FICHA TÉCNICA

McAfee Endpoint Threat Defense and Response

Detección del malware de tipo zero-day, protección del paciente cero y bloqueo de las amenazas avanzadas

Las ciberamenazas son cada vez más sofisticadas y para hacerles frente se requiere una nueva generación de soluciones de protección para endpoints. Las amenazas avanzadas y el incremento del riesgo de vulnerabilidades desconocidas están provocando que las empresas acumulen soluciones de seguridad desconectadas y redundantes que proporcionan poca visibilidad y aumentan la complejidad. McAfee resuelve este problema con McAfee® Endpoint Threat Defense y McAfee Endpoint Threat Defense and Response. Ambas soluciones utilizan análisis estáticos y del comportamiento, e inteligencia sintetizada, para proteger, detectar, corregir y adaptarse para luchar contra las amenazas emergentes. Los componentes de seguridad unificados actúan como uno a través de un enfoque abierto e integrado, con intercambio de visibilidad e inteligencia sobre amenazas, y flujos de trabajo simplificados. Una seguridad conectada y datos forenses sobre amenazas procesables proporcionan una infraestructura segura para identificar con rapidez y confianza las amenazas e ir por delante de potenciales agresores.

Neutralice el malware de tipo zero-day, al greyware y al ransomware

Vaya por delante de las amenazas emergentes con análisis estáticos y dinámicos que aprovechan análisis de reputación y del comportamiento mejorados para detectar exploits potenciales. Aplique inteligencia sintetizada con McAfee Threat Intelligence Exchange para bloquear y contener inmediatamente las amenazas y actualizar de forma instantánea la información sobre reputación de amenazas para impedir ataques futuros.

McAfee Endpoint Threat Defense y McAfee Endpoint Threat Defense and Response consiguen neutralizar el malware de tipo zero-day a través de la identificación de similitudes entre comportamientos maliciosos demostrados y los numerosos modelos de amenazas de Real Protect mediante una búsqueda en la nube (centros de datos alojados en Estados Unidos). Esta técnica de clasificación del comportamiento se utiliza para erradicar las amenazas activas que pueden haber evadido otros productos de software de seguridad.

Ventajas principales

- Detecte, proteja y corrija al tiempo que adapta de forma proactiva sus defensas contra malware de tipo zero-day, el greyware y el ransomware.
- Proteja de forma más eficaz mediante reputaciones dinámicas, análisis del comportamiento y aprendizaje automático.
- Minimice el impacto a usuarios y aplicaciones empresariales de confianza con protección mejorada.
- Responda a más amenazas y corríjalas de forma más rápida con inteligencia sobre amenazas compartida con todo el ecosistema de seguridad.
- Racionalice la investigación y corrección de incidentes con flujos de trabajo unificados y una única consola de administración a través del software McAfee® ePolicy Orchestrator® (McAfee ePO™).

Proporciona inteligencia sobre amenazas accionable a través del software McAfee ePolicy Orchestrator para permitir la detección de amenazas de tipo zero-day y la corrección en tiempo real. La clasificación del comportamiento se desarrolla automáticamente a través del aprendizaje automático dinámico, lo que ofrece protección y eficacia máximas, y reduce al mismo tiempo la exposición a riesgos de seguridad.

Reduzca el número de eventos y corrija las amenazas más rápidamente

Céntrese en lo que importa gracias a la reducción del número de eventos de seguridad, neutralizando automáticamente más amenazas, compartiendo inteligencia y utilizando alertas proactivas para definir respuestas automáticas. Reduzca el esfuerzo necesario para investigar y resolver amenazas con flujos de trabajo simplificados que resuelven los eventos más rápidamente y amplíe la capacidad de seguridad aumentando la protección de toda la empresa.

Los componentes conectados comparten automáticamente información de seguridad a través de McAfee Data Exchange Layer. McAfee Threat Intelligence Exchange le permite sintetizar inteligencia sobre amenazas completa en todo el ecosistema, con datos de McAfee Global Threat Intelligence y de otras fuentes, y compartir de manera inmediata la información sobre amenazas para adaptar su protección automáticamente.

Proteja al “paciente cero”

Detecte e impida que el malware de tipo zero-day realice cambios maliciosos en los endpoints. La tecnología Contención dinámica de aplicaciones vigila el comportamiento del greyware e impide cambios maliciosos para neutralizar eficazmente los exploits antes de que se lleven a cabo. Proteja los endpoints que entran y salen de la red y evite el comportamiento malicioso con protección que pasa desapercibida para los usuarios.

Saque rendimiento de los procesos de seguridad para ampliarlos y adaptarlos

La aplicación de directivas, la investigación y la corrección de incidentes se simplifican a través del software McAfee ePO, una consola de administración de panel único que proporciona visibilidad de todos los sistemas, para que pueda evaluar fácilmente el estado de seguridad de los endpoints y permitir la protección en tiempo real. Reduzca las tareas de supervisión, búsqueda y respuesta con flujos de trabajo unificados y la corrección mediante un solo clic en un único endpoint o en toda la infraestructura. Con McAfee Endpoint Threat Defense y McAfee Endpoint Threat Defense and Response, aproveche el aprendizaje automático para actualizar los modelos de clasificación de comportamientos y compartir de manera instantánea inteligencia sobre amenazas con todos los componentes de seguridad, de manera que pueda actuar como un sistema exclusivo y unificado contra las amenazas emergentes. Impida futuros ataques y aproveche reacciones preconfiguradas para bloquear amenazas potenciales, y reduzca de esta forma la carga de trabajo del personal para que puedan centrarse en otras prioridades de administración de la seguridad.

Identifique, asigne prioridades y corrija los ataques avanzados

McAfee Endpoint Threat Defense and Response le ayuda a determinar el origen, el alcance y el impacto de un ataque. Utiliza la tecnología McAfee Active Response para proporcionar visibilidad tanto en tiempo real como histórica de los endpoints de su infraestructura. Los indicadores de ataque se identifican y priorizan con la ayuda de un contexto completo que permita una rápida respuesta.

Tome la iniciativa con precisión, rapidez y agilidad para neutralizar las amenazas que se propagan activamente, que esperan el momento de atacar o que han eliminado su rastro para evitar ser detectadas. La visibilidad y el control basados en el conocimiento pueden identificar los puntos en los que las amenazas intentan establecerse y permiten a los responsables de las respuestas contener y corregir inmediatamente, reduciendo la exposición de meses a minutos o incluso a milisegundos.

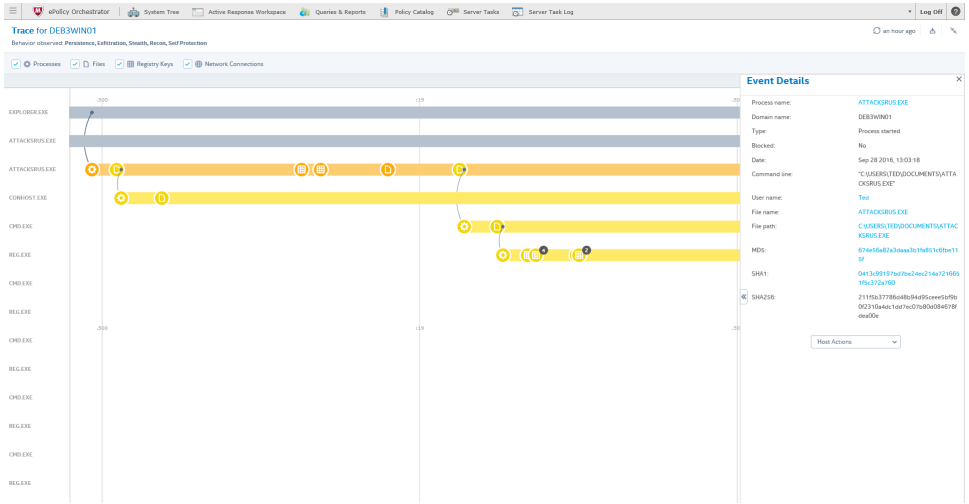

Figura 1. El espacio de trabajo de amenazas localiza el origen y comportamiento de incidentes sospechosos para acelerar la respuesta.

Funciones de McAfee Endpoint Threat Defense and Response

Componente	Ventaja	Ventajas para los clientes	Diferenciación	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Contención dinámica de aplicaciones[1]	Protege al llamado "paciente cero" impidiendo que el greyware realice cambios maliciosos en los endpoints, tanto dentro como fuera de la red.	▪ Hace posible el análisis de amenazas potenciales sin sacrificar al paciente cero. ▪ Mayor protección sin que afecte a los usuarios finales ni a las aplicaciones de confianza. ▪ Reducción del tiempo desde la detección a la contención con intervención manual mínima. ▪ Protección del paciente cero, manteniendo intacta la productividad de los endpoints y aislando de la red frente a infecciones.	▪ Componente integral de la infraestructura de McAfee para disfrutar de una protección y eficacia óptimas. ▪ Funciona con o sin conexión a Internet y no requiere intervención ni análisis externos. ▪ Transparente para el usuario. ▪ Modo de observación que ofrece visibilidad instantánea de las amenazas y comportamientos de ataque potenciales dentro del entorno.	√	√

FICHA TÉCNICA

Componente	Ventaja	Ventajas para los clientes	Diferenciación	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Real Protect	Aplica clasificación de comportamientos mediante aprendizaje automático para bloquear amenazas de tipo zero-day antes de que se ejecuten e interrumpir directamente la ejecución de las que consiguieron evadir la detección anterior.	▪ Bloqueo de una cantidad mayor de malware de tipo zero-day, incluidos objetos difíciles de detectar como el ransomware. ▪ Identificación, análisis y corrección automática de las amenazas sin intervención manual. ▪ Adaptación de las defensas mediante la clasificación automatizada y una infraestructura de seguridad conectada.	▪ Análisis del comportamiento estáticos y dinámicos que proporcionan mejor protección que los enfoques de una sola etapa. ▪ Detecta el malware que solo puede detectarse mediante análisis dinámicos del comportamiento. ▪ La integración en profundidad permite compartir actualizaciones de reputación en tiempo real y mejorar la eficacia de todos los componentes de seguridad.	√	√
McAfee Threat Intelligence Exchange	Conecta los componentes de seguridad para compartir información contextual y proporcionar visibilidad y control en toda la empresa para ofrecer una protección frente a amenazas adaptable.	▪ Identificación del paciente cero y distribución de la información a todo el sistema de seguridad para impedir la siguiente infección. ▪ Reducción del costo total de propiedad y aprovechamiento eficaz de la seguridad para endpoints. ▪ Conexión de los componentes de seguridad para crear una protección de bucle cerrado mediante la transformación de tecnologías de seguridad independientes en un sistema coordinado único.	▪ Incorporación de inteligencia de McAfee Global Threat Intelligence, local y de otras fuentes. ▪ Definición de lo que es fiable y lo que no gracias a inteligencia local o de terceros. ▪ Conexión instantánea de la información de reputación de amenazas con los endpoints, la Web, la red y los productos en la nube. ▪ Generación de informes de inteligencia sobre amenazas detallados y procesables para adaptar las protecciones.	√	√
McAfee Data Exchange Layer	Conecta la seguridad para integrar y optimizar la comunicación tanto con productos de McAfee como de terceros.	▪ Reducción del riesgo y el tiempo de respuesta. ▪ Reducción de costos operativos y de personal. ▪ Optimización de procesos y recomendaciones prácticas.	▪ Distribución de la información sobre amenazas a todos los productos de seguridad. ▪ Distribución instantánea de la información sobre el paciente cero a todos los endpoints para evitar infecciones y actualizar la protección.	√	√
Plataforma de administración McAfee ePO	Un panel de visualización único para disponer de una administración ampliable, flexible y automatizada de las directivas de seguridad a fin de identificar y responder a los problemas de seguridad.	▪ Unificación y simplificación de los flujos de trabajo de seguridad para mejorar la eficacia. ▪ Visibilidad en un solo panel de todos los sistemas para evaluar fácilmente el estado de seguridad y permitir la protección en tiempo real. ▪ Despliegue y gestión rápidos de la protección de McAfee con aplicación de directivas personalizable. ▪ Reducción del tiempo desde la detección a la respuesta a través de consultas, paneles y respuestas dinámicas y automatizadas.	▪ Mayor control, menos costos y una administración de la seguridad operativa más rápida gracias a una única consola. ▪ Paneles que se pueden arrastrar y soltar que proporcionan una mayor visibilidad en tiempo real de todo el ecosistema. ▪ Kits de desarrollo de software (SDK) de plataforma abierta que facilitan la rápida adopción de innovaciones de seguridad futuras.	√	√
McAfee Active Response	Visibilidad de amenazas proactiva, análisis del desarrollo de los eventos, búsqueda de datos de amenazas actuales e históricos, con la capacidad de tomar medidas inmediatas y adaptar la protección.	▪ Búsqueda rápida de datos sobre amenazas actuales e históricos para determinar el alcance total de un ataque, acelerar las investigaciones y reducir el tiempo de respuesta. ▪ Automatización de las respuestas a amenazas y protección de la seguridad en tiempo real sin intervención manual. ▪ Atención prioritaria a las amenazas más importantes. ▪ Uso de supervisión continua y recopiladores personalizables para buscar a fondo indicadores de ataque, que pueden estar en ejecución o estado latente, o incluso haber sido eliminados.	▪ Visibilidad instantánea de intentos de ataque desconocidos y comportamientos peligrosos que se ejecuten en el entorno y que no fueran eliminados por las tecnologías de protección. ▪ Investigación de la cronología de los eventos en cada endpoint con búsqueda en tiempo real integrada en todos los endpoints para neutralizar amenazas. ▪ Un solo clic para proteger, corregir y adaptar, reduciendo el uso de varias herramientas y pasos a una sola operación.		√

Especificaciones

McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Plataformas admitidas:	**Plataformas admitidas:**
▪ Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary	▪ Microsoft Windows: 7, 8, 8.1, 10, 10 Anniversary
▪ Mac OS X versión 10.5 o posterior	▪ RedHat 6.5
▪ Linux: RHEL, SUSE, CentOS, OEL, Amazon Linux y las últimas versiones de Ubuntu	▪ CentOS 6.5
Servidores:	▪ Windows Server 2008, 2012 y 2016
▪ Windows Server (2003 SP2 o posterior, 2008 SP2 o posterior, 2012), Windows Server 2016	
▪ Windows Embedded (Standard 2009, Point of Service 1.1 SP3 o posterior)	
▪ Citrix Xen Guest	
▪ Citrix XenApp 5.0 o posterior	

1. McAfee Endpoint Threat Defense and Response incluye centros de datos alojados ubicados en Estados Unidos que se utilizan para validar la autenticación de clientes, comprobar la reputación de los archivos y almacenar datos importantes para la detección y neutralización de archivos sospechosos. Aunque no es necesaria, la Contención dinámica de aplicaciones funcionará perfectamente en una conexión en la nube. Para disponer de todas las funciones de McAfee Active Response, Contención dinámica de aplicaciones y Real Protect se requiere acceso a la nube y soporte activo, y están sujetas a los términos y condiciones del servicio en la nube.

Más información

Para obtener más información sobre las ventajas de McAfee Endpoint Threat Defense, visite **www.mcafee.com/mx/products/endpoint-threat-defense.aspx.**

Para obtener más información sobre las ventajas de McAfee Endpoint Threat Defense and Response, visite **www.mcafee.com/mx/products/endpoint-threat-defense-response.aspx.**

McAfee Together is power.

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