



# McAfee Server Security Suite Advanced

**Obtenga una seguridad avanzada para servidores en despliegues físicos, virtuales y en la nube con listas blancas.**

## Ventajas principales

- Descubre todos los servidores físicos y virtuales, incluidos los alojados en la nube, con administración desde un solo panel en una consola central.
- Combina listas blancas y listas negras para proteger los servidores físicos y virtuales contra el malware.
  - Proporciona listas blancas dinámicas para protegerse contra amenazas desconocidas garantizando la seguridad de los hosts. Para ello, evita que las aplicaciones no deseadas puedan ejecutarse a través de McAfee Application Control for Servers.
  - Detecta continuamente los cambios a nivel de sistemas en las ubicaciones distribuidas y remotas para favorecer los requisitos de cumplimiento.

Durante los últimos años, el centro de datos ha experimentado cambios importantes en los sistemas de almacenamiento, servidores, redes y aplicaciones que ofrece. Su heterogeneidad y la rápida evolución hacia la computación en la nube exigen nuevos modos de proteger este entorno. Entre los profesionales de TI y de seguridad empresariales, el reto consiste en crear un enfoque de seguridad unificado y sólido para los entornos físicos, virtualizados y basados en la nube que ayude a asegurar su agilidad y rentabilidad. McAfee® Server Security Suite Advanced —parte de la oferta de productos de Intel® Security— ofrece la protección y la administración más exhaustivas de servidores en entornos físicos, virtuales y en la nube, proporcionando al mismo tiempo seguridad para servidores avanzada adicional, con funciones de listas blancas y control de cambios, para garantizar el cumplimiento continuo de las normativas.

## Descubra todas las cargas de trabajo

Suele ser difícil descubrir todas las cargas de trabajo y, a continuación, aplicar directivas de seguridad adecuadas en todos los despliegues físicos, virtuales y en la nube. Con reportes de análisis que permiten detectar los endpoints no protegidos y determinar el cumplimiento de las normas de seguridad, hemos simplificado la administración. Mediante los conectores para el software McAfee® ePolicy Orchestrator® (McAfee ePO™), McAfee Server Security Suite Advanced le permite descubrir todos los servidores físicos y virtuales, incluidos los de

la nube pública y privada. La solución incluye además conectores McAfee Data Center Connector for VMware vSphere, Amazon AWS, OpenStack y Microsoft Azure. Juntos, estos conectores le permiten supervisar todas las máquinas virtuales tanto in situ como de forma remota, así como aplicar directivas de seguridad específicas que proporcionan un gran nivel de seguridad. Los paneles muestran el estado de la seguridad, con la protección de memoria del sistema operativo, la posibilidad de ver qué host ejecuta cada máquina virtual y la ubicación de cada máquina virtual, entre otra información.

### Ventajas principales (continuación)

- Ofrece seguridad de virtualización optimizada para minimizar el impacto en el rendimiento con McAfee MOVE AntiVirus.
- Ofrece visibilidad total del estado de la seguridad de todas las máquinas virtuales de la nube pública y privada a través de conectores McAfee Data Center Connector for VMware vSphere, Amazon Web Services, OpenStack y Microsoft Azure.

### Proteja los servidores

McAfee Server Security Suite Advanced ofrece la protección más global para sus servidores, ya sean físicos, virtualizados o alojados en la nube. Además, proporciona control de cambios y una combinación exclusiva de tecnologías de protección con listas blancas y listas negras, única en el sector.

McAfee Server Security Suite Advanced incluye McAfee Application Control for Servers, una solución de listas blancas que solo permite ejecutar en los servidores el software autorizado. Esta solución de administración centralizada con listas blancas emplea un modelo de confianza dinámico y funciones de seguridad innovadoras que bloquean las aplicaciones no autorizadas y frustran las amenazas persistentes avanzadas (APT), evitándole la laboriosa tarea de administrar las listas. Las listas blancas reducen significativamente el impacto sobre el rendimiento del host gracias a la protección contra amenazas sin actualizaciones de firmas.

Como parte de la protección básica del servidor, la suite ofrece soluciones antimalware tradicionales para servidores Microsoft Windows y Linux, incluido el software McAfee VirusScan® Enterprise, que es el número uno contra exploits zero-day y ataques por evasión, según NSS Labs. Además del antimalware tradicional, la suite también incorpora una solución independiente especializada en entornos virtuales. McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus optimiza el antivirus para entornos virtualizados, minimizando el impacto en el rendimiento incluso en entornos dinámicos y de gran tamaño, y proporcionando soporte para todos los hipervisores principales. McAfee MOVE AntiVirus está disponible como opción sin agente adaptada para entornos VMware o como opción multiplataforma que puede desplegarse para entornos de hipervisores basados en KVM, Microsoft Hyper-V, VMware y Xen.

Aunque el antivirus es clave para la seguridad, pueden hacer falta otras soluciones a fin de protegerse de las amenazas avanzadas. Se incluye McAfee Host Intrusion Prevention

para proteger a las empresas contra las amenazas de seguridad complejas que pueden introducirse o permitirse de manera intencionada o desapercibida.

### Extiéndase a la nube

Cuando una empresa se extiende a la nube, cada vez le resulta más difícil garantizar la aplicación de las directivas de seguridad correctas a las nuevas cargas de trabajo. McAfee supera estas dificultades descubriendo automáticamente las máquinas virtuales en ejecución y detenidas a medida que se aprovisionan en las nubes privada y pública. Para ello, basta con registrar una cuenta en la nube pública en la plataforma McAfee ePO. A continuación, se pueden proteger las máquinas virtuales automáticamente con las directivas de seguridad apropiadas. Además, el panel de seguridad del centro de datos de McAfee ofrece visibilidad total del estado de protección y los incidentes de seguridad en sus nubes pública y privada.

### Optimización de los servidores, optimización de la empresa

El enorme potencial de la virtualización y la computación en la nube solo se aprovecha completamente si se protegen convenientemente. Las soluciones de seguridad para servidores que proporciona McAfee son capaces de crecer a medida que evolucionan las empresas. Ya se trate de un entorno físico, virtualizado o en la nube, McAfee ofrece una suite de soluciones para asegurar la protección de los servidores sin perder flexibilidad. McAfee Server Security Suite Advanced protege los servidores físicos, virtuales y alojados en la nube a base de soluciones avanzadas que establecen y mantienen una infraestructura de seguridad sólida en toda la organización.

Encontrará más información sobre las ventajas de McAfee Server Security Suite Advanced en [www.mcafee.com/mx/products/server-security-suite-advanced.aspx](http://www.mcafee.com/mx/products/server-security-suite-advanced.aspx).

<b>Función</b>	<b>Por qué es imprescindible</b>
<b>Listas blancas de aplicaciones</b>	<ul style="list-style-type: none"><li>• Su impacto en el rendimiento del host es considerablemente menor que con los tradicionales controles de seguridad para endpoints.</li><li>• Protección contra las amenazas persistentes avanzadas (APT) y de tipo zero-day sin actualizaciones de firmas, lo que disminuye el tiempo que se tarda en conseguir protección.</li><li>• Uso de listas blancas dinámicas, que requiere menos gastos generales operativos que las listas tradicionales.</li></ul>
<b>Control de cambios</b>	<ul style="list-style-type: none"><li>• Evita la manipulación bloqueando los cambios no autorizados en archivos, directorios y configuraciones de sistemas críticos, ahorrándoles a los administradores tiempo en resolver las brechas en la seguridad.</li><li>• Esta solución detecta y valida cada intento de cambio efectuado en tiempo real en su servidor e implementa la directiva de cambios por intervalo de tiempo, por origen o por ficha de trabajo aprobada.</li><li>• Este control permanente reduce al mínimo la repercusión de los cambios ad hoc o no autorizados.</li></ul>
<b>Consola única de administración</b>	<ul style="list-style-type: none"><li>• Administración desde un solo panel de servidores físicos y virtuales, incluidos los alojados en nubes públicas y privadas, para una mayor visibilidad de la seguridad</li><li>• Simplificación de los aspectos operativos y la inversión de tiempo necesario para el personal administrativo</li><li>• Costos de hardware inferiores debido a una reducción de servidores necesarios</li></ul>
<b>Protección del núcleo del servidor</b>	<ul style="list-style-type: none"><li>• Protección antimalware para servidores físicos considerada por NSS Labs<sup>1</sup> número uno en protección frente a exploits de tipo zero-day y ataques de evasión</li><li>• Host Intrusion Prevention para proteger a las empresas de las amenazas de seguridad complejas que pueden introducirse de manera intencionada o no</li></ul>
<b>Seguridad para la virtualización</b>	<ul style="list-style-type: none"><li>• Optimización de la seguridad de las cargas de trabajo desplegada en infraestructuras virtuales sin afectar al rendimiento ni a la utilización de recursos</li><li>• Protección de varios hipervisores en el centro de datos para tener un nivel de seguridad único para todos los tipos de hipervisores utilizados</li><li>• Despliegue sin agente optimizado para entornos basados en VMware con el fin de mejorar el rendimiento y la densidad de máquinas virtuales</li></ul>
<b>Visibilidad completa de máquinas virtuales en la nube privada y pública</b>	<ul style="list-style-type: none"><li>• Descubra no solamente los servidores físicos sino también los hipervisores y máquinas virtuales en entornos VMware vSphere, Amazon AWS, OpenStack y Microsoft Azure para disfrutar de visibilidad total de todo lo que necesita protección.</li><li>• Descubra cuándo se aprovisionan las máquinas virtuales y cuáles pueden protegerse automáticamente con directivas de seguridad para garantizar un estado de seguridad adecuado para ellas.</li></ul>



**McAfee. Part of Intel Security.**

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

1. NSS Labs, Inc., Protection & Evasion Test (Prueba sobre protección y ocultación), 2013