Resumen de la Solución

Monitoree continuamente. Responda rápidamente.

McAfee® Active Response mejora la detección y corrección ATA.

Todos los días durante el año pasado, 2.803.036 registros de datos fueron perdidos o robados como resultado de una violación de datos, y la investigación indica que los números están disparándose a un ritmo alarmante. Las violaciones de datos totalizaron 1.540 el año pasado, un aumento de 46% con respecto al año anterior.[1] La mayoría de las organizaciones preocupadas por la seguridad se están dando cuenta de que las soluciones tradicionales de endpoint de "configurar y olvidarse de ellas" están mal equipadas para manejar el bombardeo diario de día cero y ataques dirigidos avanzados (ATAs). Los equipos de seguridad necesitan visibilidad ininterrumpida hacia la actividad de endpoint, en lugar de limitarse a alertas de productos de seguridad después de que algo ya salió mal. La detección y respuesta de endpoint (EDR) es un complemento indispensable para las defensas actuales. Conforme señala Gartner, “Las organizaciones que invierten en herramientas EDR se están trasladando de una mentalidad de "respuesta a incidentes", hacia una mentalidad de "monitoreo continuo" al buscar incidentes que saben que se presentan continuamente”. [2]

El Déficit de Defensas en la Mayoría de las Soluciones de Endpoint

En vez de emprender un abordaje proactivo, la mayoría de los equipos de respuesta a incidentes emprenden actualmente un abordaje reactivo. A menudo, las amenazas no son siquiera descubiertas hasta mucho después de que el daño haya sido hecho. Después de superar sus defensas, los ATAs bajos tienen un prolongado "tiempo de permanencia", lo cual les permite proliferan en toda su infraestructura, causando eventualmente provocando una violación.

Las soluciones tradicionales de endpoint con antivirus basados en firmas, prevención de pérdida de datos, prevención de intrusiones en el host, y otras capacidades claves, ofrecen visibilidad limitada de lo que realmente está sucediendo con sus endpoints a lo largo de toda su infraestructura. Esto es especialmente verdadero si múltiples herramientas de diferentes proveedores están implementadas. Este abordaje tipo mosaico en silos, dificulta y hace costosas la búsqueda y el análisis de la actividad de amenazas. *Los equipos de seguridad han tenido que depender de análisis programados para obtener una imagen de la postura de seguridad de su compañía,pero esto destelloss* ocasionales están lejos de ser suficientes, especialmente cuando se considera que más de 307 nuevas amenazas aparecen cada minuto, o más de cinco aparecen cada segundo, según el *Informe de Amenazas de Noviembre de 2014 de McAfee Labs*.[3] Además de la avalancha de malware de día cero, los análisis programados pasan por alto amenazas latentes de multivector, que podrían haberse introducido a su infraestructura sin ser detectadas, esperando desatar su furia.

intel Security

Resumen de la Solución

En general, los equipos de seguridad son incapaces de mantenerse al corriente de la actividad maliciosa, porque los recursos son escasos, los profesionales tienen un tiempo limitado, y los rígidos procesos de respuesta a incidentes no necesariamente se escalan lo suficientemente bien para manejar los ataques grandes. Conforme más endpoints se agregan a la infraestructura, laptops, equipos de sobremesa, dispositivos móviles y servidores, TI enfrenta el desafío de gestionar estos sistemas y extraer seguridad relevante e inteligencia de amenazas.

Por qué Todo Mundo Necesita McAfee Active Response

EDR se convertirá pronto en un componente esencial de la estrategia y práctica de defensa de ciberseguridad de todo mundo. Como consultor de seguridad, John Reed Stark sugiere, "las herramientas EDR mejoran la capacidad de la compañía para detectar y responder a amenazas externas e internas; mejorar la velocidad y la flexibilidad de la compañía para contener cualquier ataque o anomalía futuros; y ayudar a una compañía a gestionar las amenazas a datos de manera más eficaz en general"[4]

McAfee Active Response completa su estrategia de seguridad por capas y mejora no sólo su protección de endpoint, sino también su postura de seguridad general. Es un elemento crítico de una solución integral que incluye las tecnologías esenciales de seguridad de endpoint, como antivirus, control de aplicaciones, inteligencia de amenazas locales, y más. Como parte de la arquitectura integrada y conectada de Intel Security, McAfee Active Response proporciona visibilidad continua y conocimiento de actividad de endpoint para ayudarle a actuar más rápidamente para solucionar problemas de la mejor manera para sus negocios.

Los administradores, investigadores y quienes responden, obtienen una visualización ininterrumpida de la actividad a lo largo de su infraestructura — que les permite responder adecuadamente a las amenazas que pueden estar latentes esperando, pueden haber sido suprimidas para evitar la detección, o pueden estar propagándose a lo largo de su red. Desencadenadores incorporados personalizados ayudan a su equipo de seguridad a descubrir los indicadores de ataque (IoAs) de hoy y de mañana, y actuar con base en esa información rápidamente.

El poder del descubrimiento inteligente, la investigación y los análisis detallados en vivo e interactivos, la elaboración de informes integrales y las alertas y acciones priorizadas, se aprovechan por la plataforma de gestión McAfee® ePolicy Orchestrator® (McAfee ePO™). Intel Security unifica capacidades para **Proteger, Detectar y Corregir** a través de la plataforma McAfee ePO, en un ciclo de retroalimentación adaptable, permitiendo que la seguridad evolucione y aprenda en un ciclo iterativo que mejora con el tiempo. McAfee Active Response es el componente para **Detectar** y **Corregir** de este ciclo de vida de defensa contra amenazas, y ayuda a las organizaciones a identificar riegos más efectivamente e implementar correcciones rápidas. El software McAfee ePO software permite escalabilidad, extensibilidad y monitoreo unificado continuo a lo largo de su infraestructura. También ayuda a controlar sus costos debido a que no se necesita personal técnico ni agentes de gestión adicionales para su administración.

McAfee Active Response

- •Monitoree persistentemente eventos críticos y cambios de estado en endpoints.
- •Use continuamente recolectores para encontrar y visualizar todos los archivos ejecutables y latentes.
- Coloque trampas, desencadenando respuestas automáticas o personalizadas.
- •Gestione toda la solución desde una sola consola.

Figura 1. Protección automatizada, adaptable y continua contra ATAs con McAfee Active Response.

Resumen de la Solución

McAfee Active Response tiene tres ingredientes que son esenciales para un EDR efectivo:

- **Automatización:** Se pueden configurar desencadenadores o trampas con base en diversos parámetros. Instruyen a los endpoints de su entorno que busquen tipos específicos de IoAs. Cuando se descubre un tipo particular de IoA, los desencadenadores activan automáticamente una reacción definida por el usuario, como “reiniciar sistema”. A diferencia de otras soluciones EDR que sólo recolectan información de manera constante, McAfee Active Response aplican automáticamente lógica para invocar una reacción específica bajo determinadas condiciones.
- **Adaptabilidad:** Cuando los administradores reciben una alerta, McAfee Active Response adapta la respuesta de acuerdo a las metodologías de ataque que están en juego. Se pueden realizar búsquedas personalizadas a lo largo de su organización para obtener una comprensión más profunda de IoAs y alinear los esfuerzos y recursos de corrección adecuados.
- **Monitoreo continuo:** McAfee Active Response opera persistentemente. Los desencadenadores activan alertas o respuestas cuando se producen eventos de ataque, y puede ajustarlos para monitorear sistemas para detectar futuras actividades de ataques.

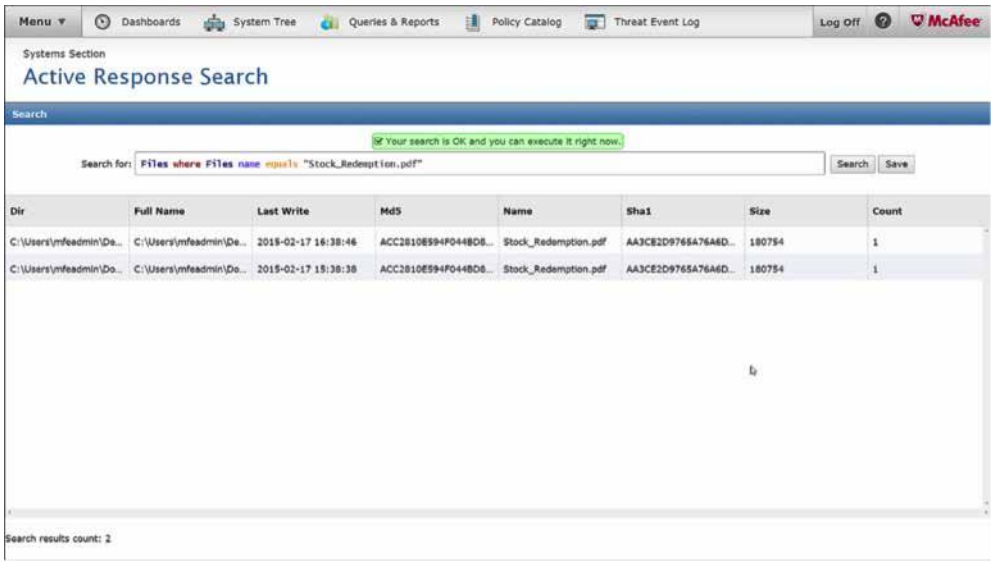

Figura 2. Resultados de búsqueda de McAfee Active Response.

La recolección precisa de datos descubre violaciones potenciales.
Los recolectores representan un componente clave de McAfee Active Response. Las capacidades incorporadas de búsqueda permiten a los usuarios realizar una inmersión profunda en sistemas para descubrir y visualizar datos de conocimiento que pueden ofrecer pistas sobre malware al asecho o actividades sospechosas. Los recolectores son como detectives que pueden ver más allá de lo obvio, examinar archivos ejecutables de programas, procesos en ejecución y archivos y objetos latentes o eliminados

Los recolectores de McAfee Active Response permiten configurabilidad, adaptabilidad y precisión óptimas. Usted tiene la opción de usar ya sea el catálogo proporcionado o escribir e importar sus propios scripts usando McAfee Data Exchange Layer para ejecutarlos. Posteriormente puede buscar a través de las fuentes de datos tradicionales o agujeros negros, donde los paquetes de datos pueden ser destruidos o suprimidos sin su conocimiento, para encontrar la combinación exacta de características que corresponden a los IoAs que usted está interesado en rastrear.

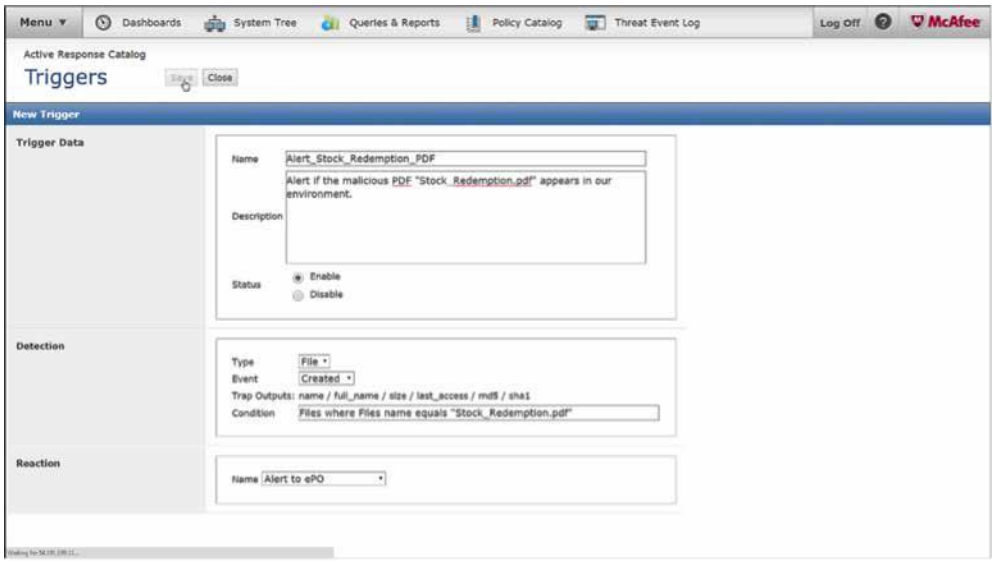

Figura 3. Establecimiento de un activador y especificación de una reacción en McAfee Active Response.

Los desencadenadores y las reacciones proporcionan respuesta automatizada y continua.
Con un único conjunto de instrucciones, los desencadenadores le ayudan a monitorear continuamente y responder a eventos de seguridad o cambios de estado, hoy y mañana. Después de definir el conjunto de posibles comportamientos de ataque o detalles que desea monitorear, puede configurar un activador para generar automáticamente una alerta o ejecutar una reacción cuando estén presentes esos IoAs. En un único y sencillo paso, su equipo de seguridad detecta y remedia, con eficiencia y efectividad, las amenazas emergentes. Gartner recomienda este tipo de capacidad EDR en su informe de 2015, *Mejores Prácticas para Detectar y Mitigar Amenazas Persistentes Avanzadas:* "… capacidades de respuesta automática para eventos de detección de amenazas al utilizar soluciones EDR, tales como el "proceso de matar", eliminar archivo, o borrar memoria, para evitar pérdidas de datos e interrumpir una 'cadena de matar activa'".[5]

McAfee Active Response en la Arquitectura de Seguridad de Intel

La infraestructura de Intel Security unifica e integra múltiples productos, servicios y soluciones de nuestros partners para obtener una mitigación centralizada, eficiente y efectiva de riesgos de seguridad. Le ayuda a responder más rápidamente cuando las ATAs amenazan a su entorno. En el centro de la arquitectura conectada e integrada de Intel Security, está la plataforma de gestión McAfee ePO, que puede utilizar para desplegar y administrar McAfee Active Response. Debido a que McAfee Active Response está tan estrechamente integrado con la plataforma de gestión McAfee ePO, funciona a la perfección con otras tecnologías avanzadas de Intel Security, incluyendo las suites McAfee Threat Intelligence Exchange, McAfee Complete Endpoint Protection y McAfee Enterprise Security Manager.

Cómo funciona.

Una vez que el cliente McAfee Active Response está instalado en el endpoint, se integra con McAfee Agent y rellena una memoria caché de hash de archivo, una memoria caché de flujo de red, y una memoria caché de registro. Se actualizan instantánea y continuamente siempre hay alguna actividad de endpoint. El recolector siempre activo capta el tipo de información especificada en sus instrucciones sobre los archivos maliciosos (incluso si están latentes) o actividad sospechosa. Estos datos son almacenados e indexados localmente en el endpoint y posteriormente servidos en la interfaz del software McAfee ePO. No hay necesidad de un dispositivo de almacenamiento de datos separado o de almacenamiento en nube. La recolección persistente se ejecuta baja y lenta, de modo que nunca hay un pico en el consumo de recursos en el endpoint. Los usuarios pueden continuar su trabajo sin interrupciones.

Si recibe una alerta de un producto de seguridad o quiere cazar a una amenaza recién descubierta de la que acaba de enterarse mediante el intercambio de inteligencia, puede realizar una búsqueda, que funciona de forma muy similar a una búsqueda en Google. Cuando los administradores inician una búsqueda desde la plataforma de gestión McAfee ePO, el cliente McAfee Active Response examina las memorias caché. Los resultados se retornan en tan sólo de 10 a 20 segundos, y usted obtendrá una imagen precisa del estado actual de su entorno en tiempo real.

Los desencadenadores y las reacciones a continuación entran en juego. Los desencadenadores actúan como centinelas, monitoreando continuamente los endpoints para detectar IoAs. Si una IoA particular está presente, el activador se activa y responde automáticamente con una reacción, que usted puede personalizar de acuerdo a sus objetivos específicos. Las reacciones típicas incluyen el envío de una alerta, la supresión de un archivo malo, matar un proceso malicioso, o la realización un análisis forense más detallado.

McAfee Active Response en Acción

No existe nada mejor que los casos de uso del mundo real para tomar conciencia de la importancia de las soluciones EDR. Aquí presentamos algunos ejemplos de cómo McAfee Active Response puede ayudar a detectar y responder a amenazas bajo diferentes circunstancias.

“Minas de tierra” sin detonar

Como se mencionó anteriormente, McAfee Active Response trabaja conjuntamente con McAfee Threat Intelligence Exchange, que permite compartir datos de amenazas significativas en tiempo real, a lo largo de los componentes de seguridad de la arquitectura de Intel Security, lo que les permite actuar como una infraestructura de colaboración unificada. McAfee Threat Intelligence Exchanges le ayuda a bloquear archivos “grises” desconocidos o emergentes que logran escabullirse y evadir los programas de antivirus. Ofrece una mejor visibilidad y control sobre estos tipos de archivos y señala dónde se lleva a cabo el intento de ejecución o la ejecución real del archivo. McAfee Threat Intelligence Exchange posteriormente envía la primer alerta en McAfee Data Exchange Layer. A partir de ahí, los equipos de seguridad pueden acudir a McAfee Active Response para sondear el entorno para detectar el hash de archivo y determinar si se han plantado minas terrestres latentes en otros lugares. Todas estas actividades se realizan de manera rápida y eficiente a través de la plataforma de gestión McAfee ePO.

Malware oculto en documentos

Cada vez más, las amenazas de día cero o el código utilizado para distribuir malware, se insertan en documentos, como archivos .zip, archivos de imagen, .PDFs, archivos de Adobe Flash o archivos .PNG. Estos ataques sigilosos suelen ser indetectables por antivirus estándar. Usted puede utilizar McAfee Active Response para realizar una búsqueda de estos tipos de archivos con base en determinados atributos. Por ejemplo, supongamos que un archivo de documento adjunto sospechoso aparece en la laptop de su asistente. Su equipo puede utilizar McAfee Active Response para definir un activador, que se mantendrá vigilante para detectar este tipo de archivos en todos los endpoints de su organización, y posteriormente limpiarlos antes de que produzcan algún daño.

Sepa Más

McAfee Active Response es automatizado, adaptable y continuo, y es una parte crítica del abordaje integrado de Intel Security para derrotar a los ATAs, que crecen en número y complejidad en el escenario de amenazas de hoy, de manera rápida y exitosa. Para saber más sobre cómo McAfee Active Response complementa el portafolio actual de productos de Intel Security, visite:

- **McAfee Active Response**
- **McAfee ePolicy Orchestrator**
- **McAfee Threat Intelligence Exchange**
- **McAfee Complete Endpoint Protection suites**

1. **http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf**
2. **https://www.gartner.com/doc/2738017/market-guide-endpoint-detection-response**
3. **http://www.mcafee.com/us/about/news/2014/q4/20141209-01.aspx**
4. **http://www.cybersecuritydocket.com/2015/05/08/edr-the-future-of-cybersecurity-and-incident-response/**
5. **https://www.gartner.com/doc/2589029/best-practices-mitigating-advanced-persistent**

McAfee. Parte de Intel Security.
2821 Mission College Boulevard Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com