



# McAfee Endpoint Protection—Advanced Suite

**Protección frente a ataques de tipo zero-day y ayuda para el cumplimiento de normativas**

## Características principales

- Proteja los dispositivos Microsoft Windows, Mac y Linux frente a las amenazas contra el sistema, los datos, el correo electrónico y la Web, y frente al riesgo de incumplimiento de normativas.
- Consolide los esfuerzos de seguridad de endpoints y datos con una solución integrada de un solo proveedor, lo que asegura una protección más sólida por un costo inferior.
- Disfrute de mayor protección inmediatamente, con la simplicidad y la eficiencia de la administración centralizada, y una plataforma de seguridad de endpoints ampliable.

La combinación de empleados móviles y el aumento de las exigencias regulatorias puede ser una auténtica pesadilla para la seguridad. Con una seguridad integrada y proactiva para combatir el malware más sofisticado y las amenazas de tipo zero-day, McAfee® Endpoint Protection—Advanced Suite, parte de la oferta de productos de Intel® Security, protege los endpoints cuando abandonan la red y ayuda a proteger la red cuando vuelven a incorporarse. Su sistema de prevención de intrusiones integrado protege a los sistemas de escritorio y portátiles frente a amenazas avanzadas. Gracias a la administración centralizada basada en directivas, la compatibilidad con distintas plataformas y las auditorías, podrá garantizar la seguridad y el cumplimiento de las normativas de todos sus endpoints.

Ante el aumento del nivel de sofisticación de los ataques de los agresores, los expertos en seguridad necesitan la visibilidad y las herramientas adecuadas para detectar y ofrecer protección contra las amenazas avanzadas. Si bien cualquier endpoint está en peligro ante las sutiles tecnologías que utilizan actualmente los delincuentes, los portátiles se enfrentan a amenazas adicionales. Estos dispositivos se arriesgan al entrar en hoteles, cafeterías y oficinas domésticas sin las tradicionales capas de protección, como gateways de la Web y del correo electrónico, firewalls de red y sistemas de prevención de intrusiones para redes. Si la red es inalámbrica, cualquiera puede escuchar y captar algo más que noticias.

Los PC pueden perderse los parches y otras actualizaciones, con lo que quedan aún más vulnerables ante las amenazas zero-day,

simplemente desconectándose de la red de la empresa. Y estos parches y actualizaciones son cada vez más necesarios para el cumplimiento de las normativas. Aparte de las regulaciones del sector, que cada vez son más rigurosas, es posible que los controles internos de la dirección de la empresa le obliguen a responsabilizarse de la distribución de datos confidenciales y el uso adecuado de la Web tanto en la oficina como fuera de ella.

McAfee Endpoint Protection—Advanced Suite le permite tomar las riendas con amplias protecciones, controles de cumplimiento de normativas y administración unificada. Se trata de una solución integral con la combinación perfecta de funciones y ahorro de costos para mantener a raya tanto a virus como a piratas informáticos, a remitentes de spam, a ladrones de datos y a auditores.

### Por qué Intel Security

- Ofrecemos a los administradores una experiencia verdaderamente centralizada.
- Nuestras plataformas de seguridad y de endpoints integradas permiten eliminar las redundancias, conectar con otras soluciones y ofrecer una arquitectura ampliable sobre la que se puede crecer.
- McAfee Global Threat Intelligence ofrece el mayor volumen de información sobre amenazas del mercado. Vemos y protegemos más que nadie.

### Defensas inteligentes y colaborativas

Las empresas requieren una estrategia para la protección, la detección de las amenazas y la corrección de sus efectos, así como un marco de seguridad que facilite la colaboración de los componentes de seguridad frente a los ataques selectivos con el fin de garantizar una rápida detección y solución. Por eso McAfee Endpoint Security 10 (que se incluye en la suite), se comunica con varias tecnologías de protección de endpoints en tiempo real para analizar y colaborar frente a las amenazas nuevas y avanzadas, bloqueándolas rápidamente antes de que afecten a sus sistemas y usuarios. Su plataforma ayuda a eliminar las tecnologías duplicadas y a conectar las demás soluciones de Intel Security para facilitar la administración y reforzar las defensas. Además, McAfee Global Threat Intelligence (GTI) proporciona información procedente de la mayor base de datos de observaciones y análisis del mercado.

### Protección avanzada del correo electrónico contra virus y spam

Nuestra solución analiza sus mensajes de correo electrónico entrantes y salientes para interceptar spam, contenidos inapropiados y virus. Podemos poner en cuarentena el correo electrónico de carácter sospechoso para evitar que las nuevas amenazas afecten a su red y a sus usuarios. Y la protección antivirus garantiza la seguridad de su servidor de correo electrónico para impedir que el malware llegue a la bandeja de entrada de los usuarios.

### Protección contra las vulnerabilidades y ataques de tipo zero-day

Olvídese de la aplicación de parches de emergencia. Las tecnologías de prevención de intrusiones y exploits vigilan sin descanso los sistemas de escritorio y portátiles, bloquean la entrada de malware e impiden que ningún código malicioso se apropie de sus aplicaciones o intente ejecutarse con más privilegios. Asimismo, proporciona automáticamente firmas actualizadas que protegen sus computadoras de escritorio y portátiles contra los ataques. Es seguro aplicar y probar los parches a su conveniencia. Si se combina con nuestra tecnología de protección por comportamientos patentada, que impide los ataques por desbordamiento del búfer, conseguirá la solución de protección contra vulnerabilidades más avanzada del mercado.

### Firewall integrado

Bloquee el tráfico entrante no solicitado y controle el tráfico saliente con nuestro firewall, que utiliza McAfee GTI para proteger los sistemas de escritorio y portátiles frente a redes de bots, ataques distribuidos de denegación de servicio (DDoS), amenazas persistentes avanzadas y conexiones web peligrosas. Los sistemas también están protegidos, ya que solo se autoriza el tráfico saliente durante el inicio del sistema, hasta que se haya implementado la directiva de firewall completa.

### Eficiencia en auditorías de directivas y cumplimiento de las normativas

Las auditorías de directivas basadas en el agente analizan endpoints y documentos para garantizar que todas las directivas estén actualizadas. Las empresas también pueden medir el nivel de cumplimiento de las normativas de mejores prácticas —ISO 27001 y CoBIT—, así como de los reglamentos más importantes del sector.

### Control total de dispositivos

Evite que los datos fundamentales salgan de su empresa a través de unidades USB, Apple iPods, dispositivos Bluetooth, o CD y DVD grabables. Nuestras herramientas le ayudan a vigilar y controlar las transferencias de datos desde todos los equipos de escritorio y portátiles, independientemente de dónde vayan los usuarios y los datos confidenciales, incluso cuando no estén conectados a la red de la empresa.

### Seguridad de la Web proactiva

Contribuya a garantizar el cumplimiento de las normativas y a reducir los riesgos asociados a la navegación por Internet. Para ello, alerte a los usuarios sobre los sitios web maliciosos antes de que los visiten. El filtrado web en el host garantiza que pueda autorizar o bloquear sitios web, lo que le permite proteger a los usuarios y asegurar su cumplimiento de las directivas en el momento y el lugar en que naveguen por Internet. Por último, también es posible bloquear URL privadas y se admiten las últimas versiones de múltiples navegadores web.

### Reducción de costos operativos gracias a una administración centralizada

Para aumentar la eficiencia y la visibilidad del estado de seguridad y cumplimiento de normativas, el software McAfee® ePolicy Orchestrator® (McAfee ePO™) proporciona una plataforma única y centralizada que permite administrar la seguridad, implementar la protección y reducir los costos de las operaciones de seguridad.

Correlacione las amenazas, ataques y eventos de seguridad de endpoints, red y datos, así como las auditorías de cumplimiento de normativas, con el fin de mejorar la relevancia y la eficiencia de los esfuerzos de protección y los informes de cumplimiento de las normativas. Ningún otro proveedor posee una única plataforma de administración integrada que cubra todos estos dominios de seguridad. El software McAfee ePO simplifica la administración de la seguridad.

### Despliegue rápido y sencillo

Mejora la protección sin demora. El instalador EASI pone en funcionamiento esta protección robusta con solo unos cuantos clics. La integración con el software McAfee ePO permite desplegar y administrar la seguridad con un único entorno.

### Migrar es fácil

Los entornos que utilizan versiones actuales del software McAfee ePO, McAfee® VirusScan® Enterprise y McAfee Agent pueden disfrutar de nuestra herramienta de migración automática para migrar sus directivas existentes a McAfee Endpoint Security 10 en cuestión de 20 minutos o menos\*.

### Más información

Para obtener más información, visite [www.mcafee.com/mx/products/endpoint-protection/index.aspx](http://www.mcafee.com/mx/products/endpoint-protection/index.aspx).

Función	Por qué es imprescindible
Administración integrada unificada	El software McAfee ePO proporciona visibilidad instantánea de los eventos y del estado de seguridad, y facilita el acceso directo a la administración para controlar de manera centralizada todas sus herramientas de seguridad y de cumplimiento de normativas.
Multiplataforma	Protege la amplia gama de endpoints que necesitan los usuarios avanzados y móviles, incluidos los sistemas Mac, Linux y Microsoft Windows.
Control de dispositivos	Le permite monitorizar y restringir los datos que se copian en dispositivos y soportes de almacenamiento extraíbles para impedir que escapen al control de la empresa.
IPS y firewall integrado para equipos de escritorio y portátiles	Proporciona protección de tipo zero-day frente a las nuevas vulnerabilidades, lo que disminuye la urgencia de aplicar parches y controla las aplicaciones que pueden acceder a la red para detener los ataques propagados por esta vía.
Antimalware	Bloquea virus, troyanos, gusanos, adware, spyware y otros programas potencialmente no deseados que roban datos confidenciales y sabotean la productividad de los usuarios.
Antispam	Ayuda a eliminar el spam, que puede inducir a usuarios desprevenidos a visitar sitios que distribuyen malware y utilizan técnicas de phishing.
McAfee Web Control con filtrado de URL y búsquedas seguras	Ayuda a garantizar el cumplimiento de las normativas, avisa a los usuarios antes de que visiten sitios web maliciosos y les protege tanto si están conectados a la red de la empresa como si no.
Seguridad de servidores de correo electrónico	Protege el servidor del correo electrónico e intercepta el malware antes de que llegue al buzón de entrada del usuario.
Auditoría de directivas	Facilita la elaboración de reportes plenamente integrados sobre cumplimiento para normas como HIPAA, PCI, etc.



McAfee. Part of Intel Security.

6205 Blue Lagoon Drive  
Suite 600  
Miami, Florida 33126  
U.S.A.  
[www.intelsecurity.com](http://www.intelsecurity.com)

\* El tiempo de migración depende de las directivas existentes y del entorno actual.

Intel y los logotipos de Intel y McAfee, ePolicy Orchestrator, McAfee ePO y VirusScan 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. 417\_0816