McAfee Host Intrusion Prevention for Server

Protección avanzada contra vulnerabilidades para servidores y aplicaciones

Los servidores de las empresas almacenan los activos de información más valiosos y son responsables del funcionamiento de la empresa. Uno de los desafíos principales para los responsables de TI es conseguir que estos servidores, así como las aplicaciones que albergan estén protegidos frente a los ataques conocidos y desconocidos que amenazan con interrumpir la marcha del negocio.

McAfee Host Intrusion Prevention for Server

McAfee® Host Intrusion Prevention for Server proporciona protección para servidores web y de bases de datos especializados, con el fin de mantener el tiempo de actividad del servidor y la continuidad del negocio, y funciona junto con el único firewall de la industria que es dinámico y que ofrece seguimiento de estado para proteger contra amenazas avanzadas y tráfico malicioso. Además, proporciona protección con un sistema de prevención de intrusiones (IPS) basado en firmas y comportamientos. McAfee Host Intrusion Prevention for Server reduce la frecuencia y la urgencia de aplicación de los parches, preserva la continuidad del negocio y la productividad de los empleados, protege la confidencialidad de los datos y simplifica el cumplimiento de normativas.

Defienda sus servidores y aplicaciones frente a ataques y evite la pérdida de datos

Cada vez con más frecuencia el objetivo de los ataques son los servidores. Esto se debe a que albergan grandes cantidades de datos y son fundamentales para realizar las actividades cotidianas. McAfee Host Intrusion Prevention for Server protege los servidores esenciales para garantizar el tiempo de actividad de los sistemas y la productividad de los empleados.

- Protección del servidor web:
  - Filtrado de solicitudes HTTP para evitar los ataques de salto de directorio, Unicode y de denegación de servicio.
  - Uso de directivas y reglas de protección predefinidas para evitar los ataques y la pérdida de datos.

Ventajas principales

Mayor protección

- Aplique la mayor protección de IPS y frente a amenazas de tipo zero-day a todos los niveles: red, aplicaciones y ejecución.

Reducción de costos

- Reduzca el tiempo y los costos con una única consola potente y unificada para despliegue, administración, generación de informes y auditoría de eventos, directivas y agentes.
- Aplique los parches a los endpoints con menos frecuencia y urgencia.

Cumplimiento de normativas simplificado

- Gestione el cumplimiento de normativas con sencillas vistas procesables, flujos de trabajo, supervisión de eventos e informes, que facilitan la realización de investigaciones y análisis forenses de manera puntual y correcta.

- Protección del servidor de bases de datos:
  - Examen de las consultas a las bases de datos para prevenir ataques, como la inyección de SQL.
  - Uso de directivas y reglas de protección predefinidas para garantizar un comportamiento normal y evitar la alteración de los datos.

Protección contra amenazas avanzadas mediante nuestro firewall de sistemas dinámico y con seguimiento de estado

A diferencia de los firewalls de sistemas tradicionales que se basan únicamente en reglas específicas, McAfee Host Intrusion Prevention for Server ha integrado la reputación de conexiones de redes de McAfee Global Threat Intelligence (McAfee GTI) para proteger los servidores contra amenazas avanzadas, como las redes de bots, los ataques de denegación de servicio distribuidos (DDoS) y el nuevo tráfico malicioso, antes de que se produzcan los ataques. Con el aumento de las amenazas avanzadas, McAfee GTI ofrece la protección más sofisticada que se puede desplegar.

Aplique los parches con menos frecuencia y urgencia, y a su propio ritmo

En un alto porcentaje, los exploits se lanzan a los tres días de descubrirse una vulnerabilidad. Pero en muchas empresas se puede tardar hasta 30 días en probar y desplegar los parches en todos los endpoints.

McAfee Host Intrusion Prevention for Server cierra la brecha en la seguridad y al mismo tiempo facilita la aplicación de parches y aumenta su eficacia.

- Se ofrece protección contra las vulnerabilidades de Microsoft y Adobe. La protección en cuanto a vulnerabilidades actualiza automáticamente las firmas para proteger los endpoints frente a los ataques que aprovechan dichas vulnerabilidades.
- Las actualizaciones de firmas se pueden descargar de manera automática y regular, para garantizar la protección.

Los servidores ya no son vulnerables durante el inicio

Los servidores son vulnerables durante el inicio del sistema cuando aún no se han implementado las directivas de seguridad. Durante este período de vulnerabilidad, los servidores pueden estar sometidos a ataques basados en la red y es posible que los servicios de seguridad estén desactivados. McAfee Host Intrusion Prevention for Server bloquea los ataques durante este intervalo con protección en el inicio mediante un sistema de prevención de intrusiones (IPS) y un firewall.

- La protección con firewall al inicio solo autoriza el tráfico saliente durante el inicio del sistema, hasta que se haya implementado la directiva de firewall completa.
- La protección mediante IPS al inicio impide que nuestros servicios de seguridad se desactiven durante el inicio del sistema, hasta que se haya implementado la directiva de IPS completa.

Requisitos del sistema

Requisitos mínimos de hardware

- Intel o AMD x86 y x64
- Espacio libre en disco (cliente): 15 MB, pero 100 MB durante la instalación
- Memoria: 256 MB de RAM
- Entorno de red: Redes Microsoft o Novell NetWare. Las redes NetWare requieren TCP/IP
- NIC: tarjeta de interfaz de red; 10 Mbits/s o superior

Sistemas operativos admitidos:

- Microsoft Windows Server 2003 SP2, 2003 R2, 2003 R2 SP2 (todas las ediciones, de 32 o 64 bits)
- Microsoft Windows Server 2008, 2008 SP1, 2008 SP2, 2008 R2 (todas las ediciones, de 32 o 64 bits)
- SPARC Solaris 9 sun4u (de 32 o 64 bits)
- SPARC Solaris 10 sun4u, sun4v (de 32 o 64 bits)
- Red Hat Linux Enterprise 4, de 32 bits
  - 2.6.9-5.EL
  - 2.6.9-5.Elhugemem
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 4, de 64 bits
  - 2.6.9-5.EL
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 5, de 32 bits
  - 2.6.18-8.el5
  - 2.6.18-8.el5PAE
- Red Hat Linux Enterprise 5, de 64 bits
  - 2.6.18-8.el5
- SUSE Linux Enterprise 10, de 32 bits
  - 2.6.16.21-0.8-bigsmp
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp

Administración simplificada y directa

En una gran empresa es necesario crear y mantener numerosas directivas de firewall y de prevención de intrusiones, sin embargo esta suele ser una tarea tediosa y que lleva mucho tiempo. La directiva de McAfee Host Intrusion Prevention for Server y los catálogos de IPS simplifican el proceso, y le permiten crear y mantener varias directivas de firewall y de IPS que pueden aplicarse según sus necesidades.

Optimice y simplifique aún más la administración con el software McAfee® ePolicy Orchestrator® (McAfee ePO™), nuestra consola centralizada que le ayuda a supervisar y administrar toda sus seguridad. La integración total con el software McAfee ePO le ahorra tiempo y dinero con una importante eficacia operativa.

Para obtener más información, póngase en contacto con nuestro representante o visite nuestro sitio web **www.mcafee.com/mx**.

Compatibilidad con las principales plataformas de virtualización

Prácticamente la totalidad de los departamentos de TI han adoptado la virtualización, y la compatibilidad con las principales plataformas de virtualización es un requisito imprescindible para que cualquier producto triunfe. McAfee Host Intrusion Prevention for Server 8.0 es compatible con las tres plataformas de virtualización principales: VMware, Citrix y Microsoft Hyper-V. En la tabla siguiente se citan los productos que admiten cada uno de estos tres proveedores.

VMware	Citrix	Microsoft
VMware ESX–3.5 y 4.0	Citrix XenServer–5.0 y 5.5	Microsoft Hyper-V Server 2008 y 2008 R2
VMware Vsphere–4.0	Citrix XenDesktop–3.0 y 4.0	Microsoft VDI
VMware View–3.1 y 4.0	Citrix XenApp–5.0 y 6.0	Microsoft App-V–4.5 y 4.6
VMware ThinApp–4.0 y 4.5		Modo de Windows XP en Windows 7
VMware ACE–2.5 y 2.6		
VMware Workstation 6.5 y 7.0		
VMware Player–2.5 y 3.0		

Requisitos del sistema (continuación)

Sistemas operativos admitidos (continuación):

- SUSE Linux Enterprise 10, de 64 bits
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 11, de 32 bits
  - 2.6.27.19-5-default
  - 2.6.27.19-5-pae
- SUSE Linux Enterprise 11, de 64 bits
  - 2.6.27.19-5-default

Servidores web compatibles

- Microsoft Windows
  - IIS 6.0 y 7.0
- SPARC Solaris
  - Servidor web Apache 1.3.6 y posteriores
  - Servidor web Apache 2.0.42 o posteriores
  - Servidor web Apache 2.2.3 o posteriores
  - Sun Java Web Server 6.1
  - Sun Java Web Server 7.0
- Linux (RHEL y SUSE)
  - Servidor web Apache 1.3.6 o posteriores
  - Servidor web Apache 2.0.42 o posteriores
  - Servidor web Apache 2.2.3 o posteriores

Servidores de base de datos admitidos

- Microsoft SQL Server 2005 y 2008

McAfee
Together is power.

Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
+52-55-50890250
www.mcafee.com/mx