McAfee Network Security Platform

Un enfoque inteligente e integral para la seguridad en Internet

McAfee® Network Security Platform (McAfee NSP) es un sistema de prevención de intrusiones (IPS) de próxima generación que descubre y bloquea amenazas de malware sofisticadas en la red. Emplea técnicas avanzadas de detección y emulación, y va más allá de la comparación con patrones para ofrecer protección contra los ataques ocultos con un alto grado de precisión. Para satisfacer las necesidades de las redes más exigentes, la plataforma puede adaptarse hasta 40 Gbit/s con un solo dispositivo. La cartera integrada de soluciones de McAfee simplifica las operaciones de seguridad mediante la combinación de la información en tiempo real de McAfee Global Threat Intelligence y los datos contextuales completos sobre usuarios, dispositivos y aplicaciones, con el fin de responder de manera rápida y precisa a los ataques que se propagan por la red.

Protección contra las amenazas sigilosas actuales

Su red se enfrenta a ataques sigilosos y avanzados capaces de evadir los métodos de detección tradicionales, que exponen a sus aplicaciones y datos a devastadoras fugas y a tiempo de inactividad. Desafortunadamente, la mayoría de las empresas carecen de los recursos financieros y operativos para implementar y administrar la combinación de herramientas y tecnologías necesarias para ofrecer una defensa adecuada.

McAfee NSP combina la prevención de amenazas inteligente con una administración de seguridad intuitiva para mejorar la precisión de las detecciones y facilitar las operaciones de seguridad. Ninguna tecnología de detección de malware es capaz de prevenir todos los ataques por sí sola, razón por la cual McAfee NSP incorpora varios motores de detección con firmas y sin firmas para evitar que el malware no deseado cause estragos en su red. Realiza inspecciones en profundidad del tráfico de red mediante una combinación de tecnologías avanzadas, que incluyen análisis de protocolo completo, reputación de amenazas y análisis de comportamientos para detectar y proteger frente a devoluciones de llamadas del malware, ataques de tipo zero-day y de denegación de servicio (DoS), y otras amenazas avanzadas.

Principales ventajas

- Detecta y bloquea rápidamente las amenazas para proteger aplicaciones y datos
- Solución de alto rendimiento y escalable para entornos dinámicos
- Administración centralizada para mejorar la visibilidad y el control
- Detección avanzada, incluido el análisis de malware sin firmas
- Cifrado SSL entrante y saliente para inspeccionar el tráfico de red
- Alta disponibilidad y protección de recuperación ante desastre

NSS LABS RECOMMENDED

Síganos

Seguridad integrada

McAfee Network Security Platform se integra con McAfee Advanced Threat Defense, que combina análisis de código estático en profundidad, análisis dinámico (con entornos aislados para malware) y aprendizaje automático, para detectar amenazas de tipo zero-day, como las que emplean técnicas de evasión y el ransomware. McAfee NSP también combina reputación de archivos de McAfee Global Threat Intelligence y ofrece integración con el software McAfee® ePolicy Orchestrator® y con McAfee Enterprise Security Manager para la correlación en tiempo real de eventos de red en todas las fuentes relevantes. La solución combinada incorpora detalles sobre dispositivos, información de usuarios, estado de seguridad de endpoints, evaluaciones de vulnerabilidades y otra información completa para ayudar a las empresas a comprender la gravedad de las amenazas y los factores que ponen en riesgo la actividad empresarial.

Rendimiento y disponibilidad

McAfee Network Security Platform ofrece todas las ventajas: seguridad y alto rendimiento. Combina una arquitectura de inspección basada en protocolos, de un solo paso, con un hardware específico de categoría de operadora para conseguir en la práctica un rendimiento de análisis de más de 40 Gbit/s con un solo dispositivo. A diferencia de otras soluciones IPS en las que el rendimiento se deteriora hasta un 50 % debido a un enfoque de que da prioridad a la seguridad frente al rendimiento, la eficaz arquitectura de McAfee Network Security Platform mantiene el rendimiento sea cual sea la configuración de la seguridad.

McAfee NSP ofrece también conmutación en caso de error activo/activo y activo/pasivo con mantenimiento de la información del estado, lo que permite cumplir los acuerdos de nivel de servicio de alta disponibilidad y, al mismo tiempo, evitar los retrasos provocados por dispositivos más lentos o la sobrecarga de las soluciones independientes.

Visibilidad y control

Tome decisiones fundamentadas sobre las aplicaciones y los protocolos de su red. McAfee Network Security Platform es la primera y la única solución IPS que combina prevención avanzada de amenazas y conocimiento de las aplicaciones en un solo motor de decisión de seguridad. Nosotros correlacionamos la actividad de las amenazas con el uso de las aplicaciones, con visibilidad de más de 1500 aplicaciones y protocolos de la capa 7 del modelo OSI, para que pueda decidir con fundamento qué aplicaciones pueden ejecutarse en su red.

Además de la identificación de aplicaciones, McAfee NSP ofrece visibilidad de usuarios y dispositivos. Prioriza los hosts y los usuarios que corren riesgos, incluidas las redes de bots activas, mediante la identificación de comportamientos anómalos en la red.

Principales ventajas (continuación)

- Hay también disponibles dispositivos virtuales.
- Se integra con la cartera de soluciones de McAfee para ofrecer seguridad del dispositivo a la nube.

Administración de seguridad inteligente y escalable

Saque el máximo partido a su inversión en seguridad con administración de seguridad inteligente e integrada. McAfee Network Security Manager ofrece administración escalable, basada en la Web, que puede incluir desde dos hasta cientos de dispositivos de seguridad de la red. Proporciona flujos de trabajo de aparición progresiva que guían a los administradores a las alertas relevantes, así como paneles de seguridad de fácil uso que priorizan los eventos de manera automática, según la gravedad y la trascendencia de la alerta.

Funciones adicionales

Prevención de amenazas avanzadas

- El cifrado Secure Sockets Layer (SSL) entrante es compatible con los cifradores Diffie-Hellman (DH) y Elliptic-Curve Diffie–Hellman (ECDH), mediante el uso de una solución de clave compartida basada en agente que no afecta al rendimiento del sensor (pendiente de patente, para la serie NS).
- Descifrado SSL saliente (serie NS)
- Motor de emulación de McAfee Gateway Anti-Malware
- Motor de emulación de PDF en JavaScript
- Motor de análisis de comportamiento de Adobe Flash
- Protección contra evasiones avanzadas
- Análisis de reputación de amenazas en dispositivos móviles y en la nube

Protección frente a redes de bots y devoluciones de llamadas de malware

- Detección de devoluciones de llamadas a DNS/DGA de flujo rápido
- "Sinkholing" de DNS
- Detección heurística de bots
- Correlación de varios ataques
- Base de datos de control y mando

Prevención de intrusiones avanzada

- Desfragmentación de IP y remontaje del tráfico TCP
- Firmas de McAfee, definidas por el usuario y de código abierto
- Compatibilidad nativa con firmas Snort (serie NS)
- Mejoras de lista blanca/lista negra para admitir Structured Threat Information eXpression (STIX) (serie NS)
- Cuarentena de hosts y limitación de velocidad
- Inspección de entornos virtuales
- Integración con McAfee Advanced Threat Defense
- Compatibilidad con descomprensión de respuestas HTTP

Prevención de denegación de servicio (DoS) y denegación de servicio distribuida (DDoS)

- Detección basada en umbrales y en análisis heurístico
- Limitación de conexiones específicas de hosts
- Detección basada en perfil con autoaprendizaje

McAfee Global Threat Intelligence

- Reputación de archivos y direcciones IP
- Reputación de aplicaciones y protocolos
- Geolocalización
- Uso de listas blancas según las categorías de McAfee Global Threat Intelligence

Alta disponibilidad

- Conmutación en caso de error con mantenimiento de la información del estado activo/activo y activo/pasivo
- Protección de carga en caso de error externa (activa)
- Protección de carga en caso de error integrada

Encapsulado de protocolos (tunneling)

- IPv6
- Túneles V4-in-V4, V4-in-V6, V6-in-V4 y V6-in-V6
- MPLS
- GRE
- VLAN doble Q-in-Q

McAfee Network Security Manager

- Administración en niveles (hasta 1000 sensores)
- Autenticación de usuarios (RADIUS y LDAP)
- Conmutación en caso de error y recuperación automáticas
- Recuperación de los datos de configuración críticos en caso de desastre
- Administración centralizada y jerárquica de directivas
- El panel de memoria muestra datos del uso de memoria por cada dispositivo.

Más información

Para obtener más detalles, consulte la **hoja de especificaciones de McAfee Network Security Platform**.

McAfee
Together is power.

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