



# McAfee Server Security Suite Essentials

**Obtenga una seguridad de base para servidores en instalaciones físicas, virtuales y alojadas en la nube.**

## **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.
- 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.

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 (cloud computing) 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 Essentials —parte de la oferta de productos de Intel® Security— permite superar estos retos mediante la integración de componentes de seguridad esenciales para descubrir cargas de trabajo en la nube, proteger servidores y ampliar la seguridad a la nube.

## **Descubra todas las cargas de trabajo**

Suele ser difícil descubrir todas las cargas de trabajo y, a continuación, aplicar directivas de seguridad adecuadas. Con informes 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 Essentials le permite descubrir todos los servidores físicos y virtuales, incluidos los de la nube pública y privada. La solución incluye conectores McAfee Data Center Connector for VMware vSphere, Amazon AWS, OpenStack y Microsoft Azure. Estos conectores permiten supervisar cada máquina virtual, in situ o de forma remota, y aplicar directivas específicas que mejoran enormemente la seguridad. La visibilidad adicional incluye protección de memoria del

sistema operativo, la posibilidad de ver en qué host se ejecuta cada máquina virtual y en qué centro de datos o en qué nube aloja cada máquina virtual, entre otra información.

## **Proteja los servidores**

McAfee Server Security Suite Essentials incluye el software McAfee VirusScan® Enterprise, que es el número uno según NSS Labs en la lucha contra exploits de tipo zero-day y ataques por evasión<sup>1</sup>. Además del antimalware tradicional, la suite ofrece también una solución independiente especializada para entornos virtuales. McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus optimiza la tecnología 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 los antivirus son fundamentales para la seguridad, es posible que se requieran otras soluciones para protegerse contra 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

Al llevar las cargas de trabajo a la nube, aumenta la dificultad para garantizar que las directivas de seguridad adecuadas se apliquen convenientemente. 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 el software 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 no limitan las posibilidades de crecimiento a medida que las empresas evolucionan. 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 Essentials sienta las bases fundamentales para la seguridad de los servidores físicos, virtuales y alojados en la nube.

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

Función	Por qué es imprescindible
<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>• Costes 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 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.

Avenida de Bruselas n.º 22  
Edificio Sauce  
28108 Alcobendas  
Madrid, España  
Teléfono: +34 91 347 8500  
[www.intelsecurity.com](http://www.intelsecurity.com)

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