Advanced Threat Defense para IPS de redes

Amplíe la protección contra el malware sigiloso.

Ventajas principales

- Encuentra, congela y soluciona automáticamente los ataques sigilosos y el malware avanzado oculto en el tráfico de red.
- Agrega a la seguridad de la red un análisis de código estático real y sandbox dirigido sin sobrecargar el IPS.
- Bloquea amenazas mediante Plug-and-play sin las demoras causadas por la intervención humana.

El sistema de prevención de intrusiones (IPS) basado en la red es el cimiento de la arquitectura en la seguridad empresarial. Los sistemas IPS, implementados en banda junto a gateways y a seguridad basada en el anfitrión, supervisan el tráfico de red y el comportamiento de los endpoints mediante una variedad de técnicas que detectan ataques y generan respuestas defensivas.

Hoy en día, sin embargo, un número creciente de amenazas desconocidas de tipo "día cero" están logrando evadir las defensas tradicionales. Estos ataques sofisticados, sigilosos, bien camuflados, de adaptación inteligente y que suelen estar cuidadosamente dirigidos, constituyen una pequeña pero desmesuradamente peligrosa y costosa parte en el campo de las amenazas cambiantes.

En respuesta, algunas organizaciones están agregando análisis dinámicos a su infraestructura IPS mediante dispositivos sandbox fuera de banda. Sandbox ejecuta programas sospechosos en un entorno virtual seguro y supervisa el comportamiento de ejecución para detectar propósitos maliciosos. Por lo general, sin embargo, esta ganancia aparente en precisión de detección se pierde ante la integración débil y los procesos de respuesta manuales.

Por ejemplo, la mayoría de los dispositivos sandbox de terceros solo pueden alertar a un analista de seguridad humano cuando se localiza un ataque nuevo. El analista debe crear manualmente nuevas reglas de bloqueo para el IPS y el firewall, y luego comenzar la tarea de identificar y reparar todos los endpoints comprometidos durante el análisis sandbox fuera de banda. Otras limitaciones comunes de las soluciones existentes incluyen:

- Un requisito de costo inflacionario en dispositivos sandbox por cada sensor IPS.
- Dependencia de un entorno de ejecución virtual genérico que puede pasar por alto comportamientos de ataques específicos al objetivo.
- Dependencia de análisis dinámicos solos, dejando al sandbox vulnerable a varias estrategias de malware para detectar entornos seguros y demorar la ejecución del comportamiento real.

Una solución IPS y sandbox de Security Connected

McAfee ofrece una solución para todos estos desafíos: una combinación estrechamente integrada de la McAfee Network Security Platform, un sensor IPS avanzado de alto rendimiento, con McAfee Advanced Threat Defense, el dispositivo de detección de malware avanzado más potente y completo de la industria. McAfee Network Security Platform proporciona inspección del tráfico en banda y bloqueo de amenazas mediante un conjunto de tecnologías de detección de malware que se optimizan para la ejecución en tiempo real. McAfee Advanced Threat Defense proporciona un conjunto de análisis más extensivo y aprovechador de recursos que incluye tanto el análisis sandbox de objetivo específico como el análisis de código estático real. Juntos, estos dos dispositivos encuentran y congelan amenazas avanzadas nuevas, desconocidas y sigilosas. Para una solución de punto a punto completa, agregue McAfee Real Time, que logra identificar y reparar cualquier sistema dañado por el malware avanzado.

- *Encontrar*: Las tecnologías innovadoras de análisis funcionan en conjunto para detectar de forma rápida y precisa las amenazas sofisticadas en diversos protocolos.
- *Congelar*: Los productos de seguridad con integración estrecha de McAfee detienen al instante los intentos de infiltración adicionales y contienen a los endpoints infectados.
- *Solucionar*: La solución de McAfee localiza automáticamente infiltraciones nuevas en el entorno e inicia el proceso de remediación del endpoint.

Implementación centralizada

Escalabilidad y costo total de propiedad inferior

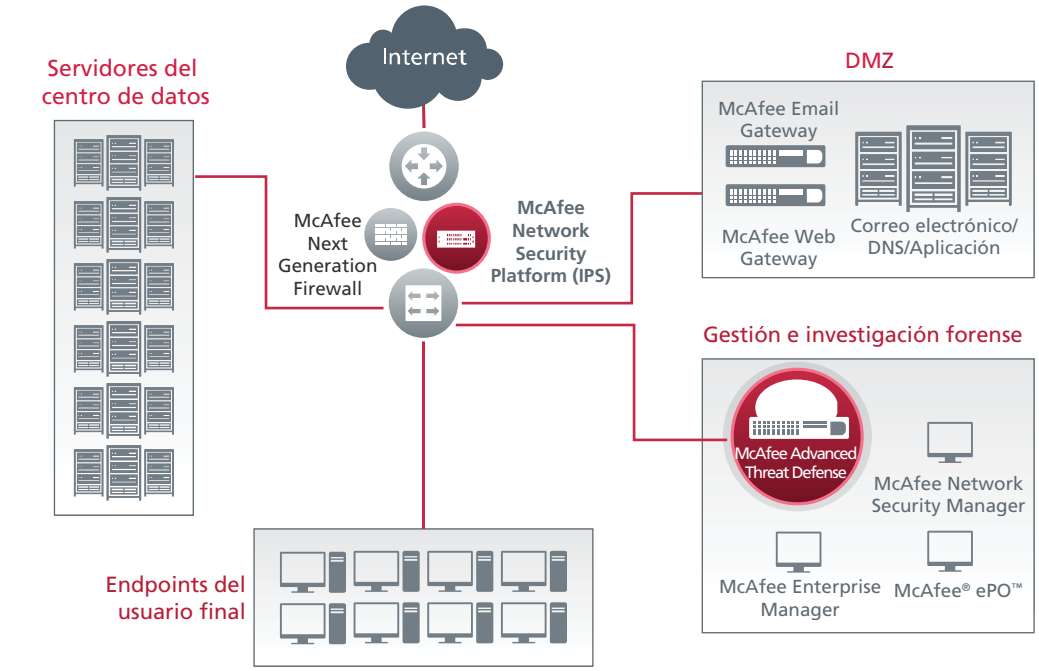

Imagen 1. Implementación centralizada de la solución McAfee® Network Security Platform IPS.

Como la solución McAfee Advanced Threat Defense para IPS de red sigue el enfoque Security Connected a la integración de seguridad empresarial, ofrece un rango de ventajas funcionales y defensivas únicas en la industria, entre otras:

- *Bloqueo de amenazas Plug-and-play*: McAfee Network Security Platform bloquea automáticamente los ataques descubiertos por McAfee Advanced Threat Defense sin necesidad o demora por la intervención humana.
- *Integración de informes y flujos de trabajo*: Los informes que genera McAfee Advanced Threat Defense se integran automáticamente a los flujos de trabajo de McAfee Network Security Platform, eliminando gran parte de la ida y vuelta entre pantallas durante las investigaciones.
- *Visibilidad del endpoint*: McAfee Advanced Threat Defense puede acceder y aprovechar cualquier inteligencia sobre endpoints almacenada en McAfee Network Security Platform para mejorar la velocidad y precisión en la detección de amenazas.

Mejores juntos

- Mejora el valor de las inversiones existentes en seguridad.
- Reduce la necesidad de reorganizar la arquitectura de la red.
- Amplía y automatiza la protección.
- Minimiza la remediación y la investigación mediante un bloqueo en línea confiable.
- Acelera los flujos de trabajo mediante la interfaz de McAfee Network Security Platform.

Security Connected

La plataforma Security Connected de McAfee proporciona un marco de trabajo unificado para cientos de productos, servicios y socios para aprender el uno del otro, compartir datos de contexto específico en tiempo real y trabajar como equipo para mantener la información y las redes a salvo. Cualquier organización puede reducir el riesgo y el tiempo de respuesta y minimizar los gastos generales y los costos de personal mediante los conceptos innovadores, los procesos optimizados y las recomendaciones prácticas de la plataforma.

IPS: McAfee Network Security Platform

McAfee Network Security Platform es una familia de dispositivos integrados de sistemas de prevención de intrusiones (IPS) que descubre y bloquea amenazas sofisticadas en la red, incluido el malware avanzado, las amenazas de día cero, ataques de denegación de servicio y botnets. McAfee Network Security Platform, al combinar una arquitectura de inspección profunda ultra eficiente y en un solo paso con un hardware operador fabricado expresamente, ofrece velocidades de línea de hasta 40 Gbps con un único dispositivo y mantiene un desempeño y precisión excepcionales en volúmenes de información más allá de las configuraciones de seguridad. Los análisis de amenazas incluyen firmas personalizadas, análisis completos de protocolos, reputación de las amenazas, análisis profundos de archivos con emulación y detección JavaScript, y correlación del comportamiento de la amenaza con el uso de la aplicación basado en una visibilidad de 7 capas para más de 1500 aplicaciones y protocolos.

Quizá la característica más potente de McAfee Network Security Platform es su capacidad para integrar y aprovechar los conocimientos y capacidades de otras soluciones de seguridad de McAfee. La importancia especial de esta solución es su integración perfecta con:

- Real Time para el software McAfee® ePolicy Orchestrator® (McAfee ePO), el cual proporciona visibilidad del endpoint en tiempo real y acceso a la gestión necesaria para aislar y remediar ataques exitosos.
- McAfee Enterprise Security Manager, una solución revolucionaria de gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés) que proporciona una vista en tiempo real del entorno de TI interno combinado y correlacionado con el contexto global del mundo exterior. La base de datos bien personalizada de McAfee Enterprise Security Manager reúne miles de millones de eventos de registros y los correlaciona con otros flujos de datos relevantes, poniendo a disposición varios años de datos sobre eventos de seguridad de inmediato. Calcula límites para todos los flujos de datos entrantes para identificar anomalías y amenazas posibles antes que se desarrollen, y simplifica la aplicación de la gestión con cientos de paneles prediseñados e informes específicos.
- McAfee Advanced Threat Defense es el componente de detección de malware avanzado de esta solución.

Sandbox: McAfee Advanced Threat Defense

McAfee Advanced Threat Defense es una solución de detección de malware de varias capas que apila una serie extensible de motores de inspección y capacidades analíticas en una secuencia de reducción por selección de intensidad informática creciente. Este enfoque único a una evaluación completa y eficiente, ofrece un nivel muy alto de precisión y confiabilidad en la detección, con un desempeño extremadamente alto en volúmenes de información. Los análisis aplicados por McAfee Advanced Threat Defense incluyen:

- Detección basada en firmas de virus, gusanos, spyware, bots, troyanos, desbordamientos del búfer y ataques combinados mediante una base de conocimiento completa creada y mantenida por McAfee Labs, que actualmente incluye cerca de 150 millones de firmas.
- Detección basada en reputación mediante la red McAfee Global Threat Intelligence para detectar nuevas amenazas emergentes.
- Análisis estático en tiempo real y emulación para descubrir rápidamente malware y amenazas de día cero no identificadas mediante técnicas basadas en firmas o reputación.
- Análisis de código estático completo que realiza ingeniería inversa del código del archivo para evaluar todos los atributos y conjuntos de instrucciones y analiza por completo el código fuente sin ejecución. Las capacidades integrales de desempaquetado abren a todo tipo de archivos comprimidos o empaquetados para permitir un análisis completo y clasificación del malware, ayudando así a las organizaciones a comprender mejor el malware específico con el que están lidiando y el impacto que tiene en su organización. El análisis de código estático completo proporciona conocimiento vital y crítico sobre los comportamientos de entradas dependientes y las rutas de ejecución ocultas o demoradas que normalmente no se ejecutan durante el análisis dinámico y que otras soluciones sandbox menos completas suelen pasar por alto.

- Análisis sandbox dinámico que ejecuta el código del archivo en un entorno de tiempo de ejecución virtual y que observa el comportamiento resultante. McAfee Advanced Threat Defense, único entre las soluciones sandbox actuales, configura entornos de ejecución virtuales para que coincidan con el anfitrión objetivo en función de consultas al software McAfee ePO. Analizar el comportamiento del archivo bajo las condiciones precisas del anfitrión objetivo produce resultados precisos de forma rápida y eficiente, revelando así los comportamientos maliciosos que no se activarían en un entorno genérico. Ya que muchos ataques avanzados están diseñados para evitar la detección sandbox, McAfee Advanced Threat Defense incluye técnicas innovadoras para garantizar la ejecución del código durante el análisis dinámico.

Estas técnicas funcionan de manera conjunta y coordinada para identificar con eficacia muchos tipos de malware conocidos y desconocidos. La combinación de análisis dinámico y estático completo revela malware ofuscado y avanzado que otros motores de análisis de menor peso no identificarían.

Los dispositivos de McAfee Advanced Threat Defense se configuran con facilidad para aplicar solo los análisis que no se hayan realizado en sensores IPS de flujo de carga, eliminando las reducciones de desempeño en inspecciones redundantes. Los dispositivos de McAfee Advanced Threat Defense se escalan mediante capacidades de volúmenes de información de hasta 250 000 objetos por día, permitiendo a un sistema de malware avanzado soportar varios sensores de McAfee Network Security Platform. Junto con McAfee Network Security Platform, los dispositivos de McAfee Advanced Threat Defense se gestionan de forma centralizada mediante la interfaz web que proporciona McAfee Network Security Manager.

Una solución para la prevención avanzada de amenazas que logra cerrar el círculo

La combinación de McAfee Network Security Platform y McAfee Advanced Threat Defense provee una protección excepcionalmente eficiente, junto con una extremadamente efectiva detección y respuesta contra malware avanzado. Esta es una solución automatizada que logra cerrar el círculo, que encuentra ataques sofisticados, los congela en el camino, y repara estaciones afectadas sin la necesidad de intervención manual de operadores o analistas de seguridad.

Para obtener más información sobre cómo las soluciones de McAfee pueden asegurar su red contra amenazas avanzadas y sigilosas, comuníquese con su representante de McAfee o ingrese a www.mcafee.com/atd.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

61051brf_atd-network-ips_0514_fnl_ETMG