McAfee Network Threat Behavior Analysis

Total visibilidad del comportamiento y las amenazas de la red

McAfee® Network Threat Behavior Analysis es un componente integrado de McAfee Network Security Platform —parte de la oferta de productos de McAfee— que ofrece en tiempo real visibilidad y protección frente a amenazas para la infraestructura de red. Mediante el análisis del tráfico de conmutadores y enrutadores, McAfee Network Threat Behavior Analysis detecta comportamientos de riesgo en la red y previene de manera eficaz ataques ocultos. Evalúa holísticamente las amenazas a nivel de la red, identifica el comportamiento global de cada elemento de la red y permite la abstracción instantánea de la posible anomalía o tipo de ataque, como malware, ataques de tipo zero-day, redes de bots y gusanos. McAfee Network Threat Behavior Analysis integra también alguno de los motores avanzados de McAfee Network Security Platform, como el motor de emulación en tiempo real, que identifica el malware sin necesidad de utilizar firmas.

Visibilidad inteligente para los sigilosos ataques de la actualidad

Su red se enfrenta a ataques sigilosos y avanzados capaces de evadir los métodos de detección tradicionales, que la exponen a devastadoras fugas y tiempo de inactividad. McAfee Network Threat Behavior Analysis supervisa e informa de forma inteligente de la presencia de comportamientos inusuales mediante el análisis del tráfico de la red desde los conmutadores y enrutadores. De esta forma puede identificar y responder rápidamente a los ataques en su red.

El dispositivo McAfee Network Threat Behavior Analysis aprovecha los datos de NetFlow y J-Flow para identificar las amenazas que se encuentran fuera del perímetro típico de los sistemas de prevención de intrusiones (IPS). Se trata de un dispositivo totalmente equipado con procesadores de núcleo cuádruple, una matriz de discos RAID y conectividad Gigabit Ethernet. También proporciona conectividad fuera de línea a una red de área de almacenamiento (SAN, Storage Area Network). Con su capacidad de flujos diferenciados, puede gestionar grandes cantidades de tráfico de red, lo que facilita un análisis más rápido del tráfico.

Ventajas principales

Visibilidad para proteger la red

- Supervisión y detección del comportamiento inusual de la red mediante el análisis del tráfico de la red.
- Detección proactiva de amenazas basada en el comportamiento.
- Detección eficaz de las amenazas desconocidas.
- La detección de anomalías incluye los ataques de tipo zero-day, el spam, las redes de bots y los ataques de reconocimiento.

Protección antimalware completa

- Detención del malware con emulación en tiempo real de archivos maliciosos.
- Correlación avanzada en toda la red para detectar la actividad de redes de bots.
- Información sobre endpoints y correlación para los flujos y eventos de la red.

Visibilidad y conocimiento de la red inigualables

McAfee Network Threat Behavior Analysis le permite tomar decisiones fundamentadas sobre las aplicaciones y los protocolos de su red. Supervisa e informa de los comportamientos inusuales en la red e identifica las amenazas mediante algoritmos basados en comportamientos. Analizando el comportamiento del host y de las aplicaciones, proporciona detección de anomalías que permiten localizar ataques zero-day, spam, redes de bots y ataques de reconocimiento. Con un análisis de flujos global, se identifica el uso de aplicaciones no autorizado y se señalan los segmentos de la red que presentan problemas.

Control y prevención de brotes de malware

McAfee Network Threat Behavior Analysis, que actúa junto con McAfee Network Security Platform, proporciona emulación en tiempo real para la inspección avanzada y el bloqueo de archivos sospechosos. El motor de emulación en tiempo real analiza los archivos sospechosos para detectar y bloquear el comportamiento malicioso. Con correlación avanzada en varios IPS y dispositivos de red, McAfee Network Threat Behavior Analysis encuentra las redes de bots ocultas que sortean las defensas tradicionales, basadas en firmas. Junto a McAfee Endpoint Intelligence Agent, detecta y controla los endpoints atacados que transmiten tráfico malicioso disfrazado como tráfico de red legítimo. El análisis de la actividad de los endpoints basado en la reputación limita la filtración de datos y previene brotes de malware.

Simplificación de las operaciones de seguridad y ahorro de dinero

McAfee Network Threat Behavior Analysis ofrece la información de utilidad que necesita para la administración rentable de la seguridad. El dispositivo acelera el tiempo de respuesta a incidentes y simplifica el rendimiento de la red, mientras que evita que las amenazas y exploits en la red interrumpan las operaciones de la empresa.

Características adicionales

- Seguridad ampliada gracias a la integración con McAfee Global Threat Intelligence (McAfee GTI).
- Edición virtual para implementaciones económicas.
- Mayor visibilidad y correlación gracias a la integración del software McAfee ePolicy Orchestrator® (McAfee ePO™), McAfee Enterprise Security Manager y el software McAfee Vulnerability Manager.
- Clasificación y análisis del tráfico de red sin esfuerzo.
- Panel de metadatos por flujo (ID de aplicación, Archivos, URL).
- Aumento del perfil de seguridad con opciones globales de cuarentena.
- Visibilidad del host externo con calificaciones detalladas de factores de amenazas al host.
- Compatible con conmutadores y enrutadores Cisco (NetFlow v5 y v9) y Juniper (J-Flow v5 y v9).

FICHA TÉCNICA

	NTBA T-600	NTBA T-1200
Especificaciones		
Paquetes por segundo	Hasta 60 000	Hasta 100 000
Cisco NetFlow	v5 y v9	v5 y v9
Juniper J-Flow	v5 y v9	v5 y v9
Procesador	1x Xeon E5-2658	2 x Xeon E5-2658
Memoria	46 GB	96 GB
Almacenamiento aprovechable	4,4 TB/Raid 10	8,8 TB/Raid 10
Conexiones de red	x4 de cobre 10/100/1000	x4 de cobre 10/100/1000
Entorno		
Formato	1U	2U
Ancho	43,8 cm	43,8 cm
Fondo	70,94 cm	70,78 cm
Alto	4,32 cm	8,76 cm
Peso máximo	14,96 kg	21,6 kg
Uso de energía estimado (como máximo)	402 W	667 W
Fuente de alimentación redundante	750 W	750 W
Requisitos de refrigeración del sistema (BTU/hora)	1370	2280
Temperatura de funcionamiento	De +10 °C a +35 °C, con una tasa máxima de variación que no supere los 10 °C por hora	

Especificaciones de NTBA virtual	T-VM	T-100VM	T-200VM
RAM recomendada	16 GB	8 GB	16 GB
CPU recomendada	4	4	4
Flujos por segundo	Hasta 25 000 fps	Hasta 10 000 fps	Hasta 25 000 fps

McAfee
Together is power.

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