



McAfee Endpoint Threat Protection

Protección esencial y eficaz que crece conforme lo hace su empresa

Ventajas principales

- Fortalezca su estado de seguridad con capas de tecnologías de protección colaborativas.
- Disfrute de la flexibilidad de ampliar fácilmente su protección a medida que cambien sus necesidades.
- Aumente la productividad gracias a la administración centralizada, análisis que no afectan en absoluto a los usuarios y con un impacto mínimo en los recursos del sistema.

No existe ninguna duda de que el panorama de amenazas seguirá evolucionando. Ya sabe que disponer de una defensa robusta empieza en el endpoint. Sin embargo, en la actualidad puede ser complicado disponer de la protección que necesita si no dispone de la capacidad de integrar nuevas tecnologías sin complicar por ello las operaciones de seguridad. McAfee® Endpoint Threat Protection ofrece la protección esencial que necesita hoy y le prepara para los requisitos de protección contra amenazas avanzadas del futuro. Ofrece funciones de prevención de amenazas, protección de la Web, el correo electrónico, los dispositivos y mediante firewall integradas, que trabajan de forma conjunta en tiempo real para analizar y colaborar frente a las amenazas, bloqueándolas y corrigiéndolas rápidamente antes de que afecten a sus sistemas o usuarios.

Una plataforma para endpoints colaborativa

Creadas con la vista puesta en la integración, las defensas de McAfee Endpoint Threat Protection colaboran y comparten lo que observan en tiempo real para coordinar la identificación y bloquear la ejecución de archivos y sitios web sospechosos, así como de programas potencialmente no deseados para disponer de un mayor nivel de protección.

Caso práctico

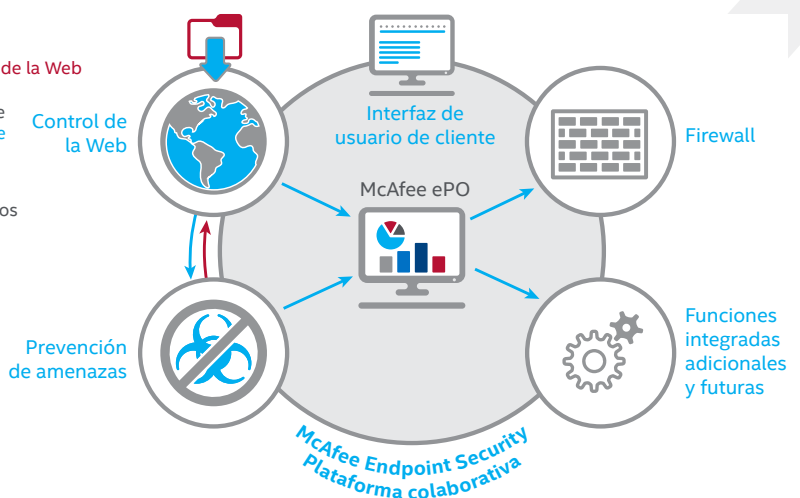
Descarga de un archivo malicioso de la Web

Se envía un hash de archivo desde **Control de la Web** a **Prevención de amenazas**, que activa un análisis bajo demanda.

Se detectan y **bloquean** los archivos maliciosos antes de que consigan acceso total al sistema.

Se obtienen datos forenses (URL de origen y hash de archivo, entre otros).

Se **comparten** los datos de eventos con otros módulos y con el software McAfee® ePolicy Orchestrator® (McAfee ePO™), y se muestran en la interfaz de usuario de cliente.



Una solución integrada para hoy y para el futuro

Con McAfee Endpoint Threat Protection, puede sustituir despliegues de productos individuales desconectados por una plataforma colaborativa conectada y protección casi en tiempo real con varias tecnologías de protección. Esto no solo permite llevar a cabo un análisis más profundo de las amenazas, sino compartir los datos forenses sobre amenazas recopilados con otras protecciones para hacerlas más inteligentes y ayudarles a identificar y bloquear más rápidamente las amenazas en otros endpoints o cuando se localizan en un punto de entrada distinto.

Este enfoque permite además un despliegue flexible. Puede instalar el contenido completo de su compra desde hoy mismo y decidir qué funciones va a configurar y activar inmediatamente. Podrá activar fácilmente las funciones que decida utilizar más adelante mediante el cambio de una directiva.

Por último, nuestra plataforma le permite ampliar fácilmente su protección a medida que cambien sus necesidades, gracias a una arquitectura diseñada para integrar otras tecnologías. Esto le garantizará que está preparado en todo momento para incorporar otras funciones de protección avanzadas para proteger su entorno contra amenazas más sofisticadas.

Asequible sin sacrificar el rendimiento

McAfee Endpoint Threat Protection ofrece una plataforma ampliable formada por tecnologías de protección esenciales sin introducir complejidad ni sacrificar el rendimiento, lo que permite aumentar su productividad y la de los usuarios. Por ejemplo, sus operaciones se ejecutarán con mayor eficacia gracias a la administración centralizada a través del software McAfee ePolicy Orchestrator, que ofrece un panel único para desplegar, supervisar y administrar las directivas de seguridad en todo su entorno. 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. Y, gracias a que los componentes de McAfee Endpoint Threat Protection utilizan un lenguaje común (McAfee Data Exchange Layer), puede optimizar los procesos entre tecnologías y acelerar las respuestas frente a amenazas, reduciendo riesgos al estrechar la ventana de exposición.

Además, los usuarios aumentarán su productividad gracias a análisis sin impacto alguno sobre ellos, la memoria y el uso de la CPU, optimizados para minimizar el impacto en los sistemas. Asimismo incluye una interfaz de usuario intuitiva que le permite a usted y a los usuarios determinar las acciones que se ha adoptado y por qué.

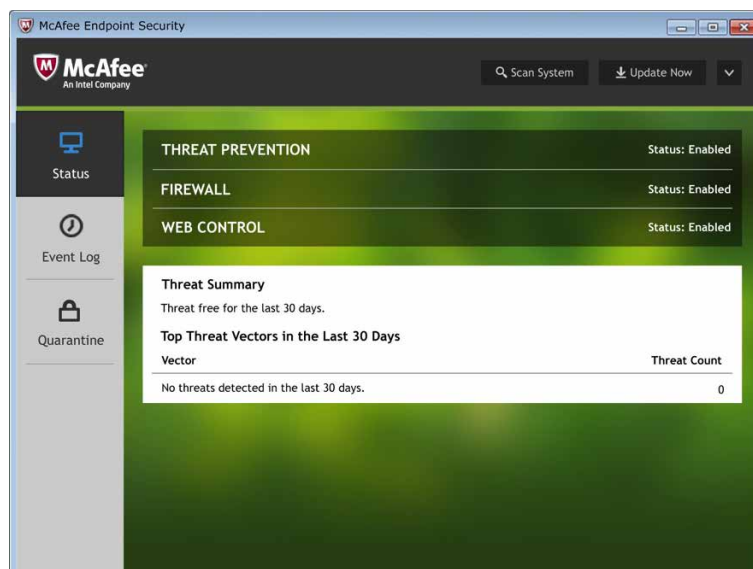


Figura 2. Una interfaz de usuario intuitiva para facilitar el trabajo a administradores y usuarios.

Ficha técnica

Plataformas admitidas

- 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: RHEL, SUSE, CentOS, OEL, Amazon Linux y las últimas versiones de 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

Componente	Ventaja	Ventajas para los clientes	Diferenciación
Prevención de amenazas	Protección completa que identifica, bloquea y elimina el malware rápidamente gracias a varias capas de protección.	<ul style="list-style-type: none"> • Detección del malware conocido y desconocido mediante técnicas de análisis heurístico y en tiempo real. • Simplificación de las directivas y los despliegues ofreciendo protección para plataformas Windows, Mac y Linux. • Mayor rendimiento evitando análisis de procesos de confianza y centrándose en los que parecen sospechosos. 	Antimalware multicapa que colabora e informa a las defensas de la Web y mediante firewall para fortalecer el análisis y aplicar de forma inteligente reglas para bloquear amenazas potenciales.
Firewall integrado	Protege los 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.	<ul style="list-style-type: none"> • Protección de los usuarios y la productividad a través de la aplicación de sus propias directivas. • Ahorro de ancho de banda mediante el 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 escritorio y portátiles, especialmente cuando no están conectados a la red de la empresa.
Control de la Web	Garantiza una navegación segura con protección web y filtrado para endpoints.	<ul style="list-style-type: none"> • Reducción del riesgo y supervisión del cumplimiento de normativas. Para ello, alerta a los usuarios antes de que visiten sitios web maliciosos. • Neutralización de las amenazas y protección de la productividad autorizando o bloqueando los sitios web peligrosos o inapropiados. • Bloqueo de las descargas peligrosas antes de que se produzcan. 	Protección para sistemas Windows, Mac, Linux y un gran número de navegadores, gracias a la información de McAfee Global Threat Intelligence.
McAfee Data Exchange Layer	Conecta la seguridad para integrar y optimizar la comunicación tanto con productos de Intel Security como de terceros.	<ul style="list-style-type: none"> • La integración reduce el riesgo y el tiempo de respuesta. • Reducción de costos operativos y de personal. • Procesos optimizados y recomendaciones prácticas. 	<ul style="list-style-type: none"> • Comparte la información sobre amenazas más importantes con los productos de seguridad. • Distribución instantánea de la información sobre el paciente cero a todos los endpoints para evitar infecciones y actualizar la protección.
Administración con 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.	<ul style="list-style-type: none"> • 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 aplicación de directivas personalizable. • Reducción del tiempo desde la detección a la respuesta a través de paneles, consultas y respuestas dinámicas y automatizadas. 	<ul style="list-style-type: none"> • Mayor control, menos costos 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.

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



McAfee. Part of Intel Security.

6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.intelsecurity.com

Intel y los logotipos de Intel y McAfee, ePolicy Orchestrator y McAfee ePO son marcas comerciales de Intel Corporation o McAfee, Inc. en EE. UU. y/o en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros. Copyright © 2016 Intel Corporation. 1770_1016
OCTUBRE DE 2016