McAfee Network Threat Response

Centrada específicamente en las amenazas persistentes avanzadas dentro de la red

McAfee® Network Threat Response está especializada en desenredar la madeja de amenazas para localizar ese ataque persistente dirigido específicamente contra su empresa que consigue escabullirse e introducirse subrepticiamente en la red. La plataforma de motores de próxima generación de McAfee Network Threat Response se centra en desenmascarar los ataques del lado del usuario, comúnmente conocidos como "amenazas persistentes avanzadas". Los eventos de seguridad se clasifican por orden de prioridad y solo se muestran los que requieren un examen en profundidad, lo que reduce a minutos el tiempo de análisis. La integración de McAfee Global Threat Intelligence™ (McAfee GTI™), McAfee Network Security Platform y McAfee Firewall Enterprise garantiza la protección contra la amenaza de seguridad que más preocupa en la actualidad: los ataques selectivos persistentes.

Ventajas principales

Detección del malware avanzado de tipo zero day
- Amenazas prevalentes avanzadas
- Archivos PDF infectados
- Redes de bots
- Descargas desapercibidas
- Ingeniería social
- Amenazas únicas, dirigidas exclusivamente a su empresa

Reducción del tiempo de respuesta
- Identifica el malware automáticamente
- Acelera el análisis de las amenazas complejas y clasifica los eventos por orden de prioridad para examinarlos en minutos, en lugar de semanas

Análisis avanzados para equipos de seguridad de todos los tamaños
- Identifica las amenazas que escapan a la detección de otras herramientas
- Captura, archiva y registra el tráfico de red para realizar un análisis complementario
- Acelera el análisis de los dispositivos de registro de paquetes de red

Opciones de despliegue flexibles
- Sensores virtuales
- Dispositivos que ofrecen un rendimiento de detección de hasta 2 Gbits/s
- Plataforma de categoría de operadora de más de 10 Gbits/s que utiliza dispositivos SAIC/CloudShield

Facilidad de despliegue
- La instalación del dispositivo McAfee Network Threat Response sólo lleva unos minutos

Dejar al descubierto lo que los ciberdelincuentes quieren disimular

El malware avanzado se caracteriza fundamentalmente por su capacidad para eludir la detección. McAfee Network Threat Response frustra estos intentos mediante la incorporación de una plataforma de herramientas para protegerse contra los archivos PDF maliciosos, las redes de bots, las descargas desapercibidas y los ataques de ingeniería social. Estas herramientas incluyen analizadores heurísticos de archivos PDF, bases de datos de amenazas en tiempo real, verificación de tipos de archivos y detección de ejecutables ocultos.

McAfee Network Threat Response no solo alerta de la presencia de la ocultación, sino que descodifica el tráfico, lo que ofrece a los analistas un nivel de visibilidad inigualable sobre los ataques.

Encontrar el arma del crimen

En una investigación criminal, el arma del crimen permite encontrar al asesino. En el caso de los ataques selectivos, el "asesino" es el código shell.

El código shell es un conjunto de instrucciones que utiliza el malware para infectar y controlar un equipo. McAfee Network Threat Response utiliza análisis heurísticos, pendientes de patente, para detectar la presencia de código shell, sin necesidad de conocer previamente la carga útil, en constante evolución, asociada a los ataques.

Juntar las piezas del rompecabezas

El código shell se introduce progresivamente en la red a la espera del momento idóneo para ejecutar su código y desencadenar el ataque. McAfee Network Threat Response tiene la capacidad única de descubrir los ataques persistentes, de evolución lenta, identificando y recopilando datos de las distintas fases de los ataques. Ninguna otra utilidad existente le permite reconstruir el rompecabezas de la amenaza que pesa sobre su empresa reuniendo las piezas introducidas sigilosamente en la red.

Código shell: antes y después

Antes

Después

http://w.hack.info/data_theft.exe

Reducir a minutos el tiempo de análisis

Las soluciones de captura y análisis forense de los datos de la red permiten a los analistas reproducir el tráfico histórico con el fin de determinar la causa subyacente de un evento de malware, así como la exposición generada. Las funciones de importación PCAP de McAfee Network Threat Response aceleran este análisis. A medida que los datos son filtrados por lo motores de análisis, McAfee Network Threat Response descodifica el tráfico oculto y deja al descubierto los indicadores clave. De esta forma, los analistas disponen de elementos confirmados que pueden servir de punto de partida de exámenes complementarios, lo que permite reducir en varios días el tiempo de análisis.

Optimizar la eficacia del personal de seguridad

Los dispositivos de seguridad convencionales generan a diario una gran cantidad de eventos, de los que un porcentaje ínfimo son indicadores de actividad asociada a ataques selectivos. McAfee Network Threat Response identifica estos ataques con precisión, permitiendo a los analistas reconocer totalmente los eventos pertinentes en cuestión de minutos. La solución es tan poderosa que un solo analista consigue el nivel de eficacia de 20 investigadores de malware.

Garantizar la protección a nivel local gracias a un sistema de información global

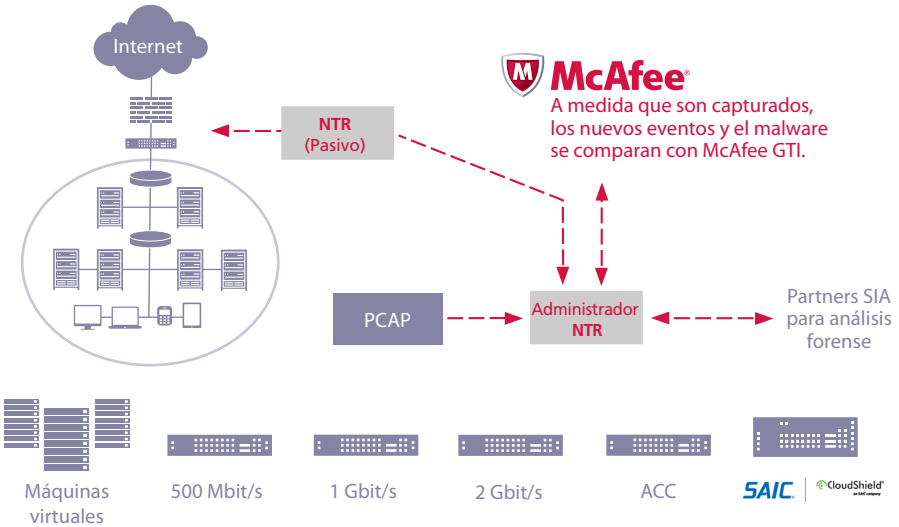
McAfee Global Threat Intelligence (GTI) recopila la información procedente de cientos de miles de dispositivos repartidos por todo el mundo. Este sistema mundial de información permite ir más allá de la simple detección de sistemas de mando y control de redes de bots e identifica los servidores origen del malware malicioso utilizados durante la fase inicial de la infección. Gracias a estos vastos bancos de datos de reputación mundial, McAfee Network Threat Response es capaz de detectar las comunicaciones con ciberdelincuentes conocidos en todo el mundo, con el fin de actuar rápidamente contra las amenazas potenciales.

Bloquear las amenazas persistentes avanzadas de todos los tipos

McAfee Network Threat Response es la tecnología con el mejor rendimiento del sector en protección de la red contra amenazas persistentes avanzadas. Esta plataforma de análisis forense y evaluación de exposición a amenazas es capaz de detectar el malware avanzado, inspeccionar el tráfico fuera de banda e identificar los ataques nuevos y desconocidos que escapan a la acción de otras tecnologías de seguridad. McAfee Network Threat Response descubre las amenazas persistentes avanzadas, las redes de bots, los troyanos, las secuencias de comandos y el código shell. A continuación, los somete a un análisis profundo y captura su carga útil, con el fin de proporcionar toda la información relativa a sus puntos de origen, los vectores de infección y las vulnerabilidades que pretenden aprovechar. Asimismo, McAfee Network Threat Response descodifica las cargas activas y los ataques fragmentados (y posteriormente emsamblados) que han sido ocultados deliberadamente en la red.

Gracias a esta comprensión precisa de la amenaza en todas sus fases (desde la infiltración inicial hasta la exfiltración destinada a robar información), puede repeler los ataques en todas sus formas posibles. Este conocimiento ofrece además una visibilidad inigualable que la empresa puede aprovechar para elaborar una estrategia de protección completa que la inmunice frente a futuras amenazas.

Basada en una infraestructura de investigación ampliable, capaz de evolucionar a medida que lo hacen las tecnologías de ataque, McAfee Network Threat Response se adapta en función del crecimiento de la red y garantiza un ahorro de tiempo, todo ello poniendo a su disposición en todo momento las soluciones más sofisticadas.



McAfee

Especificaciones de hardware de McAfee Network Threat Response

Número de modelo	A50VM	A50	A100	A200	ACC
Función	Sensor virtual	Sensor	Sensor	Sensor	Consola de administración
Rendimiento de producción	200 Mbits/s	500 Mbits/s	1 Gbit/s	2 Gbits/s	Hasta 10 sensores
Puertos					
Puertos Ethernet 10/100/1000 para los sensores	—	4	3	5	—
Puertos de administración 10/100/1000	—	1	1	1	1
Modo de funcionamiento					
Conectividad a McAfee Network Security Platform serie M	Sí	Sí	Sí	Sí	—
Supervisión de puertos SPAN	Sí	Sí	Sí	Sí	—
Máquina virtual	Sí	—	—	—	—
Hardware					
Servidor Intel	—	SR1630HGPRX	SR1625URSAS	SR1625URSAS	SR1625URSAS
Núcleos de procesador	—	4	4	8	8
Procesador	—	1	1	2	2
Memoria	—	2 GB	6 GB	12 GB	12 GB
Discos duros	—	500 GB	2 x 300 GB	4 x 300 GB	4 x 300 GB
Sistema operativo	—	RHEL5	RHEL5	RHEL5	RHEL5
Alta disponibilidad					
Alimentación redundante	—	NO	SÍ	SÍ	SÍ
Nivel RAID	—	SATA	RAID 1	RAID 10	RAID 10
Características físicas					
Factor de forma	Máquina virtual	1U	1U	1U	1U
Dimensiones del chasis	—	4,31 cm (Alto) x 43 cm (Ancho) x 64,79 cm (Fondo)	4,31 cm (Alto) x 43 cm (Ancho) x 66,54 cm (sin el brazo de recogida de cables) (Fondo)	4,31 cm (Alto) x 43 cm (Ancho) x 66,54 cm (sin el brazo de recogida de cables) (Fondo)	4,31 cm (Alto) x 43 cm (Ancho) x 66,54 cm (sin el brazo de recogida de cables) (Fondo)
Dimensiones del paquete	—	59,18 cm (Ancho) x 106,17 cm (Largo) x 21,84 cm (Alto)	59,18 cm (Ancho) x 106,17 cm (Largo) x 21,84 cm (Alto)	59,18 cm (Ancho) x 106,17 cm (Largo) x 21,84 cm (Alto)	59,18 cm (Ancho) x 106,17 cm (Largo) x 21,84 cm (Alto)
Peso	—	Aprox. 19,73 kg	Aprox. 24,72kg	Aprox. 25,4kg	Aprox. 25,4kg
Consumo eléctrico	Hasta dos módulos de alimentación de 650 W				
Potencia de entrada	Conmutación automática 110-220 V CA				
Temperatura de funcionamiento	+10 °C a +35 °C, con una tasa máxima de variación que no supere los 10 °C por hora				
Temperatura en apagado	Por debajo de -40 °C y por encima de +70 °C				

Continúa en la página siguiente.

Especificaciones de hardware de McAfee Network Threat Response

Humedad en apagado	90%, sin condensación a 35 °C
Cumplimiento de normativas en materia de seguridad	UL60950—CSA 60950 (EE. UU./Canadá), EN60950 (Europa), IEC60950 (International), certificado e informe CB, IEC60950 (informe que cubre todas las desviaciones por país), certificación GS (Alemania), GOST R 50377-92 - certificación (Rusia), certificación para Bielorrusia (Bielorrusia), certificación para Ucrania (Ucrania), Directiva 73/23/EEE (Europa) relativa al material eléctrico de baja tensión, certificación IRAM (Argentina)
Conformidad del producto en materia de compatibilidad electromagnética—Conformidad con la Clase A	FCC/ICES-003 - verificación de emisiones (EE. UU./Canadá), CISPR 22 - emisiones (Internacional), EN55022 - emisiones (Europa), EN55024 - inmunidad (Europa), EN61000-3-2 - corriente armónica (Europa), EN61000-3-3 - fluctuaciones de tensión (Europa), Directiva 89/336/CEE relativa a la compatibilidad electromagnética (Europa), emisiones VCCI (Japón), AS/NZS 3548 - emisiones (Australia/Nueva Zelanda), BSMI CNS 13438 - emisiones (Taiwán), GOST R 29216-91 - emisiones (Rusia), GOST R 50628-95 - inmunidad (Rusia), certificación para Bielorrusia (Bielorrusia), certificación para Ucrania (Ucrania), certificación KCC (interferencia electromagnética) (Corea)

McAfee, S.A.
Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8535
www.mcafee.com/es

31101ds_ntr_1011