McAfee Complete Endpoint Threat Protection

Protección contra amenazas avanzada para ataques sofisticados

Los tipos de amenazas a los que se enfrenta su empresa requieren mayor visibilidad y herramientas que le permitan actuar y controlar el ciclo de vida completo de protección contra amenazas. Esto supone dotar a los especialistas en seguridad con funciones que actúen con mayor precisión y que ofrezcan información más sólida sobre las amenazas avanzadas. McAfee® Complete Endpoint Threat Protection ofrece protecciones avanzadas que investigan, contienen y actúan contra amenazas de tipo zero-day y ataques sofisticados. Esta protección de endpoints esencial utiliza las tecnologías de aprendizaje automático y contención dinámica integradas para detectar amenazas de tipo zero-day casi en tiempo real, y para ello las clasifica y las bloquea antes de que puedan ejecutarse. Los datos e informes forenses procesables le mantienen informado y le ayudan a avanzar de la mera respuesta a brotes a la investigación y fortalecimiento de sus defensas. Y, gracias a que está creada mediante una plataforma ampliable, puede añadir fácilmente otras protecciones contra amenazas avanzadas, ahora y en el futuro, en función de la evolución de sus necesidades y del panorama de amenazas.

Ventajas principales

- Aprendizaje automático y contención dinámica para ir por delante de las amenazas de tipo zero-day, el ransomware y el greyware.
- Corrección de amenazas y protección rápidas con acciones y análisis automatizados.
- Simplificación del entorno, el despliegue y la gestión diaria con administración centralizada.

Protecciones contra amenazas avanzadas y automatizadas

Es necesario que detenga las amenazas avanzadas antes de que actúen. Por eso McAfee Complete Endpoint Threat Protection incluye tecnologías como Contención dinámica de aplicaciones y Real Protect[1]. La Contención dinámica de aplicaciones detiene automáticamente el greyware y las amenazas de tipo zero-day sospechosas cuando se detectan comportamientos maliciosos, e impide que infecten sus sistemas o afecten a sus usuarios. Gracias al uso del aprendizaje automático, Real Protect es capaz de investigar y clasificar las amenazas, almacenando la información que recopila para acciones futuras que pueden aplicarse automáticamente.

Creada para reducir la complejidad

La complejidad es el enemigo de la eficacia. Ahora puede olvidarse del tiempo dedicado a administrar

varias soluciones individuales con interfaces y consolas de administración distintas. McAfee Complete Endpoint Threat Protection se administra mediante una única consola: el software McAfee® ePolicy Orchestrator® (McAfee ePO™). Gracias a este panel de visualización único, podrá acelerar los tiempos de despliegue y reducir las cargas de administración permanentes. Los clientes que utilicen varios sistemas operativos en su entorno verán aumentada su productividad gracias al uso de directivas para varias plataformas: sistemas Microsoft Windows, Apple Macintosh y Linux.

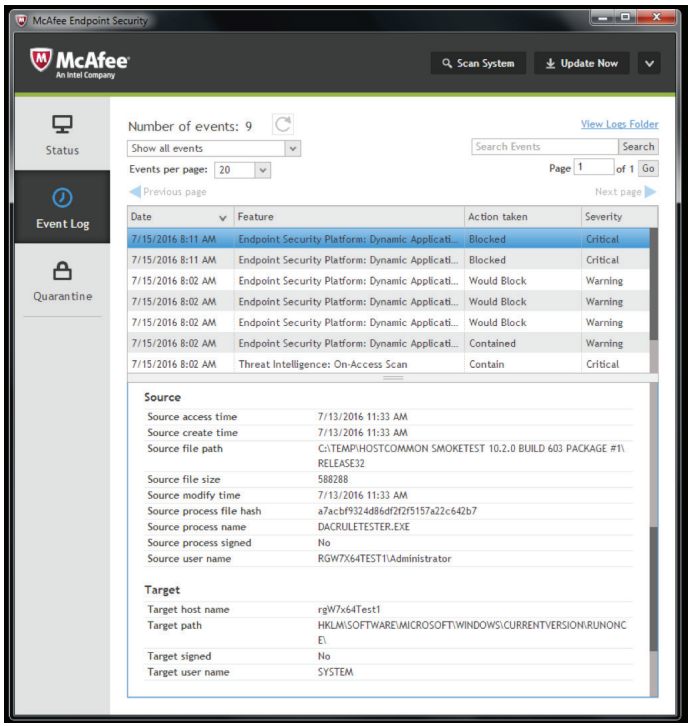

Figura 1. La Contención dinámica de aplicaciones bloquea y detiene las amenazas en función de su gravedad.

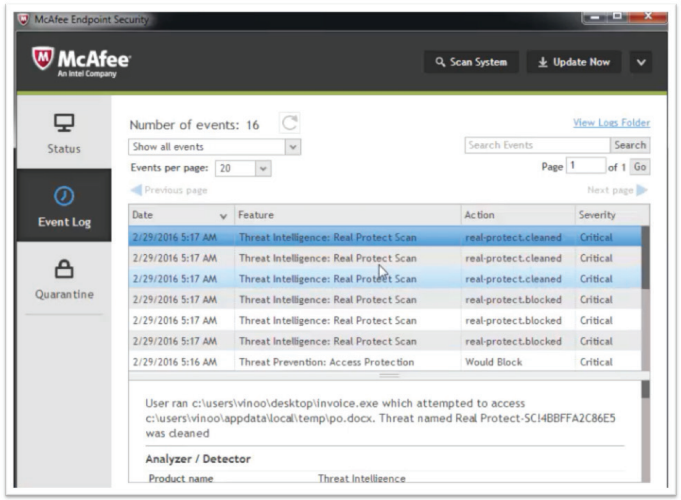

Figura 2. Real Protect utiliza el aprendizaje automático para detectar casi en tiempo real el malware de tipo zero-day que los análisis basados en firmas a menudo pasan por alto.

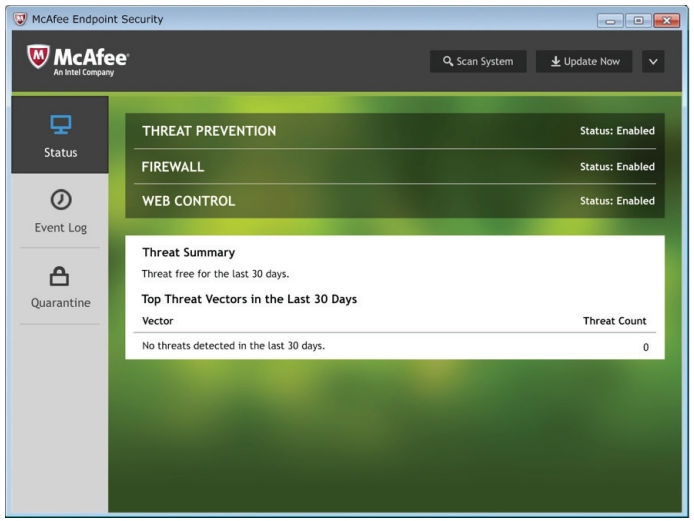

Figura 3. Una interfaz de usuario intuitiva para facilitar el trabajo a administradores y usuarios.

Una plataforma flexible creada para hoy y para el futuro

McAfee Complete Endpoint Threat Protection le ofrece una plataforma conectada y colaborativa, así como protección casi en tiempo real a través de varias tecnologías de protección. Esto permite no solo realizar análisis de amenazas más robustos, sino compartir los datos forenses sobre amenazas recopilados con otras protecciones para hacerlas más inteligentes. Gracias a una capa de comunicación común, los productos de protección para endpoints centrales pueden informar y consultar a las protecciones contra amenazas avanzadas, para disponer de datos claros desde el momento exacto en el que se detectan.

Este enfoque también permite un despliegue más flexible, de manera que pueda instalar el contenido completo de su compra desde hoy mismo. Puede decidir las funciones que va a configurar y activar inmediatamente y, a partir de ahí, activar fácilmente las que decida utilizar más adelante con un cambio de directivas.

Por último, nuestra plataforma le permite ampliar su protección a medida que cambien sus necesidades, gracias a una arquitectura diseñada para integrar otras tecnologías.

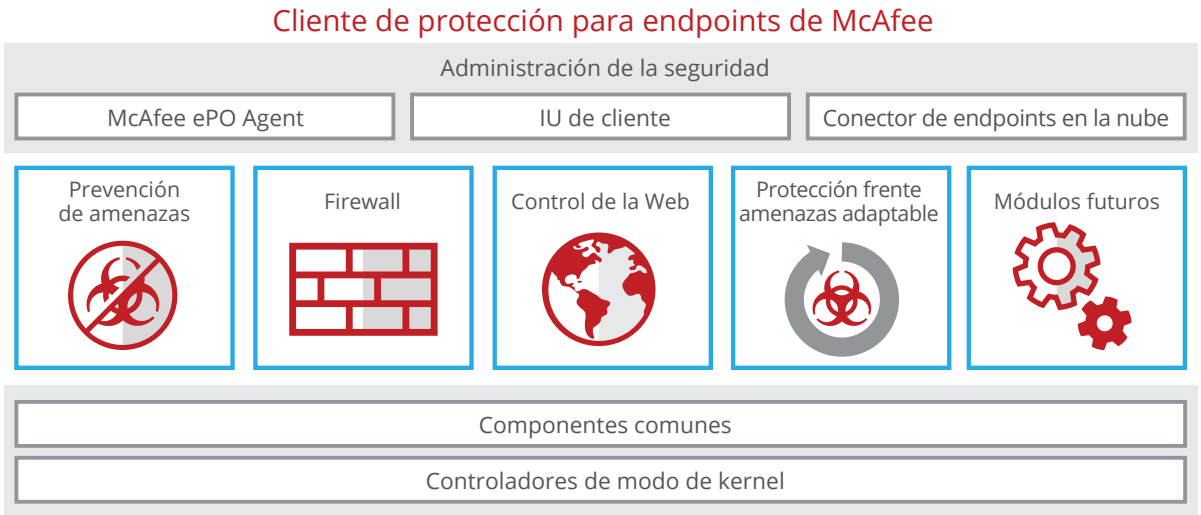

Figura 4. La plataforma de cliente de protección para endpoints de McAfee.

Plataformas admitidas

- Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary
- Mac OS X versión 10.5 o posterior
- Plataformas Linux de 32 y de 64 bits: las últimas versiones de RHEL, SUSE, CentOS, OEL, Amazon Linux y Ubuntu

Servidores:

- 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

FICHA TÉCNICA

Componente	Ventaja	Ventajas para los clientes	Diferenciación
Contención dinámica de aplicaciones	Protege el llamado "paciente cero" impidiendo que el greyware realice cambios maliciosos en los endpoints.	▪ Mayor protección sin impacto alguno en los usuarios finales ni en las aplicaciones de confianza. ▪ Reducción del tiempo desde la detección a la contención con intervención manual mínima. ▪ Protección del paciente cero y aislamiento de la red frente a infecciones.	▪ 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.
Real Protect	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 mayor cantidad 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 protecciones mediante la clasificación automatizada y una infraestructura de seguridad conectada.	▪ Detecta el malware que solo puede encontrase 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.
Prevención de amenazas	Protección completa que identifica, bloquea y elimina el malware rápidamente gracias a varias capas de protección.	▪ Bloqueo del malware conocido y desconocido mediante técnicas de análisis heurístico, del comportamiento y en tiempo real. ▪ Simplificación de las directivas y los despliegues para equipos de sobremesa y servidores, con protección para equipos Windows, Mac y Linux. ▪ Mayor rendimiento evitando análisis de procesos de confianza y centrándose en los que parecen sospechosos.	Antimalware multicapa que colabora con las protecciones web y mediante firewall para ofrecer análisis y prevención de amenazas más robustos.
Firewall integrado	Protección de endpoints frente a las redes de bots, los ataques de denegación de servicio distribuidos (DDoS), los ejecutables no fiables, las amenazas avanzadas persistentes y las conexiones peligrosas a la Web.	▪ Protección de los usuarios y la productividad mediante la implementación de sus propias directivas. ▪ Ahorro de ancho de banda gracias al bloqueo de las conexiones entrantes no deseadas y el control de las solicitudes salientes. ▪ Los usuarios reciben información sobre las redes y ejecutables de confianza, y de los archivos o conexiones peligrosas.	Directivas de aplicaciones y ubicaciones que protegen los equipos de sobremesa y portátiles, especialmente cuando no están conectados a la red de la empresa.

FICHA TÉCNICA

Componente	Ventaja	Ventajas para los clientes	Diferenciación
Control de la Web	Navegación segura con protección web y filtrado para endpoints.	▪ Reducción del riesgo y supervisión del cumplimiento de normativas. Para ello, se alerta a los usuarios antes de que visiten sitios web maliciosos. ▪ Prevención de amenazas y protección de la productividad autorizando o bloqueando el acceso a sitios web. ▪ Bloqueo de las descargas peligrosas antes de que se produzcan.	Protección para sistemas Windows, Mac, y varios navegadores.
Data Exchange Layer	Conexión de la seguridad para integrar y optimizar la comunicación tanto entre productos de McAfee como con productos de terceros.	▪ Reducción del riesgo y el tiempo de respuesta, gracias a la integración. ▪ Reducción de costes operativos y de personal. ▪ Procesos optimizados y recomendaciones prácticas.	Intercambio de la información sobre amenazas más importante entre los productos de seguridad.
Administración con McAfee ePO	Un panel de visualización único para facilitar 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. ▪ Mayor visibilidad y flexibilidad para actuar con confianza. ▪ Despliegue y gestión rápidos de un único agente con implementación de directivas personalizable. ▪ Reducción del tiempo desde la detección a la respuesta con paneles e informes intuitivos.	▪ Mayor control, menos costes y una administración de la seguridad operativa más rápida gracias a una única consola. ▪ Una interfaz de eficacia probada que ha sido reconocida en todo el sector por su extraordinaria calidad. ▪ Paneles que se pueden arrastrar y soltar en un amplio ecosistema de seguridad. ▪ Una plataforma facilita la rápida adopción de las innovaciones en seguridad.

Más información

Para obtener más información sobre las ventajas de McAfee Complete Endpoint Threat Protection, visite: **www.mcafee.com/es/products/complete-endpoint-threat-protection.aspx**.

1. La solución incluye centros de datos alojados ubicados en Estados Unidos que se utilizan para comprobar la reputación de los archivos y almacenar datos importantes para la detección de archivos sospechosos. Aunque no es imprescindible, una conexión a la nube mejorará el rendimiento de la función Contención dinámica de aplicaciones. Para disponer de todas las funciones de la tecnología Contención dinámica de aplicaciones y Real Protect se requiere acceso a la nube y soporte activo. Estas funciones están sujetas a los términos y condiciones del servicio en la nube.

McAfee Together is power.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid España
+34 91 347 85 00
www.mcafee.com/es