Resumen de la Solución

Seguridad en conjunto

La inteligencia adaptable le permite responder inmediatamente ante las amenazas emergentes.

Las organizaciones enfrentan diversos desafíos operativos y de seguridad a medida que intentan montar una defensa eficaz contra las amenazas emergentes de la actualidad. Los ataques dirigidos avanzados y de día cero utilizan cargas útiles nunca antes vistas. Las amenazas polimórficas de malware también presentan desafíos similares. Por sí mismas, las contramedidas tradicionales y basadas en firma tienen dificultades para detectar las cargas avanzadas de malware.

Para combatir eficazmente las amenazas emergentes, las organizaciones necesitan un sistema de seguridad que proporcione una combinación de capacidades de evaluación basada en el comportamiento, la reputación y las firmas, tanto en la red como en los endpoints. Mientras cada una de estas capas de tecnología son eficaces para identificar amenazas de manera individual, es importante que funcionen en conjunto para compartir información, obtener más conocimientos y adaptarse en conjunto con el fin de enfrentar las amenazas en evolución. Las comunicaciones manuales entre las soluciones de red y de endpoints requieren mucho tiempo y simplemente no son lo suficientemente rápidas para contrarrestar las amenazas actuales.

McAfee® Threat Intelligence Exchange y McAfee Advanced Threat Defense funcionan en conjunto para entregar una protección adaptable y automatizada frente a las amenazas emergentes. Sin importar cuál es el primer punto de contacto de un archivo desconocido de malware, una vez que se sanciona al archivo, todo el entorno conectado se actualiza de inmediato. Si McAfee Advanced Threat Defense detecta a un archivo, McAfee Threat Intelligence Exchange comparte dicha sanción con todas las contramedidas de la organización a través de una actualización de la reputación mediante la capa de intercambio de datos (DXL – data exchange layer). Los endpoints que cuentan con McAfee Threat Intelligence Exchange poseen una protección proactiva, en caso de que el archivo vuelva a aparecer en el futuro. Los gateways que cuentan con McAfee Threat Intelligence Exchange impiden que el archivo ingrese a la organización. Asimismo, cuando los endpoints que cuentan con McAfee Threat Intelligence Exchange detectan archivos con reputaciones desconocidas, los envían a McAfee Advanced Threat Defense para determinar si el objeto es malicioso. De este modo se eliminan los puntos ciegos de la distribución de cargas útiles fuera de banda.

Cierre la brecha de exposición

Detecte las cargas de malware

McAfee Threat Intelligence Exchange y McAfee Advanced Threat Defense funcionan en conjunto para analizar objetos sospechosos, sin importar cuál es el primer punto de contacto. Cuando se intentan ejecutar archivos nuevos, estos deben estar sujetos a la combinación de reglas de endpoint, los conocimientos de reputación global y del entorno y el análisis estático y dinámico en profundidad de los componentes conectados de esta solución de colaboración. Este enfoque conectado para el análisis de amenazas proporciona una detección más precisa del malware oculto que de otro modo podría pasar desapercibido.

Beneficios clave

- Reduzca significativamente el tiempo de contención a través de una respuesta ante amenazas automatizada y adaptable.
- Obtenga mayor visibilidad, agilidad y control mediante la colaboración de la red al endpoint.
- Responda inteligentemente ante las detecciones mediante la reputación de archivos y el conocimiento de ejecución definitivos.
- Mejore la seguridad al tiempo que optimiza el costo total de propiedad (TCO) gracias a la integración e implementación simplificadas.

intel Security

Aumente la detección de amenazas con el análisis de amenazas basado en el comportamiento
McAfee Advanced Threat Defense ofrece una clasificación de la reputación con capacidades innovadoras de desmantelamiento de malware, incluido un poderoso "desempaquetado" que pasa por las técnicas de evasión para revelar el código ejecutable original con el fin de determinar el comportamiento deseado. En conjunto, el análisis estático y dinámico del código proporciona una evaluación completa y representa la tecnología de detección de amenazas más avanzada del mercado.

Obtenga visibilidad y control desde el endpoint hasta la red
McAfee Advanced Threat Defense también recibe muestras de malware que otros productos de su entorno recopilan en los puntos de ingreso a la red. Por su parte, estos componentes de la red pueden compartir con McAfee Threat Intelligence Exchange la nueva inteligencia que se recopila a partir de estas muestras. Dicha inteligencia y el uso compartido de la reputación demuestran el aprovechamiento de la plataforma Security Connected de McAfee del endpoint a la red. Asimismo, McAfee Threat Intelligence Exchange mantiene una base de conocimientos que indica dónde se ejecutaron los últimos objetos del entorno del endpoint para proporcionar una visibilidad definitiva de las detecciones.

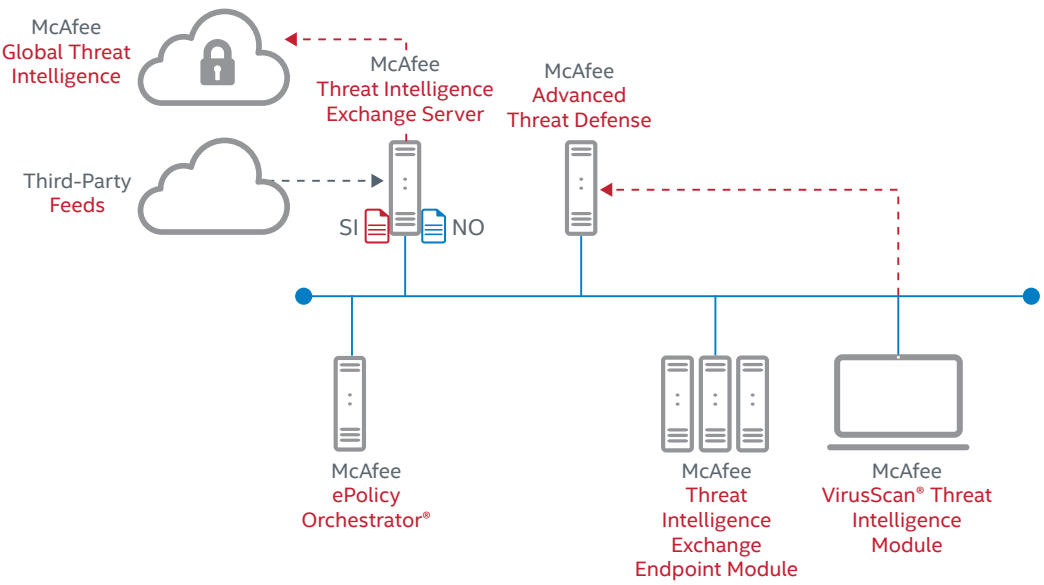

Figura 1. de la inteligencia y la reputación de la nube, la red y el endpoint.

Respuesta adaptable

Una vez que McAfee Advanced Threat Defense analiza y clasifica un archivo, los resultados se envían a McAfee Threat Intelligence Exchange. La reputación del nuevo archivo, ya sea buena o mala, se publica instantáneamente en todas las respuestas compatibles con McAfee Threat Intelligence Exchange del entorno. Se detectará cualquier instancia futura del archivo y todos los componentes compatibles con McAfee Threat Intelligence Exchange responderán de acuerdo con la política para autorizar, bloquear o limpiar el archivo. Esta respuesta adaptable proporciona protección instantánea en todo el entorno, incluida la red, el gateway y los componentes de endpoint. Se produce un aumento en la agilidad de las respuestas a la vez que disminuye significativamente el tiempo para la contención y la corrección, todo ello sin la necesidad de reestructurar la red.

Cómo habilitar Security Connected en McAfee Data Exchange Layer

McAfee Threat Intelligence Exchange es la primera solución que usa la capa de intercambio de datos (DXL) de McAfee, una estructura de comunicación bidireccional, liviana y ultrarrápida que habilita la inteligencia de seguridad y la seguridad adaptable a través de la integración de productos y el contexto compartido. Los productos conectados con DXL de McAfee simplemente se suscriben y publican información a la estructura sin la necesidad de integraciones complejas de interfaz de programación de aplicaciones (API, application programming interface) y configuraciones molestas. Eso marca el comienzo de una nueva era en la seguridad en la cual todos los componentes se combinan para funcionar como un sistema cohesivo.

Implementación y gestión simples

La integración de McAfee Threat Intelligence Exchange y McAfee Advanced Threat Defense en el DXL no tiene interrupciones. DXL ha sido diseñado como un marco abierto y permite que los componentes de seguridad se unan dinámicamente a McAfee Threat Intelligence Exchange sin la necesidad de API extensas o configuraciones complejas de productos, lo que permite reducir la cantidad de errores y eliminar gran parte de los esfuerzos manuales.

Figura 2. Integración sin interrupciones en la capa de intercambio de datos (DXL) a través de Security Connected.

Más información

McAfee Threat Intelligence Exchange y McAfee Advanced Threat Defense son fundamentales para conectar componentes de seguridad diferentes, lo que permite proteger el entorno, responder ante las detecciones y adaptarse automáticamente a las amenazas emergentes. Mediante la oferta de un ecosistema que integra análisis de amenazas avanzadas, productos de red y soluciones de endpoint, McAfee proporciona visibilidad en toda la organización y contexto para las amenazas a la vez que reduce los tiempos de respuesta y simplifica la corrección.

http://www.mcafee.com/TIE

http://www.mcafee.com/ATD

http://www.mcafee.com/securityconnected

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com