McAfee Threat Intelligence Exchange

Compartir la información sobre amenazas para luchar contra los ataques avanzados

McAfee® Threat Intelligence Exchange facilita una detección de amenazas y una respuesta adaptables, gracias al empleo de la información adquirida en tiempo real en sus soluciones de seguridad para endpoints, gateways, redes y centro de datos. La combinación los datos sobre amenazas globales importados con la información recopilada de forma local, así como la capacidad para compartir dicha información de forma instantánea permite a sus soluciones de seguridad funcionar como una sola, intercambiando los datos compartidos y actuando en función de ellos. McAfee Threat Intelligence Exchange reduce a milisegundos el intervalo de días, semanas y meses que suele haber entre detección y contención.

Ventajas principales

- La protección adaptable contra amenazas reduce a milisegundos el intervalo de días, semanas y meses que suele haber entre la detección y la contención de los ataques selectivos avanzados.
- La información colectiva sobre amenazas se genera a partir de fuentes de datos globales y se combina con información sobre amenazas local.
- De esta forma obtiene una visibilidad inmediata de la presencia de ataques selectivos avanzados en la empresa.
- La información de seguridad relevante se comparte en tiempo real entre soluciones de seguridad para endpoints, gateways, redes y centros de datos.

Cree un ecosistema de información sobre amenazas colaborativo

McAfee Threat Intelligence Exchange emplea McAfee Data Exchange Layer para compartir información y ofrecer seguridad integrada. Las aportaciones combinadas de varias fuentes de información sobre amenazas se comparte de manera instantánea con todas sus soluciones de seguridad conectadas, incluidas las de terceros.

Cuando los componentes de seguridad funcionan como uno, la información relevante para la detección y protección contra amenazas se comparte inmediatamente entre las soluciones de seguridad para endpoints, gateways, centros de datos, la nube y otros puntos de control de seguridad de su entorno. La simplicidad de integración, gracias a McAfee Data Exchange Layer, reduce de manera importante los costes operativos y de implementación, y proporciona una seguridad, una eficacia operativa y una efectividad inigualables.

Diseñada como plataforma abierta, McAfee Data Exchange Layer permite incorporar de manera dinámica al ecosistema McAfee Threat Intelligence Exchange todas las soluciones de seguridad, incluidas las de terceros. El coste total de propiedad disminuye, y usted está mejor equipado para aprovechar el valor de sus soluciones de seguridad actuales y sus inversiones en seguridad, gracias a que sus componentes de seguridad están totalmente comunicados entre sí.

La prevención de amenazas colaborativa y adaptable constituye un enfoque totalmente nuevo de la seguridad de TI a nivel empresarial, que unifica sistemas diferentes con el fin de proporcionar una verdadera coordinación de la seguridad. Para los equipos de seguridad es imprescindible tener la posibilidad de automatizar el mecanismo para compartir la información sobre amenazas y aplicar protecciones y directivas de prevención de forma proactiva a todos los puntos de su red, a fin de eliminar las barreras de las fronteras empresariales y presupuestarias.

intel Security

Ventajas principales (continuación)

- Podrá decidir qué hacer con archivos nunca vistos anteriormente en función del contexto de los endpoints (atributos de archivo, proceso y entorno) con la información colectiva sobre amenazas.
- La integración es sencilla a través de McAfee Data Exchange Layer. Se reducen los costes operativos gracias a la conexión de soluciones de seguridad de Intel Security con otras propiedad de terceros a fin de aplicar su información sobre amenazas en tiempo real.

Al transformar la infraestructura de seguridad en un sistema de colaboración, los administradores de seguridad pueden detectar, compartir e inmunizar su entorno frente a las amenazas. McAfee Threat Intelligence Exchange aumenta significativamente la resiliencia y el control en la batalla contra los ataques selectivos nuevos y emergentes.

Adáptese e inmunícese frente a las amenazas

Cada vez que se comparte información, sea cual sea la ubicación de la red, mejora su situación en la batalla que se libra contra los ataques selectivos. Estas amenazas son ataques diseñados con precisión milimétrica, por lo que las empresas requieren un sistema de vigilancia local para descubrir las tendencias generales y las agresiones dirigidas exclusivamente a ellas. Los datos contextuales locales obtenidos del intercambio, combinados con la información global sobre amenazas, permiten tomar mejores decisiones sobre archivos desconocidos hasta el momento, lo que agiliza la protección y detección.

McAfee Threat Intelligence Exchange evalúa de forma local todos los archivos no identificados que se encuentren en su red. Según los resultados, la protección se propaga a todos los sistemas en tiempo real. Esta información local sobre amenazas se almacena para el futuro, lo que significa que si se vuelven a detectar en otro dispositivo o servidor, ya no serán archivos desconocidos, y el ataque será detectado inmediatamente.

Por ejemplo, la información sobre un archivo malicioso encontrado en su gateway se envía a través de McAfee Data Exchange Layer a McAfee Threat Intelligence Exchange, y llega en milisegundos a sus endpoints y su centro de datos, para que dispongan de la información necesaria para inmunizarse de manera proactiva contra esta amenaza. Todo intento de ataque que se bloquee en un endpoint indica la presencia de malware, y esta información se comparte de manera instantánea con el gateway y otros componentes de seguridad, lo que permite blindar el perímetro frente a la amenaza.

Aproveche la información sobre amenazas en tiempo real

Ahora puede combinar la información sobre amenazas procedente de fuentes a nivel mundial importadas, como McAfee Global Threat Intelligence (McAfee GTI), con datos obtenidos de indicadores de riesgo (IOC) compartidos, como archivos Structured Threat Information eXpression (STIX). McAfee Global Threat Intelligence recopila datos en tiempo real e históricos locales de los endpoints, el centro de datos, los gateways, su red y la solución de entorno aislado (sandboxing) McAfee Advanced Threat Defense. Estos datos de amenazas globales y locales combinados se aplican y se comparten en tiempo real en todo el ecosistema de seguridad.

Con McAfee Threat Intelligence Exchange, los administradores pueden adaptar fácilmente la información exhaustiva sobre amenazas que reciben de las fuentes de datos globales, como McAfee GTI, datos de terceros y archivos STIX importados. Esto se combina con información sobre amenazas local procedente de datos en tiempo real e históricos de los endpoints, los gateways, las soluciones de entorno aislado y otros componentes de seguridad. Los administradores de seguridad tienen la posibilidad de reunir, omitir, sumar y adaptar la información con el fin de personalizar la protección según su entorno y su empresa (por ejemplo, listas negras y blancas de archivos o certificados asignados y utilizados por una empresa).

Esta información adaptada y con prioridades asignadas localmente proporciona una respuesta instantánea en caso de detecciones en el futuro. Además, se guardan metadatos descriptivos sobre los principales objetos y se reflejan en la información colectiva recopilada. Según esta información, en función de la actividad maliciosa del pasado,

Los ataques avanzados son un problema del mundo real

Diseñados para eludir los radares y establecer su presencia a largo plazo con el fin de extraer datos de gran valor, los ataques selectivos avanzados continúan asediando a las organizaciones. Según datos recientemente publicados como parte del *informe sobre investigaciones sobre amenazas de Verizon de 2015 (Verizon 2015 Data Breach and Investigations Report)* entre el 70 y el 90 % de las muestras de malware son exclusivas para una sola empresa, lo que indica que la detección de indicadores de amenazas exclusivos es el mayor de los retos actuales[1].

Para obtener más información, visite **www.mcafee.com/es/products/threat-intelligence-exchange.aspx**.

los administradores y los productos de administración de información y eventos de seguridad (SIEM) pueden colaborar para identificar al instante los sistemas con mayor probabilidad de ser atacados.

Consiga protección de última generación para los endpoints

McAfee Threat Intelligence Exchange ofrece una innovadora protección a los endpoints mediante el uso del módulo VirusScan Enterprise de McAfee Threat Intelligence Exchange. Utilizando reglas configurables, este módulo toma decisiones precisas de ejecución de archivos y emplea la información contextual combinada que le llega del contexto de los endpoints locales (atributos de archivo, proceso y entorno) con la información colectiva sobre amenazas disponible en ese momento (por ejemplo, prevalencia empresarial, antigüedad, reputación, etc.).

Cuando el módulo VirusScan Enterprise de McAfee Threat Intelligence Exchange se personaliza de acuerdo con el nivel de tolerancia a riesgos de los endpoints de la empresa, los administradores tienen flexibilidad para definir las condiciones de ejecución a partir de sus requisitos específicos. Las condiciones pueden ser todo lo rígidas que se desee, como una política de tolerancia cero frente a los archivos desconocidos o "inciertos" compuesta por normas que no permitan el acceso a ningún archivo a menos que su reputación sea conocida y aceptable.

Gestione los endpoints en cualquier momento y en cualquier lugar

McAfee Threat Intelligence Exchange ofrece una prevención adaptable contra amenazas y una administración de seguridad de alcance mundial. Llega a los endpoints estén donde estén y proporciona el medio de administrar las directivas y detecciones de amenazas, así como las actualizaciones y la investigación remota sobre la seguridad. Los componentes de seguridad funcionan como una unidad, sean cuales sean las fronteras físicas. Comparten inmediatamente los datos de seguridad relevantes entre endpoints, gateways y otros productos de seguridad —al margen de su ubicación—, lo que permite que la prevención de amenazas sea adaptable.

Las demás soluciones de administración de seguridad son incapaces de introducir de forma inmediata en los endpoints cambios de directivas, contenido y actualizaciones de programas, lo que deja abierta la ventana cuando las empresas se exponen a riesgos mayores. Al utilizar McAfee Data Exchange Layer, McAfee Threat Intelligence Exchange puede mantener una conexión continua a pesar de los obstáculos que haya en la red y, de este modo, cierra eficazmente esta brecha de seguridad y garantiza la inclusión de todos los endpoints.

Benefíciese de la colaboración

Consulta de reputación con un solo clic

Cuando un componente de seguridad de una empresa —gateway, endpoint o red— encuentra un archivo desconocido, es fácil averiguar su reputación en función de atributos y de información sobre amenazas combinada de la que dispone.

Análisis de amenazas avanzadas

Si se requiere más información sobre un archivo, puede enviarse automáticamente desde McAfee Threat Intelligence Exchange a McAfee Advanced Threat Defense para obtener información instantánea sobre las nuevas amenazas potenciales. Juntos, aprovechan el análisis de amenazas, ya sea análisis de código estático o dinámico, para definir la reputación del archivo en cuestión. Todo ello está automatizado y se documenta y comparte colectivamente a través de McAfee Data Exchange Layer a fin de proteger todo su ecosistema de seguridad.

Gestión de incidentes de seguridad

McAfee Enterprise Security Manager le permite investigar más a fondo los indicadores de riesgo que detecta McAfee Threat Intelligence Exchange. El acceso a la información de seguridad histórica y la posibilidad de crear listas de seguimiento automatizadas incrementan la eficacia de la seguridad en las empresas.

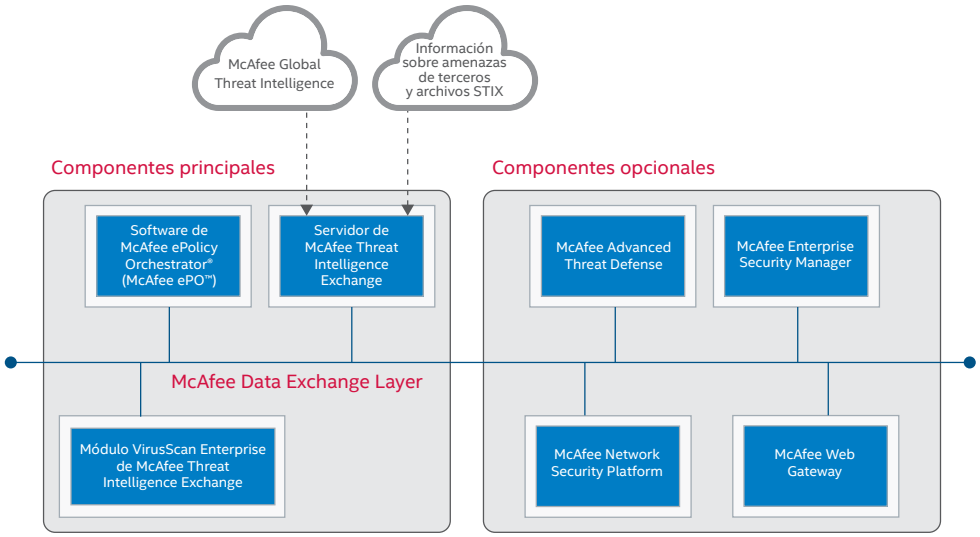

Figura 1. La facilidad de integración, posible a través de McAfee Data Exchange Layer, reduce los costes de implementación y operativos, y proporciona una eficacia de funcionamiento inigualable que favorece la evolución de la plataforma Security Connected.

1. http://www.verizonenterprise.com/DBIR/2015/

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com

62276ds_threat-intelligence-exchange_0216