Resumen de la solución

Seguridad al unísono

La información adaptable le permite responder inmediatamente a las amenazas emergentes.

A la hora de organizar una defensa eficaz contra las amenazas emergentes actuales las empresas deben superar varias dificultades de carácter operativo y de seguridad. Los ataques selectivos avanzados y de tipo zero-day emplean cargas útiles nunca vistas hasta la fecha. Y las amenazas de malware polimórfico también plantean retos similares. Por sí solas, las medidas tradicionales basadas en firmas tienen dificultades a la hora de detectar las cargas útiles del malware avanzado.

Para combatir eficazmente las amenazas emergentes, las empresas necesitan un sistema de seguridad que ofrezca una combinación de funciones de evaluación basadas en el comportamiento, la reputación y las firmas, tanto en la red como en los endpoints. Si bien cada una de estas tecnologías podría ser eficaz en la identificación de amenazas de manera individual, para hacer frente a las amenazas en constante evolución es importante que actúen de manera conjunta para compartir información, adquirir conocimiento y adaptarse al unísono. Las comunicaciones manuales entre las soluciones para la red y los endpoints sencillamente no son lo bastante rápidas para contrarrestar las amenazas actuales.

McAfee® Threat Intelligence Exchange y McAfee Advanced Threat Defense colaboran para proporcionar protección automatizada y adaptable frente a las amenazas emergentes. Independientemente de cuál sea el primer punto de contacto de un archivo de malware desconocido, una vez detectado, todo el entorno conectado se actualiza inmediatamente. 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 a través de la capa de intercambio de datos. Si el archivo aparece de nuevo en el futuro, los endpoints que tienen activada McAfee Threat Intelligence Exchange dispondrán de protección proactiva. Por su parte, los gateways con McAfee Threat Intelligence Exchange evitan que el archivo entre en la empresa. Además, cuando los endpoints con McAfee Threat Intelligence Exchange encuentran archivos con reputación desconocida, los envían a McAfee Advanced Threat Defense para determinar si el objeto es malicioso, lo que elimina los ángulos muertos cuando la carga útil de distribuye fuera de banda.

Cierre la brecha en la seguridad

Identifique las cargas útiles de malware sigiloso.

McAfee Threat Intelligence Exchange y McAfee Advanced Threat Defense colaboran para analizar objetos sospechosos, independientemente de cuál sea el primer punto de contacto. Cuando se intentan ejecutar nuevos archivos, se les aplican las reglas para endpoints combinadas, la información sobre reputación global y del entorno, así como un profundo análisis dinámico y estático de los componentes conectados en esta solución de colaboración. Este análisis conectado de las amenazas garantiza una identificación más precisa del malware sigiloso que de otra forma pasaría desapercibido.

Principales ventajas

- Reduzca drásticamente el tiempo necesario para la contención mediante una respuesta a amenazas automatizada y adaptable.
- Consiga mayor visibilidad, agilidad y control a través de la colaboración entre la red y los endpoints.
- Responda de manera inteligente a los incidentes con información concluyente sobre la reputación y la ejecución de los archivos.
- Mejore la seguridad y al mismo tiempo optimice el coste total de propiedad gracias a la integración y la implementación simplificadas.

intel Security

Mejore la detección de amenazas gracias al análisis basado en el comportamiento.
McAfee Advanced Threat Defense ofrece clasificación de reputación con innovadoras funciones de deconstrucción de malware. Entre ellas se incluye un potente sistema de descompresión que desmonta las técnicas de evasión, a fin de identificar el código del ejecutable original para determinar el comportamiento previsto. Juntos, los análisis del código estático y dinámico proporcionan una completa evaluación y representan la tecnología de detección de amenazas avanzadas más robusta del sector.

Consiga visibilidad y control, desde el endpoint a la red.
McAfee Advanced Threat Defense recibe también muestras de malware recopiladas en puntos de entrada a la red por otros productos de su entorno. Estos componentes de red pueden a su vez compartir la información extraída de estas muestras mediante McAfee Threat Intelligence Exchange. Esta capacidad de compartir información y datos de reputación pone de manifiesto las ventajas de la integración de endpoints y redes que ofrece la plataforma Security Connected de McAfee. Además, McAfee Threat Intelligence Exchange mantiene una base de datos de conocimientos que indica dónde se ejecutaron los últimos objetos del entorno de endpoints, a fin de proporcionar una visibilidad concluyente de los incidentes.

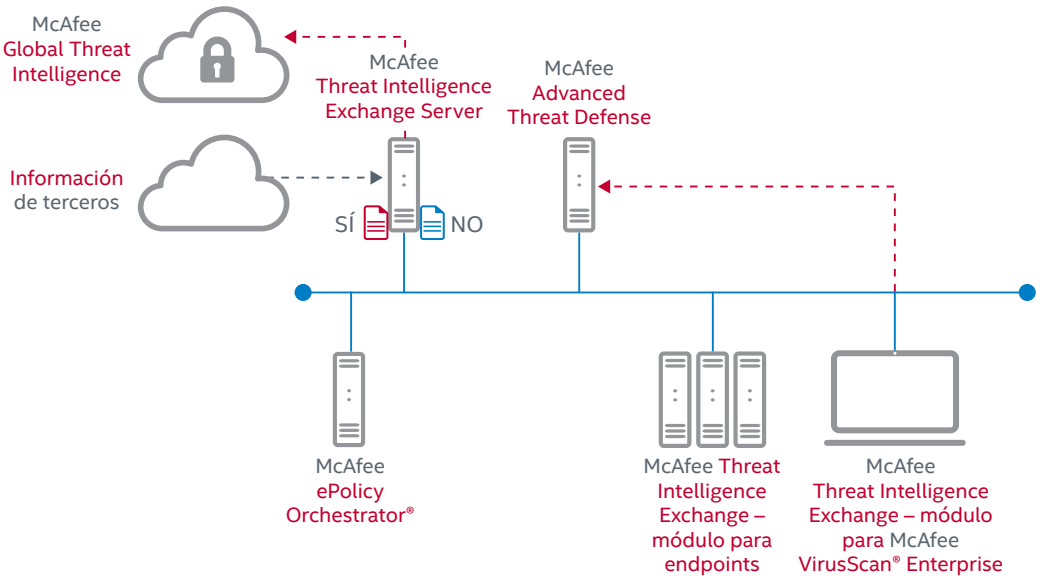

Figura 1. Síntesis de información y reputación de la nube, la red y los endpoints.

McAfee Data Exchange Layer facilita Security Connected

McAfee Threat Intelligence Exchange es la primera solución que utiliza la capa de intercambio de datos de McAfee, Data Exchange Layer, un tejido de comunicación bidireccional, ultrarápido y ligero que proporciona información de seguridad y una protección adaptable mediante la integración de productos y la capacidad para compartir los contextos. Los productos conectados a McAfee Data Exchange Layer solo tienen que suscribirse y publicar en el tejido, sin necesidad de complejas integraciones mediante una interfaz de programación de aplicaciones (API) ni laboriosas configuraciones. Este sistema abre una nueva era en la seguridad en la que todos los componentes se unen para funcionar como un sistema único.

Respuesta adaptable

Una vez que McAfee Advanced Threat Defense analiza y clasifica un archivo, los resultados se envían a McAfee Threat Intelligence Exchange. La nueva reputación del archivo, ya sea buena o mala, se publica al instante en todos los sistemas de McAfee Threat Intelligence Exchange del entorno. Cualquier instancia futura del archivo será identificada, y todos los componentes con McAfee Threat Intelligence Exchange actuarán en función de la directiva para permitir, bloquear o eliminar el archivo. Esta respuesta adaptable ofrece protección instantánea en todo el entorno, incluidos los componentes de red, el gateway y los endpoints. De esta forma, se aumenta la agilidad de las respuestas, al tiempo que se reduce de manera importante el tiempo necesario para la contención y corrección, todo ello sin necesidad de modificar la arquitectura de la red.

Despliegue y administración sencillos

La integración entre McAfee Threat Intelligence Exchange y McAfee Advanced Threat Defense se realiza perfectamente a través de la capa de intercambio de datos. Diseñada como una infraestructura abierta, la capa de intercambio de datos permite que los componentes de seguridad se unan automáticamente a McAfee Threat Intelligence Exchange sin necesidad de complicadas API ni complejas configuraciones de productos, lo que reduce los errores y elimina el importante trabajo manual.

Figura 2. Perfecta integración con la capa de intercambio de datos mediante Security Connected.

Más información

McAfee Threat Intelligence Exchange y McAfee Advanced Threat Defense son fundamentales para conectar distintos componentes de seguridad, proteger su entorno, responder a los incidentes y adaptarse automáticamente a las amenazas emergentes. Gracias al ecosistema de seguridad que integra el análisis avanzado de las amenazas, los productos para la red y las soluciones para los endpoints, McAfee proporciona visibilidad en toda la empresa e información del contexto de las amenazas y, al mismo tiempo, reduce el tiempo de respuesta y simplifica la corrección.

- **www.mcafee.com/es/products/threat-intelligence-exchange.aspx**
- **www.mcafee.com/es/products/advanced-threat-defense.aspx**
- **www.mcafee.com/es/enterprise/security-connected/index.aspx**

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