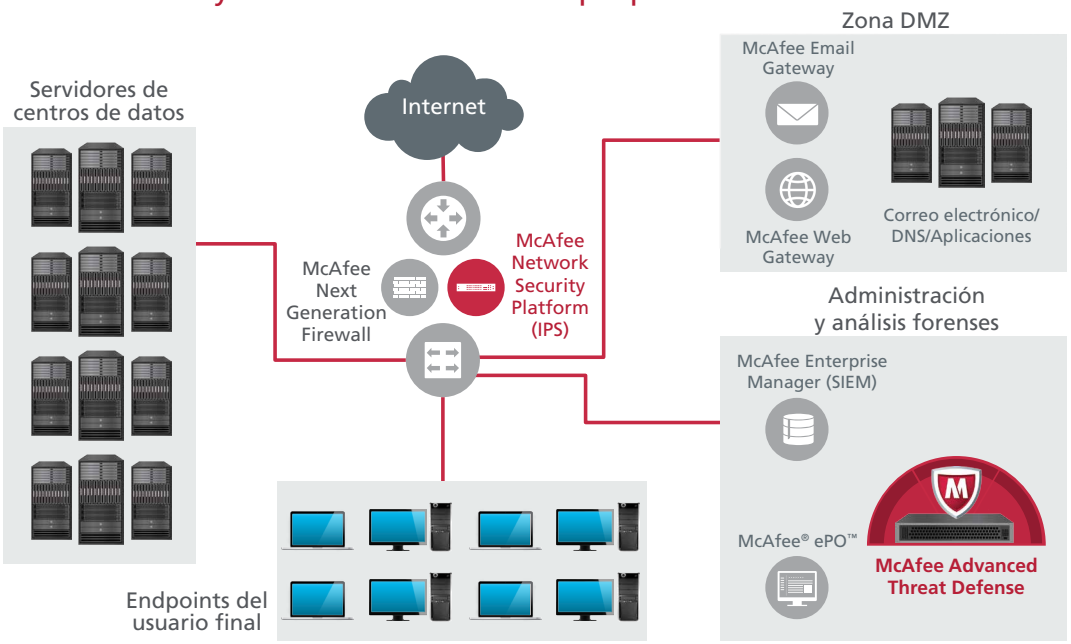
Security Connected: integración de IPS y entorno aislado

La respuesta a todas estas necesidades es la estrecha integración entre McAfee Network Security Platform, un sensor de IPS avanzado de alto rendimiento, y McAfee Advanced Threat Defense, el dispositivo de detección de malware avanzado más potente y completo del sector. McAfee Network Security Platform proporciona inspección de tráfico dentro de banda y bloqueo de amenazas mediante un conjunto de tecnologías de detección de malware que están optimizadas para su ejecución en tiempo real. McAfee Advanced Threat Defense ofrece un grupo de análisis más amplios y que incluyen más recursos, entre los que destacan entornos aislados para objetivos concretos y análisis de código estático. Juntos, estos dos dispositivos localizan y bloquean las amenazas avanzadas nuevas, desconocidas y ocultas. Si desea una solución integral completa, añada McAfee Real Time para identificar y reparar rápidamente los sistemas que hayan sufrido el ataque de malware avanzado.

- *Localización:* innovadoras tecnologías de análisis funcionan juntas para detectar de forma rápida y precisa las amenazas sofisticadas en varios protocolos.
- *Bloqueo*: los productos de seguridad de McAfee totalmente integrados detienen de inmediato los intentos de filtración adicionales y gestionan los endpoints infectados.
- *Corrección*: la solución de McAfee localiza automáticamente las nuevas filtraciones que se descubren en el entorno e inicia el proceso de reparación de los endpoints.

Despliegue centralizado

Escalabilidad y reducción del coste de propiedad



La solución McAfee Advanced Threat Defense para IPS de red aplica el enfoque Security Connected en cuanto a integración de la seguridad en la empresa, por lo que proporciona una serie de ventajas operativas y defensivas que son exclusivas en la industria. Por ejemplo:

- *Bloqueo de amenazas plug-and-play*: los ataques descubiertos por McAfee Advanced Threat Defense son bloqueados automáticamente por McAfee Network Security Platform sin necesidad de esperar a la intervención humana.
- *Integración de informes y flujos de trabajo*: los informes que genera McAfee Advanced Threat Defense se integran automáticamente en los flujos de trabajo de McAfee Network Security Platform, eliminando tareas duplicadas durante las investigaciones.
- *Visibilidad de los endpoints*: McAfee Advanced Threat Defense puede acceder y aprovechar la información sobre endpoints que guarda McAfee Network Security Platform para mejorar la velocidad y precisión en la detección de amenazas.

La prevención de intrusiones: McAfee Network Security Platform

McAfee Network Security Platform es una familia de dispositivos de prevención de intrusiones integrados que identifican y bloquean las amenazas sofisticadas en la red, incluido el malware avanzado, las amenazas de tipo zero-day, los ataques de denegación de servicio y las redes de bots. Mediante la combinación de una arquitectura extremadamente eficaz, de inspección profunda en un paso, con un hardware con fiabilidad de operadora y especialmente diseñado, McAfee Network Security Platform ofrece velocidades lineales de hasta 40 Gbit/s con un solo dispositivo y mantiene un rendimiento y una precisión excepcionales, sea cual sea la configuración de la seguridad. Entre los análisis de amenazas en placa se incluyen firmas personalizadas, análisis de protocolo completo, reputación de amenazas, análisis de archivos en profundidad con emulación y detección de JavaScript, y correlación entre los comportamientos de las amenazas basada en la visibilidad de capa 7 de más de 1500 aplicaciones y protocolos.

Mejor juntos

- Amplía el valor de las inversiones en seguridad actuales.
- Reduce la necesidad de rediseñar la arquitectura de la red.
- Amplía y automatiza la protección.
- Minimiza el trabajo de reparación e investigación con bloqueo en línea fiable.
- Simplifica los flujos de trabajo con la interfaz de McAfee Network Security Platform.

Security Connected

La plataforma Security Connected de McAfee ofrece una infraestructura unificada para cientos de productos, servicios y partners que permite compartir conocimientos, datos sobre el contexto en tiempo real y actuar conjuntamente con el fin de garantizar la seguridad de la información y las redes. Cualquier organización puede reducir los riesgos y el tiempo de respuesta, y minimizar los costes operativos y de personal gracias a los conceptos innovadores, los procesos optimizados y las recomendaciones prácticas que ofrece la plataforma.

Quizás la cualidad más destacable de McAfee Network Security Platform sea su capacidad para integrar y aprovechar la información y las funciones de otras soluciones de seguridad de McAfee. Particularmente importante para esta solución es su total integración con:

- El software Real Time for McAfee® ePolicy Orchestrator® (McAfee ePO), que ofrece visibilidad de los endpoints en tiempo real y el acceso para administración necesario para aislar y solucionar los ataques que consiguen su objetivo.
- McAfee Enterprise Security Manager, una revolucionaria solución de información de seguridad y administración de eventos (SIEM) que proporciona una visión en tiempo real del entorno de TI interno combinada y correlacionada con el contexto global del mundo exterior. La base de datos de McAfee Enterprise Security Manager, muy optimizada, recopila billones de eventos del registro y los contrasta con otros flujos de datos relevantes, para ofrecer acceso inmediato a años de datos de eventos de seguridad. Además, calcula líneas de base para todos los datos entrantes con el fin de identificar anomalías y amenazas potenciales antes de que se desarrollen, y simplifica la gestión del cumplimiento de normativas con cientos de paneles prediseñados e informes específicos para los estándares.
- McAfee Advanced Threat Defense es el componente de detección de malware avanzado de esta solución.

El entorno aislado: McAfee Advanced Threat Defense

McAfee Advanced Threat Defense es una solución de detección de malware multicapa que apila una serie ampliable de motores de inspección y funciones analíticas en una secuencia de selección descendente, de intensidad computacional incremental. Este enfoque exclusivo de una evaluación completa y, al mismo tiempo, eficaz ofrece un gran nivel de precisión y fiabilidad de detección, con un rendimiento elevadísimo. Los análisis en placa que aplica McAfee Advanced Threat Defense incluyen:

- Detección de virus, gusanos, spyware, bots, troyanos, desbordamientos del búfer y ataques combinados, basada en firmas, empleando una base de conocimientos global que crea y mantiene McAfee Labs, y que actualmente incluye casi 150 millones de firmas.
- Detección basada en la reputación utilizando la red de McAfee Global Threat Intelligence para localizar las nuevas amenazas que acaban de aparecer.
- Análisis estáticos en tiempo real y emulación para localizar rápidamente las amenazas de malware y zero-day no identificadas mediante las técnicas basadas en firmas o reputación.
- Análisis de código estático completo que revierte la ingeniería del código de los archivos con el fin de evaluar todos los atributos y conjuntos de instrucciones, y analizar íntegramente el código fuente sin ejecutarlo. Funciones de descompresión globales que abren todo tipo de archivos empaquetados y comprimidos con el fin de facilitar su análisis total y la clasificación del malware, de manera que las organizaciones puedan entender cómo es ese malware en concreto y el impacto que tiene en su organización. El análisis de código estático completo ofrece una visión crítica de los comportamientos que dependen de la entrada y de rutas de ejecución retardada u oculta que con frecuencia no se ejecutan durante el análisis dinámico y que suelen pasar por alto las soluciones de entorno aislado que no son tan completas.
- El análisis de entorno aislado dinámico que ejecuta el código de los archivos en un entorno de tiempo de ejecución virtual y observa el comportamiento resultante. McAfee Advanced Threat Defense configura los entornos de tiempo de ejecución virtuales para que reflejen el host atacado basándose en consultas al software McAfee ePO. Esta característica es exclusiva de esta solución de entorno aislado. El análisis del comportamiento de los archivos en las mismas condiciones que en el host destino del ataque genera resultados precisos de manera rápida y eficaz, revelando comportamientos maliciosos que no se habrían desencadenado en un entorno genérico. Y puesto que muchos ataques avanzados han sido diseñados para evadir la detección en entornos aislados, McAfee Advanced Threat Defense incluye innovadoras técnicas que garantizan la ejecución del código durante el análisis dinámico.

Dichas técnicas funcionan juntas de manera coordinada, con el fin de identificar de forma eficaz muchos tipos de malware conocido y no conocido. La combinación de análisis completo estático y dinámico descubre el malware oculto y avanzado que no se identifica mediante motores de análisis de menor peso.

Los dispositivos McAfee Advanced Threat Defense se configuran fácilmente para aplicar solamente los análisis que no se han realizado en los sensores de IPS de subida, eliminando el impacto que tienen en el rendimiento las inspecciones redundantes. Los dispositivos McAfee Advanced Threat Defense se adaptan a rendimientos de hasta 250 000 objetos al día, lo que permite utilizar un sistema antimalware avanzado con varios sensores de McAfee Network Security Platform. Junto a McAfee Network Security Platform, los dispositivos de McAfee Advanced Threat Defense se administran de forma centralizada mediante la interfaz basada en la Web que ofrece McAfee Network Security Manager.

Una solución de bucle cerrado eficaz para la prevención de amenazas avanzadas

La combinación de McAfee Network Security Platform y McAfee Advanced Threat Defense ofrece una protección extremadamente eficaz para prevención de intrusiones en la red, además de niveles máximos de detección de malware avanzado y respuesta. Se trata de una solución automatizada, de bucle cerrado que detecta los ataques sofisticados y los bloquea de raíz, reparando los sistemas host afectados sin necesidad de la intervención manual de los operadores de red o los analistas de seguridad, que normalmente están tan ocupados.

Para obtener más información sobre cómo las soluciones de McAfee pueden proteger su red contra las amenazas avanzadas ocultas, póngase en contacto con su representante de McAfee o visite www.mcafee.com/es/products/advanced-threat-defense.aspx

McAfee, S.A.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 85 00
www.mcafee.com/es

61051brf_atd-network-ips_0514_fnl_ETMG