

## Suite McAfee Endpoint Protection

Proteja los PCs de Windows frente a malware en tiempo real y dispositivos no autorizados

Probablemente, los ordenadores de sobremesa tradicionales y los sistemas fijos de su LAN están protegidos con distintas capas de seguridad de gateways y de red. Aun así necesitan funciones básicas de seguridad que bloqueen el malware avanzado, que controlen las pérdidas de datos y los riesgos de cumplimiento de normativas que generan los soportes extraíbles y que proporcionen acceso seguro al correo electrónico y a las aplicaciones web, cuyo uso es crucial. La suite McAfee® Endpoint Protection integra estas funciones imprescindibles en un único entorno de fácil administración, ideal para proteger los equipos de sobremesa y otros sistemas tradicionales que tienen una exposición limitada a las amenazas de Internet.

### Puntos clave

- Protección fundamental con seguridad consolidada de endpoints y datos
- Reducción del tiempo y el esfuerzo invertidos en desplegar y administrar la seguridad
- Protección adecuada para ordenadores de sobremesa tradicionales y fijos con un solo producto



Mejor solución antimalware y mejor solución de seguridad para empresas

¿Qué tienen en común un centro de llamadas, un estudio de ingeniería y la consulta de un médico? Que en todos ellos se utilizan torres y ordenadores tradicionales de sobremesa que nunca salen de la oficina. Dado que estos sistemas no visitan puntos de acceso inalámbrico gratuitos, que no los emplean sus hijos para navegar por Internet a escondidas ni son susceptibles de ser olvidados en un aeropuerto, corren menos riesgo de sufrir ataques informáticos, recibir descargas maliciosas o ser robados con datos confidenciales en su interior. Sin embargo, los usuarios de empresa utilizan masivamente el correo electrónico y las aplicaciones basadas en la Web, por lo que también las máquinas fijas necesitan una protección avanzada frente a los ataques de malware selectivo y en tiempo real que transmiten estas aplicaciones. El servidor de correo electrónico debe contar con una capa extra de defensas antimalware, reforzada por la protección antimalware de cada endpoint en cuestión.

Además, la mayoría de los ordenadores modernos tiene varios puertos USB y unidades de DVD. En nuestro caso del centro de llamadas, estudio de ingeniería o consulta médica, un empleado descontento puede llevarse a casa bases de datos de clientes, diseños técnicos u otra propiedad intelectual, o historias clínicas y datos financieros de pacientes. Los controles de dispositivos pueden ayudarle a restringir el uso de soportes extraíbles y dispositivos de almacenamiento portátiles para evitar estas pérdidas de datos.

La suite McAfee Endpoint Protection integra perfectamente varias soluciones probadas de seguridad para gestionar todos estos riesgos, mejorando la eficacia operativa y el ahorro de costes cómodamente con una sola solución.

### 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™. Bloquea o pone en cuarentena virus, troyanos, gusanos, adware, spyware y otros programas potencialmente no deseados que se apoderan de información confidencial y comprometen la productividad de los usuarios.

### Protección avanzada contra virus y spam que se propagan a través del correo electrónico

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.

### Control total de dispositivos

Con nosotros es posible evitar que los datos fundamentales salgan de su empresa a través de soportes extraíbles, como unidades USB, iPods, dispositivos Bluetooth, o CD y DVD grabables. Nuestras herramientas le ayudan a supervisar y controlar las transferencias de datos desde todos los equipos de sobremesa, incluso cuando no están conectados a la red corporativa.

**McAfee establece el estándar del sector**

- Reconocido por Gartner durante cuatro años seguidos entre los líderes en la categoría de seguridad de endpoints y protección de datos móviles
- Primer producto capaz de administrar una amplia gama de soluciones de seguridad (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 de 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 seguridad de endpoints y la protección de datos en una suite verdaderamente integrada

**Plataformas operativas admitidas**

**Estaciones de trabajo**  
(nota: la compatibilidad con sistemas operativos de 64 bits está disponible para algunas tecnologías).

- Windows 7 o Embedded
- Windows Vista
- Windows XP Home, Professional, Embedded (WEPOS), Tablet PC
- Windows 2000 Professional con Service Pack 2 (SP2) o superior

**Servidores** (nota: la compatibilidad con sistemas operativos de 64 bits está disponible para algunas tecnologías).

- Windows Server 2008, Hyper-V, Core, Datacenter, Storage Server, Cluster Server, Small Business Server
- Windows Server 2003, Storage Server, Cluster Server, Datacenter, Small Business Server
- Windows Server 2000, Advanced Server, Small Business Server

**Requisitos del servidor de correo electrónico**

- Microsoft Exchange 2003 SP1; 2007 (64 bits); 2010 (v7.0.2)
- Microsoft Exchange 2000 SMB, 2003 Server o Advanced Server
- Lotus Domino 6.0.3-6.0.5; 7.0; 8.0 (32 bits); 8.5 (32 bits)

**Firewall de control de estado para equipos de sobremesa**

Controle las aplicaciones de escritorio que pueden acceder a la red para detener los ataques propagados por esta vía y los consiguientes tiempos de inactividad. Puede desplegar y administrar directivas de firewalls según la ubicación para garantizar una protección completa y el cumplimiento de las normativas.

**Seguridad web proactiva**

En Internet, muchas amenazas son invisibles y pasan desapercibidas para los usuarios. 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. También puede autorizar o bloquear el acceso a sitios web por usuario y grupo, y controlar el acceso de los usuarios a sitios confidenciales o inapropiados, como los de juegos y contenido para adultos.

**Reducción de costes de explotación gracias a una administración centralizada**

Todas las funciones de la suite McAfee Endpoint Protection se gestionan con el software McAfee ePolicy Orchestrator® (ePO™), una plataforma centralizada que administra la seguridad, implementa la protección y reduce el coste de las operaciones de seguridad. Basada en la Web para facilitar el acceso, ofrece seguridad inteligente para agilizar y optimizar la toma de decisiones y reforzar el control.

McAfee ePO permite recortar el coste de administrar la seguridad de TI y el cumplimiento de las normativas en más del 60% (fuente: MSI International, estudios sobre 488 medianas y grandes empresas).

Este concepto abierto de la infraestructura de administración se basa en un único agente y una sola consola. En comparación con las soluciones individuales de generaciones anteriores, nuestro modelo racionalizado simplifica enormemente la instalación y el mantenimiento de las medidas de defensa, así como de sus reglas y directivas. Además, elimina el impacto que tiene en los sistemas la actuación de varios agentes y los conflictos de decisiones derivados del uso de distintas consolas. Cuando se deben revisar las directivas, las actualizaciones se realizan de manera rápida, precisa y coherente. Además, puede correlacionar las amenazas, ataques y eventos de la 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 normativas. Ningún otro proveedor posee una única plataforma de administración integrada que cubra todos estos dominios de seguridad.

**Más información**

Para obtener más información, visite [www.mcafee.com/endpoint](http://www.mcafee.com/endpoint).

| Función  | Por qué necesita esta solución  |
|--|---|
| <b>Administración integrada unificada</b>            | McAfee ePolicy Orchestrator (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.   |
| <b>Control de dispositivos</b>                       | 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.   |
| <b>Firewall para equipos de sobremesa</b>            | Garantiza la prevención de ataques procedentes de la red y la exclusiva autorización del tráfico legítimo.  |
| <b>Antimalware</b>                                   | 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.  |
| <b>Antispam</b>                                      | Ayuda a eliminar el spam, que puede inducir a usuarios desprevenidos a visitar sitios que distribuyen malware y captan datos personales y financieros con técnicas de phishing.   |
| <b>Seguridad de servidores de correo electrónico</b> | Protege su servidor de correo electrónico e intercepta el malware antes de que llegue a la bandeja de entrada del usuario.  |
| <b>Búsqueda y navegación seguras</b>                 | Ayuda 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. |



McAfee, S.A.  
Avenida de Bruselas nº 22  
Edificio Sauce  
28108 Alcobendas  
Madrid, España  
Teléfono: +34 91 347 8535  
[www.mcafee.com/es](http://www.mcafee.com/es)

McAfee, el logotipo de McAfee, McAfee ePolicy Orchestrator, McAfee ePO, McAfee Global Threat Intelligence y McAfee Labs son marcas comerciales registradas o marcas comerciales de McAfee, Inc. o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros. La planificación, las especificaciones y las descripciones de productos incluidas en este documento se proporcionan únicamente a título informativo y están sujetas a cambios sin previo aviso. Además, se incluyen sin garantía alguna, ni expresa ni implícita. Copyright ©2010 McAfee, Inc. 14005ds\_eps\_0910\_fnl\_ASD