McAfee Host Intrusion Prevention for Server

Advanced vulnerability protection for servers and applications

Corporate servers house an organization's most valuable information assets and keep the business running. One of the top IT challenges is to successfully protect these servers and the applications they host from known and unknown attacks that threaten to disrupt business.

Key Advantages

Stronger protection

- Enforce the broadest IPS and zero-day threat protection coverage across all levels: network, application, and execution

Lower costs

- Reduce time and costs with one powerful, unified console for deployment, management, reporting, and auditing of events, policies, and agents
- Patch endpoints less frequently and with less urgency

Simplified compliance

- Manage compliance with easy-to-understand actionable views, workflow, event monitoring, and reporting for prompt and proper investigation and forensics

McAfee Host Intrusion Prevention for Server

McAfee® Host Intrusion Prevention for Server delivers specialized web and database server protection to maintain system uptime and business continuity along with the industry's only dynamic and stateful firewall to shield against advanced threats and malicious traffic. In addition, it also provides signature and behavioral intrusion prevention system (IPS) protection. McAfee Host Intrusion Prevention for Server reduces patching frequency and urgency, preserves business continuity and employee productivity, protects data confidentiality, and simplifies regulatory compliance.

Defend servers and applications from attacks, and prevent data loss

Servers are increasingly the target of attacks because they house large amounts of corporate data and are also critical for performing day-to-day activities. McAfee Host Intrusion Prevention for Server secures mission-critical servers to maintain system uptime and productivity.

- Web server protection
  - » Filter HTTP requests to prevent directory traversal, Unicode, and denial-of-service (DoS) attacks
  - » Use predefined shielding policies and rules to prevent attacks and loss of data
- Database server protection
  - » Examine database queries to prevent attacks, such as SQL injection
  - » Use predefined shielding policies and rules to ensure normal behavior and prevent tampering of data

Advanced threat protection through our dynamic, stateful system firewall

Unlike traditional system firewalls that rely on specific rules, McAfee Host Intrusion Prevention for Server has integrated McAfee Global Threat Intelligence™ network connection reputation to protect servers against advanced threats such as botnets, distributed denial-of-service (DDoS), and emerging malicious traffic before attacks can occur. With the increase in advanced threats, McAfee Global Threat Intelligence offers the most sophisticated protection you can deploy.

Apply operating system and application patches less frequently, less urgently, and on your own schedule

A large percentage of exploits are released as early as three days after disclosure of the vulnerabilities. Yet, for many organizations, it may take up to 30 days to test and deploy patches for all endpoints. McAfee Host Intrusion Prevention for Server bridges the security gap while making the patching process easier and more efficient.

- Out-of-the-box protection boasts a superior track record. McAfee Host Intrusion Prevention for Server protects against an average of 97 percent of exploits[1]. Protection is afforded against both Microsoft and Adobe vulnerabilities. Vulnerability shielding automatically updates signatures to protect endpoints against attacks resulting from exploited vulnerabilities
- Signature updates can be automatically and regularly downloaded for protection assurance

1 *NSS Labs Endpoint Protection Products Group Test Report: Host Intrusion Prevention,* Q2 2010

System Requirements

Minimum hardware requirements

- Intel or AMD x86 and x64
- Free disk space (client): 15 MB, but 100 MB during installation
- Memory: 256 MB RAM
- Network environment: Microsoft or Novell NetWare networks. NetWare networks require TCP/IP
- NIC: Network interface card; 10 mbps or higher

Supported operating systems

- Microsoft Windows Server 2003 SP2, 2003 R2, 2003 R2 SP2 (all editions, 32- and 64-bit)
- Microsoft Windows Server 2008, 2008 SP1, 2008 SP2, 2008 R2 (all editions, 32- and 64-bit)
- SPARC Solaris 9 sun4u (32- and 64-bit)
- SPARC Solaris 10 sun4u, sun4v (32- and 64-bit)
- Red Hat Linux Enterprise 4, 32-bit
  - 2.6.9-5.EL
  - 2.6.9-5.Elhugemem
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 4, 64-bit
  - 2.6.9-5.EL
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 5, 32-bit
  - 2.6.18-8.el5
  - 2.6.18-8.el5PAE
- Red Hat Linux Enterprise 5, 64-bit
  - 2.6.18-8.el5
- SUSE Linux Enterprise 10, 32-bit
  - 2.6.16.21-0.8-bigsmp
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 10, 64-bit
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 11, 32-bit
  - 2.6.27.19-5-default
  - 2.6.27.19-5-pae
- SUSE Linux Enterprise 11, 64-bit
  - 2.6.27.19-5-default

Supported web servers

- Microsoft Windows
  - IIS 6.0 and 7.0
- SPARC Solaris
  - Apache 1.3.6 and later Web Server
  - Apache 2.0.42 or later Web Server
  - Apache 2.2.3 or later Web Server
  - Sun Java Web Server 6.1
  - Sun Java Web Server 7.0
- Linux (RHEL and SUSE)
  - Apache 1.3.6 or later Web Server
  - Apache 2.0.42 or later Web Server
  - Apache 2.2.3 or later Web Server

Supported database servers

- Microsoft SQL Server 2005 and 2008

Servers are no longer vulnerable during startup

Servers are vulnerable during startup because the security policies have not yet been enforced. During this vulnerable startup time, they could be subject to network-based attacks and security services could be disabled. McAfee Host Intrusion Prevention for Server blocks attacks from occurring during this vulnerable window with firewall and IPS startup protection.

- Startup firewall protection allows only outbound traffic during startup until the complete firewall policy has been enforced
- Startup IPS protection prevents McAfee security services from being disabled during startup until the complete IPS policy has been enforced

Simplified and streamlined management

Creating and maintaining multiple firewall and IPS policies is necessary in a large organization but is usually tedious and time consuming. McAfee Host Intrusion Prevention for Server policy and IPS catalogs streamline that process, allowing you to create and maintain multiple firewall and IPS policies that can be applied as needed.

Optimize and simplify management further with McAfee ePolicy Orchestrator® (McAfee ePO™) software, our single, centralized console, which helps you oversee and administer all your protection. Full integration with McAfee ePO software saves you money and time with significant operational efficiencies.

For more information, please contact a McAfee representative, or visit our website at www.mcafee.com.

Compatibility with major virtualization platforms

Virtualization has been adopted by practically all IT departments and compatibility with the major virtualization platforms is essential for any product to be successful. McAfee Host Intrusion Prevention for Server 8.0 is compatible with the three major virtualization platforms, VMware, Citrix, and Microsoft Hyper-V. The following table lists the supported products from each of these three vendors.

VMware	Citrix	Microsoft
VMware ESX–3.5 & 4.0	Citrix XenServer–5.0 & 5.5	Microsoft Hyper-V Server 2008 & 2008 R2
VMware Vsphere–4.0	Citrix Xen Desktop–3.0 & 4.0	Microsoft VDI
VMware View–3.1 & 4.0	Citrix Xen App–5.0 & 6.0	Microsoft App-V–4.5 & 4.6
VMware ThinApp–4.0 & 4.5		XP Mode on Windows 7
VMware ACE–2.5 & 2.6		
VMware Workstation 6.5 & 7.0		
VMware Player–2.5 & 3.0		

McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

17802ds_hips-server_1110_fnl_ASD