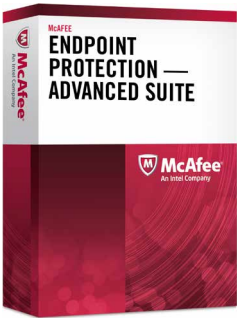


# McAfee Endpoint Protection— Advanced Suite

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



## Características principales

- Proteja los dispositivos 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 en una solución integrada de un solo proveedor, lo que asegura una protección más sólida por un costo inferior
- Incremente la protección de forma inmediata con la facilidad y la eficacia de un entorno de administración centralizado

McAfee recibió la máxima puntuación posible en protección contra exploits de tipo zero-day y ataques por evasión. Consulte NSS Labs Corporate AV/EPP Comparative Analysis, Exploit Evasion Defenses (Análisis comparativo de antivirus y protección de endpoints de NSS Labs: defensas ante las técnicas de evasión de los exploits).

Los principales productos antimalware de McAfee (McAfee VirusScan Enterprise, McAfee Host Intrusion Prevention y McAfee SiteAdvisor Enterprise) lograron un 97 %, la máxima puntuación general, en el informe de la prueba de protección frente a exploits. Consulte NSS Labs Corporate AV/EPP Comparative Analysis, Exploit Protection (Análisis comparativo de antivirus y protección de endpoints de NSS Labs: protección frente a exploits).

Solo unas medidas defensivas que contemplen comportamientos y sistemas pueden proteger los endpoints frente al malware más insidioso, diseñado para evitar la detección basada en firmas antes de que se publiquen los parches. 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 normativas 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.

## Protección antimalware permanente y en tiempo real

Con el crecimiento sin precedentes de las amenazas avanzadas persistentes, las empresas no pueden depender de soluciones que utilicen únicamente el análisis mediante firmas para la protección de los endpoints. Hay un vacío de entre 24 y 72 horas desde el momento en que una amenaza se identifica hasta que su firma se aplica a los endpoints. Entre tanto, sus datos y sistemas están expuestos a la amenaza. Este vacío lo llena la reputación de archivos

del servicio de información global sobre amenazas McAfee Global Threat Intelligence™, ya que ofrece una protección permanente en tiempo real basada en los conocimientos sobre amenazas multivectoriales que reúnen los laboratorios McAfee Labs.

## 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. El sistema de prevención de intrusiones en host vigila sin descanso los endpoints para bloquear la entrada de malware e impedir que ningún código malicioso se apropie de sus aplicaciones. 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. Combinado 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 de control de estado para equipos de escritorio

Es posible controlar las aplicaciones para equipos de escritorio que pueden acceder a la red con el fin de detener los ataques propagados por esta vía y los consiguientes tiempos de inactividad. Despliegue y administre directivas de firewalls según la ubicación para garantizar una protección completa y el cumplimiento de las normativas.

## McAfee establece el estándar del sector

- Reconocido por Gartner como líder en la categoría de seguridad de endpoints y protección de datos móviles
- Primer producto capaz de administrar una amplia gama de soluciones de seguridad (para endpoints, red, datos, entorno web y correo electrónico) mediante una sola consola
- Primer producto de administración de la seguridad de endpoints mediante un único agente y una única consola
- Primera plataforma de administración unificada para la seguridad de endpoints y el cumplimiento de las normativas
- Primera solución en administrar productos de seguridad de McAfee y de terceros
- Primeros en combinar la auditoría de directivas y la implementación de directivas en un único motor
- Primeros en combinar la seguridad de endpoints y la protección de datos en una suite verdaderamente integrada

## Eficacia 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 supervisar y controlar las transferencias de datos desde todas las computadoras 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 le asegura que puede autorizar o bloquear los sitios web, lo que le permite proteger a los usuarios y garantizar su conformidad con las directivas en el momento y el lugar en que naveguen por Internet.

## Reducción de costos operativos gracias a una administración centralizada

Para aumentar la eficacia 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. Basada en la Web para facilitar el acceso en cualquier lugar, ofrece seguridad inteligente para agilizar y optimizar la toma de decisiones y reforzar el control.

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 eficacia 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.

## Cuando los minutos cuentan, Real Time for McAfee ePO es la solución

El software Real Time for McAfee ePO utiliza una metodología peer-to-peer (P2P) escalable para consultar la información de todos sus endpoints en cuestión de minutos, sin necesidad de emplear hardware adicional. De esta forma, los administradores pueden evaluar el estado de seguridad de las defensas de McAfee cuando sea necesario. A continuación, gracias al panel unificado y las acciones predefinidas, el flujo de trabajo desde el diagnóstico hasta mitigar el riesgo lleva minutos, y no días. Esta innovadora tecnología reduce enormemente el riesgo de exposición y el costo de los eventos de seguridad, las interrupciones, las posibilidades de filtraciones y los daños a la reputación. Mejore el conocimiento de la situación y la respuesta a incidentes para los administradores de endpoints de primera línea mediante un enfoque que se adapta perfectamente a las grandes empresas.

## 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).

<b>Función</b>	<b>Por qué es imprescindible</b>
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.
Real Time for McAfee ePO	Visibilidad instantánea del estado de la seguridad de los productos de McAfee. Las acciones en tiempo real garantizan que las defensas estén instaladas, en ejecución, configuradas correctamente y actualizadas.
Multiplataforma	Protege la amplia gama de endpoints que necesitan los usuarios avanzados y móviles, incluidos los de sistemas Mac, Linux y Windows.
Control de dispositivos	Le permite monitorizar y restringir los datos que se copian en los dispositivos y soportes de almacenamiento extraíbles para evitar que escapen al control de la empresa.
Prevención de intrusiones en host y firewall para equipos de escritorio	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 se apoderan de información confidencial y comprometen 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.
Búsqueda y navegación seguras	Contribuye a garantizar el cumplimiento de las normativas y a reducir los riesgos asociados a la navegación por Internet. Para ello, alerta a los usuarios sobre los sitios web maliciosos antes de que los visiten, dejando que sean los administradores los que decidan autorizar o bloquear el acceso a los sitios web.
Filtrado web (host)	Gracias al filtrado de contenido y a la restricción del acceso a los sitios web por usuarios o grupos, controla a los usuarios independientemente de que naveguen por Internet dentro o fuera de la red de la empresa.
Seguridad de servidores de correo electrónico	Protege su servidor de correo electrónico e intercepta el malware antes de que llegue a la bandeja de entrada del usuario.
Auditoría de directivas	Proporciona informes perfectamente integrados sobre el cumplimiento de las normativas HIPAA y PCI, entre otras.

