McAfee Active Response

Detección y respuesta global frente amenazas para endpoints

En la actualidad, las organizaciones son conscientes de la importancia de la seguridad y se enfrentan a amenazas que cambian a un ritmo vertiginoso, y se crean y propagan a velocidades nunca vistas. Los ataques selectivos "de diseño" tienen un objetivo concreto y emplean información específica sobre las empresas elegidas como víctimas para aumentar su eficacia y minimizar las posibilidades de ser detectados. Además, los agresores consiguen sortear con más frecuencia las tecnologías de prevención. Por este motivo, las empresas con visión de futuro demandan herramientas integradas y fáciles de utilizar que faciliten la detección de la presencia de agresores y, a continuación, permitan llevar a cabo la investigación y la corrección con celeridad. Las mejores soluciones de detección y respuesta aumentan la eficacia de la seguridad incluso ahora, cuando cada vez se captura más información de un número cada vez mayor de sistemas. Gracias a sus extraordinarias funciones preconfiguradas y a la interacción automatizada con las soluciones de administración de la seguridad existentes, así como a las funciones de personalización para el usuario, McAfee® Active Response reduce enormemente las oportunidades que tienen los agresores de dañar sus activos informáticos y su marca corporativa.

Las amenazas están en constante evolución

Las empresas ya son conscientes de que pueden sufrir un ataque en cualquier momento y saben que deben estar preparadas para hacer frente de manera eficaz a estos incidentes mediante la detección precoz de los ataques, la identificación de la actividad en curso o el descubrimiento de los indicadores de ataque (IoA). Además, saben que necesitan nuevas tecnologías para suplir las carencias actuales en cuanto a visibilidad, descubrimiento, detección y respuesta.

Limitaciones de los enfoques actuales de respuesta a incidentes

Generalmente, cuando los responsables de la respuesta a incidentes y los administradores de seguridad deben

Ventajas principales

- **Automatización:** conozca y supervise el contexto y el estado de los sistemas para saber si se producen cambios que puedan estar asociados a indicadores de ataque. Además, identifique componentes del ataque que estén en estado latente y envíe información a los equipos de análisis, operaciones e investigación forense.
- **Adaptabilidad:** cuando reciba una alerta, puede realizar ajustes según los cambios en las metodologías de ataque; automatizar la recopilación de datos, alertas y respuestas según los temas de interés; y personalizar sus configuraciones en función de los flujos de trabajo de los clientes.
- **Continuidad:** los recopiladores continuos ponen en marcha activadores cuando se detectan incidentes relacionados con un ataque, para avisarle a usted y a sus sistemas de que se ha observado actividad de ataque.

investigar un incidente sospechoso o conocido en toda la organización, se enfrentan a dos problemas principales: el tiempo y la escala. Aunque los sistemas y herramientas existentes recaban una gran cantidad de información detallada, se necesita mucho tiempo para reunirla y analizarla. La velocidad es fundamental a la hora de recopilar los datos, por lo que en ocasiones se deben realizar concesiones importantes en cuanto a la naturaleza de los datos recopilados y al número de sistemas desde los que se recopilan. Además, cada vez es más difícil procesar la ingente cantidad de datos recopilados con el fin de identificar la información clave.

Las herramientas de respuesta a incidentes más utilizadas son secuencias de comandos desarrolladas por los propios responsables de la respuesta a incidentes. Estas herramientas proporcionan la base de datos que se va a utilizar en otros análisis a mayor escala. A pesar de que este corpus de datos, junto con las herramientas asociadas, es bastante completo, las posibilidades de aprovecharlo a la velocidad y escala adecuadas son limitadas. Esta incapacidad para llevar a cabo una investigación en tiempo real de algunos indicadores de ataque específicos en toda la empresa ofrece a menudo a los responsables una visión limitada que afecta a sus esfuerzos de descubrimiento y respuesta. Es habitual que estos esfuerzos sufran de manera artificial las limitaciones de tiempo y esto puede generar lagunas importantes en el proceso de respuesta a incidentes. Esta circunstancia perjudica gravemente a los responsables de la respuesta a incidentes, ya que se ven limitados debido a exigencias de las herramientas actuales.

Detección y respuesta integral frente a amenazas para endpoints

McAfee Active Response facilita la detección y respuesta a amenazas de seguridad avanzadas de manera continua, para ayudar a los profesionales de la seguridad a supervisar el estado de su seguridad, mejorar la detección de amenazas y ampliar la respuesta a incidentes gracias al descubrimiento orientado al futuro, el análisis detallado, la investigación forense, la generación de informes completos, y las alertas y acciones por prioridades. Optimizada para satisfacer los rigurosos criterios de respuesta y detección de incidentes de los endpoints, McAfee Active Response emplea recopiladores predefinidos y personalizables por el usuario para buscar a fondo en todos los sistemas y conseguir detectar indicadores de ataque no solo en los procesos en ejecución, sino también en los que están en estado latente o han sido eliminados. Además, McAfee Active Response no solo permite a los usuarios buscar indicadores de ataque en el presente, sino que también podrán alertar y actuar de acuerdo a sus objetivos de seguridad por medio de activadores que dan instrucciones si el indicador de ataque se detecta de nuevo en el futuro.

McAfee Active Response es la prueba palpable de la eficacia de la arquitectura de seguridad integrada de McAfee, ya que está diseñada para solucionar más amenazas, de manera más rápida, y con menos recursos en un mundo cada vez más complejo. Le ofrece visibilidad continua y un conocimiento eficaz de sus endpoints para que pueda identificar

Requisitos del sistema

Requisitos mínimos de hardware
En caso necesario, el servidor puede instalarse en una máquina virtual. Los requisitos de mínimos de hardware recomendados para el servidor de McAfee Active Response son los siguientes:

- 4 CPU Intel Xeon X5675, 3,07 GHz
- 8 GB de RAM
- 120 GB de disco en estado sólido

Infraestructura de servicio necesaria

- McAfee ePO 5.1.1 o posterior
- Extensión McAfee Agent 5.0 o posterior
- Agente Data Exchange Layer 2.0.0.405 o posterior

Navegadores web admitidos

- Microsoft Internet Explorer 9 o posterior
- Google Chrome 17 o posterior
- Mozilla Firefox 10.0 o posterior

Infraestructura cliente necesaria

- McAfee Agent 5.0.0.2710 o posterior para endpoints Linux
- McAfee Agent 5.0.0.2610 o posterior para endpoints Windows
- Agente Data Exchange Layer 2.0.0.405 o posterior en todos los endpoints gestionados

los ataques más rápidamente. Asimismo, le proporciona las herramientas que necesita para corregir los problemas con mayor rapidez y de la manera más conveniente para su negocio. Todo esto se administra a través del software McAfee® ePolicy Orchestrator® (McAfee ePO™), que aprovecha la capa de intercambio de datos Data Exchange Layer, que ofrece escalabilidad y capacidad de ampliación sin necesidad de aumentar el personal para administrar el producto.

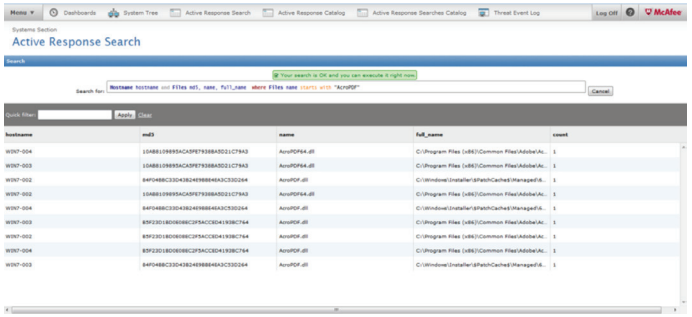

Figura 1. Interfaz de usuario de búsqueda de McAfee Active Response.

Función	Ventaja	Ventajas para los clientes	Diferenciación
Recopiladores	Los recopiladores permiten a los usuarios encontrar y visualizar datos de sus sistemas.	Ofrecen funciones de búsqueda para examinar los sistemas a fondo. Permiten detectar fugas o ataques críticos potenciales para poder recopilar y examinar datos de esos sistemas. Con la ayuda de varios lenguajes de secuencias de comandos habituales, los usuarios pueden personalizar fácilmente sus propios recopiladores y respuestas, lo que facilita al máximo la capacidad de configuración y adaptación.	McAfee Active Response no solo busca archivos ejecutables y en ejecución, sino que también identifica el código que puede estar latente o incluso que puede haber sido eliminado en un intento de borrar el rastro del agresor. McAfee Active Response puede realizar búsquedas en archivos, flujos de red, el Registro y mapas de procesos.
Activadores	Los activadores permiten a los profesionales de la seguridad supervisar de manera continua un evento o un cambio de estado crítico con un conjunto de instrucciones para el presente y para el futuro.	Las acciones se inician mediante un activador definido previamente, que genera un evento o ejecuta respuestas. McAfee Active Response no se limita a controlar los "picos" estáticos y actúa en modo de respuesta continua.	Puede ver las amenazas hoy y poner en marcha acciones para otras que puedan surgir en el futuro.
Reacciones	Las reacciones proporcionan acciones preconfiguradas y personalizables que se desencadenan cuando se cumplen las condiciones del activador, lo que facilita el seguimiento y la erradicación de las amenazas.	Las reacciones permiten a los usuarios tomar medidas; por ejemplo, buscar archivos que han sido eliminados del sistema por código hash (MD5 y SHA1), descubrir si hay hosts conectados de forma activa a una dirección IP o si se han conectado a una dirección IP en el pasado, o buscar un archivo malicioso no PE al que no se haya accedido o que no se haya "detonado" en el sistema (es decir, buscar un archivo PDF malicioso que se ha copiado en el sistema de archivos pero que no se ha abierto nunca).	La solución McAfee Active Response está preconfigurada para actuar en función de los resultados de las búsquedas y acepta las acciones personalizadas que determina el usuario para satisfacer una necesidad específica.

Requisitos del sistema (continuación)

Sistemas operativos cliente admitidos

- Microsoft Windows
  - Windows 8.0, Base, 32 y 64 bits
  - Windows 8.1, Base, U1; 32 y 64 bits
  - Windows Server 2012 Base R2; U1; 64 bits
  - Windows Server 2008 R2 Enterprise, SP1, 64 bits
  - Windows Server 2008 R2 Standard, SP1, 64 bits
  - Windows 7 Enterprise, hasta el SP1; 32 y 64 bits
  - Windows 7 Professional, hasta el SP1; 32 y 64 bits
- CentOS 6.5, 32 bits
- RedHat 6.5 de 32 bits

Función	Ventaja	Ventajas para los clientes	Diferenciación
Administración centralizada con el software McAfee ePO	El entorno con una sola consola facilita la administración y automatización globales.	Los administradores pueden aprovechar el software de McAfee ePO como parte de la arquitectura de seguridad integrada de McAfee para generar respuestas automatizadas para los activadores y las búsquedas, y responder y mitigar las amenazas. La administración desde un solo panel ofrece mayor visibilidad de la seguridad sin aumentar la carga de trabajo administrativo. Esto simplifica los aspectos operativos y la inversión de tiempo necesario para el personal de administración.	La administración y la capacidad de actuación de manera centralizada es un claro factor diferenciador. Gracias al uso de una única consola, protegemos de manera exclusiva una amplia variedad de plataformas con un potente conjunto de controles de seguridad, incluido McAfee Active Response.
Arquitectura de seguridad integrada	Emplea Data Exchange Layer para facilitar la comunicación con otros productos de McAfee.	Como parte de la arquitectura de seguridad integrada de McAfee, McAfee Active Response reduce los riesgos y el tiempo de respuesta, y minimiza los costos indirectos y de personal gracias a los conceptos innovadores, los procesos optimizados y las recomendaciones prácticas que ofrece la plataforma.	

Más información

Para obtener más información sobre las ventajas de McAfee Active Response, visite **www.mcafee.com/mx/products/active-response.aspx**.

Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
+52-55-50890250
www.mcafee.com/mx