McAfee Advanced Threat Defense

Detección de ataques selectivos avanzados

McAfee® Advanced Threat Defense permite a las empresas detectar los ataques selectivos avanzados y convertir la información sobre las amenazas en acción y protección inmediatas. A diferencia de los entornos aislados tradicionales, incluye nuevas funciones de inspección que mejoran la detección y revelan las amenazas evasivas. La firme integración entre las soluciones de seguridad —desde la red hasta los endpoints— permite compartir al instante la información sobre las amenazas con todo el entorno, lo que redunda en beneficio de la protección y la investigación. Opciones de despliegue flexibles para todas las redes.

Principales diferenciadores de McAfee Advanced Threat Defense

Máxima integración de las soluciones de McAfee

- Reduce el intervalo entre la detección, la contención y la protección de toda la organización.
- Simplifica los flujos de trabajo para agilizar la reacción y la corrección.

Potentes funciones de análisis

- Utiliza potentes técnicas de descompresión que permiten realizar análisis mejores y más completos.
- Combina análisis en profundidad de código, análisis dinámicos y aprendizaje automático para garantizar una detección más precisa con datos de análisis inigualables.

Despliegue flexible y centralizado

- Reduce el coste gracias al despliegue centralizado que admite un gran número de protocolos.
- Opciones de despliegue flexibles para todas las redes.

Nuestra tecnología ha revolucionado el ámbito de la detección al conectar las funciones de análisis del malware avanzado con las defensas existentes —desde el perímetro de la red hasta los endpoints— y compartir la información sobre las amenazas con todo el entorno de TI. Compartiendo esta información entre los sistemas de administración, redes y endpoints, nuestras soluciones cierran inmediatamente las comunicaciones de comando y control y ponen en cuarentena los sistemas en peligro, bloquean las demás instancias de la misma amenaza u otras similares, evalúan dónde puede haberse producido el daño e inician las acciones pertinentes.

McAfee Advanced Threat Defense: detección de amenazas avanzadas

McAfee Advanced Threat Defense detecta el malware más sigiloso, de tipo zero-day, con una estrategia innovadora por capas. Esta solución combina motores de análisis estático que no requieren intervención, como las firmas antivirus, los basados en la reputación y la emulación en tiempo real, con análisis dinámicos (en entornos aislados), con el fin de examinar el comportamiento real. La investigación continúa con un análisis detallado del código estático que examina los atributos de archivos y los grupos de instrucciones con el fin de descubrir el comportamiento previsto o evasivo, y evaluar las semejanzas con familias de malware conocidas. En el último paso del análisis, McAfee Advanced Threat Defense busca específicamente indicadores de actividad maliciosa identificados a través de aprendizaje automático mediante una red neuronal. Con todo ello se obtiene la protección contra el malware avanzado más sólida del mercado y se garantiza una inspección en profundidad eficaz, sin sacrificar el rendimiento. Este se ve favorecido por los métodos de menor intensidad analítica, como las firmas y la emulación en tiempo real, que detectan el malware conocido, mientras que la incorporación al entorno aislado del análisis de código estático en profundidad y de la información obtenida a través del aprendizaje automático amplía la protección contra las amenazas más camufladas y evasivas. Si hay indicadores de actividad maliciosa que no se ejecutan en un entorno dinámico, es posible identificarlos mediante

McAfee
Together is power.

Soluciones integradas

- McAfee Active Response
- McAfee Advanced Threat Defense Email Connector
- McAfee Enterprise Security Manager
- Software ePolicy Orchestrator®
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
  - McAfee Application Control
  - McAfee Endpoint Protection
  - McAfee Server Security
- McAfee Web Gateway

la descompresión, el análisis en profundidad del código estático y la información obtenida del aprendizaje automático.

Los creadores de malware utilizan la compresión para modificar la composición del código u ocultarlo a fin de eludir la detección. La mayoría de los productos no pueden descomprimir correctamente el código ejecutable original (fuente) para su análisis. McAfee Advanced Threat Defense incluye numerosas funciones de descompresión que dejan al descubierto el código ejecutable original. De esta forma, el análisis en profundidad de código estático no se limita a examinar los atributos de archivo de primer nivel, sino que detecta anomalías analizando los atributos y conjuntos de instrucciones para averiguar el comportamiento previsto.

Juntos, el análisis en profundidad de código estático, el aprendizaje automático y el análisis dinámico, proporcionan una evaluación completa y detallada del malware sospechoso. Unos resultados de análisis inigualables generan informes de resumen que ayudan a comprender mejor la amenaza y las acciones prioritarias, e informes más detallados que proporcionan datos de alta calidad sobre el malware.

Protección mejorada

Encontrar el malware avanzado es importante, pero si una solución se limita a presentar un informe o a emitir una alerta, los administradores siguen enfrentándose a una enorme cantidad de trabajo y la red continúa desprotegida.

La estrecha integración entre McAfee Advanced Threat Defense y los dispositivos de seguridad —desde el perímetro de la red hasta los endpoints— permite que los dispositivos actúen inmediatamente cuando McAfee Advanced Threat Defense califica un archivo de malicioso. Esta integración firme y automatizada entre la detección y la protección es crucial.

McAfee Advanced Threat Defense se integra de distintas formas: directamente con soluciones de seguridad concretas, a través de McAfee Threat Intelligence Exchange o mediante McAfee Advanced Threat Defense Email Connector.

La integración directa permite que las soluciones de seguridad de McAfee tomen medidas inmediatas con los archivos que McAfee Advanced Threat Defense identifica como maliciosos, como incorporar al instante la información sobre la amenaza en los procesos existentes de implementación de directivas y bloquear las demás instancias de esos archivos o archivos similares para que no entren en la red.

Las calificaciones de McAfee Advanced Threat Defense aparecen en los registros y paneles de los productos integrados como si estos hubiesen realizado todo el análisis, lo que agiliza los flujos de trabajo y, al operar con una sola interfaz, permite a los administradores manejar las alertas con eficacia.

La integración con McAfee Threat Intelligence Exchange amplía las funciones de McAfee Advanced Threat Defense con defensas tales como McAfee Endpoint Protection, y posibilita que una amplia variedad de soluciones de seguridad integradas accedan a los resultados de los análisis y los indicadores de ataque. Si McAfee Advanced Threat Defense califica un archivo como malicioso, McAfee Threat Intelligence Exchange pone inmediatamente la información sobre la amenaza a disposición de todas las medidas de seguridad integradas en la empresa mediante una actualización de reputación.

Los endpoints que tienen McAfee Threat Intelligence Exchange activado pueden bloquear la instalación del malware, lo que evita que se conviertan en el "paciente cero", y ofrecen protección proactiva si el archivo aparece en el futuro. Por su parte, los gateways que funcionan con McAfee Threat Intelligence Exchange pueden evitar que el archivo entre en la organización. Además, los endpoints siguen recibiendo información sobre archivos sospechosos aun estando desconectados de la red, lo que elimina los ángulos muertos cuando la carga útil se distribuye fuera de banda.

McAfee Advanced Threat Defense Email Connector permite a McAfee Advanced Threat Defense recibir adjuntos de correo electrónico para su análisis desde un gateway de correo electrónico. McAfee Advanced Threat Defense analiza los archivos de los adjuntos y devuelve un veredicto al gateway de correo electrónico incluido en el encabezado

del mensaje. A continuación, el gateway de correo electrónico puede realizar una acción basada en las directivas, como eliminar o poner en cuarentena el adjunto, para evitar que el malware infecte y se propague por la red interna.

Búsqueda y corrección de los sistemas afectados

Para corregir un ataque, las organizaciones necesitan una total visibilidad e información práctica por prioridades para tomar mejores decisiones y responder convenientemente. Las soluciones de McAfee trabajan de manera conjunta para proporcionar a las organizaciones exactamente lo que necesitan.

McAfee Enterprise Security Manager recibe y correlaciona los eventos de ejecución y reputación de archivos que envían McAfee Advanced Threat Defense y otros sistemas de seguridad para proporcionar alertas avanzadas y vistas históricas con las que mejorar los datos de seguridad, clasificar los riesgos y conocer la situación en tiempo real. Basándose en los datos de indicadores de peligro de McAfee Advanced Threat Defense, McAfee Enterprise Security Manager realiza una búsqueda retrospectiva de 6 meses para localizar estos componentes entre los datos de redes o sistemas que haya recopilado. De esta forma es capaz de descubrir sistemas que se han comunicado previamente con fuentes de malware recién identificadas. McAfee Enterprise Security Manager permite comprender claramente el riesgo e iniciar acciones correctivas inmediatas, ya sean interactivas o automáticas. La estrecha interacción entre McAfee Endpoint Protection, McAfee Threat Intelligence Exchange y McAfee Active Response optimiza la respuesta y la eficacia de las operaciones de seguridad con visibilidad y con acciones que puedan reducir el riesgo proactivamente, como publicar nuevas configuraciones, implementar nuevas directivas, eliminar archivos o desplegar actualizaciones de software. McAfee Active Response identifica automáticamente endpoints infectados en la red y se incluyen en los informes de McAfee Advanced Threat Defense, lo que facilita la adopción de la acción adecuada.

Despliegue

Opciones de despliegue de análisis de amenazas avanzadas flexibles para todas las redes. McAfee Advanced Threat Defense está disponible como dispositivo in situ o con factor de forma virtual. Todos los factores de forma actúan como recurso compartido entre varias soluciones de seguridad de McAfee, adaptándose en toda la red de forma rentable y reduciendo costes.

Los centros de operaciones de seguridad y los analistas de malware también pueden utilizar McAfee Advanced Threat Defense para tareas de investigación.

La solución ofrece las siguientes funciones avanzadas:

- Sistema operativo configurable y compatibilidad con aplicaciones: imágenes de análisis adaptadas con variables de entorno concretas para verificar las amenazas y facilitar la investigación.
- Modo interactivo de usuario: permite a los analistas interactuar directamente con las muestras de malware.
- Gran número de funciones de descompresión: reduce el tiempo de investigación de días a minutos.
- Ruta lógica completa: permite un análisis de muestras más profundo al forzar la ejecución de rutas lógicas adicionales que permanecen inactivas en entornos aislados típicos.
- Envío de muestras a varios entornos visuales: acelera la investigación determinando las variables de entorno necesarias para la ejecución de archivos.
- Informes detallados con resultados desglosados y volcados de memoria, representaciones gráficas de llamadas a función, información sobre archivos incrustados o distribuidos, registros API de usuario y datos PCAP: proporcionan datos cruciales para la investigación de los analistas.

Si desea obtener más información o iniciar una evaluación de McAfee Advanced Threat Defense, póngase en contacto con su representante o visite **www.mcafee.com/es/products/advanced-threat-defense.aspx**.

Especificaciones de McAfee Advanced Threat Defense		
Factor de forma físico	ATD-3100 Montaje en bastidor (1 unidad)	ATD-6100 Montaje en bastidor (1 unidad)
Factor de forma virtual	v1008, v1016, v3032, v6064 ESXi 5.5, 6.0	v1008, v1016, v3032, v6064 ESXi 5.5, 6.0
Detección		
Tipos de archivos admitidos	Archivos PE, archivos Adobe, archivos de la suite Microsoft Office, archivos de imagen, archivos comprimidos, Java, paquetes de aplicaciones Android, URL	
Métodos de análisis	McAfee Anti-Malware Engine, reputación de McAfee GTI (archivo/URL/IP), Gateway Anti-Malware (emulación y análisis basado en comportamiento), análisis dinámico (entornos aislados), análisis en profundidad de código, reglas YARA personalizadas, aprendizaje automático: red neuronal profunda.	
Sistemas operativos admitidos	Windows 10 (64 bits), Windows 8.1 (64 bits), Windows 8 (32/64 bits), Windows 7 (32/64 bits), Windows XP (32/64 bits), Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003, Android Compatibilidad con los sistemas operativos Windows disponible en todos los idiomas.	
Formatos de salida	STIX, OpenIOC, XML, JSON, HTML, PDF, texto	
Métodos de envío	Integraciones de productos individuales, API RESTful, envíos manuales y McAfee Threat Defense Email Connector (SMTP)	

McAfee
Together is power.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/es

JUNIO DE 2017