Data Sheet

McAfee Host Intrusion Prevention for Desktop

Advanced vulnerability protection for desktops and laptops

Managing security and controlling connectivity for desktop and laptop computers across an organization is increasingly challenging with the growing number of profit-driven cybercriminals and the sophisticated nature of today's threats. As workers become increasingly mobile, that places additional pressure on IT to ensure that users connect safely to the corporate network. Additionally, organizations need zero-day protection against threats to gain more time to be able to properly prioritize, test, and deploy the necessary patches.

Key Advantages

Stronger protection

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

The Challenge

Anti-virus alone is not enough, as attacks and vulnerability exploits are being released faster and are becoming more complex. The solution is to implement a proactive security strategy that prevents attacks from happening in the first place. With a proactive approach to securing endpoints, IT departments can ensure that all endpoints and confidential data are protected and business continuity is maintained.

McAfee Host Intrusion Prevention for Desktop

As an integral part of McAfee endpoint suites, McAfee® Host Intrusion Prevention for Desktop delivers unprecedented levels of protection from known and unknown zero-day threats by combining signature and behavioral intrusion prevention system (IPS) protection with the industry's only dynamic, stateful firewall. McAfee Host Intrusion Prevention for Desktop reduces patching frequency and urgency, preserves business continuity and employee productivity, protects data confidentiality, and simplifies regulatory compliance.

Advanced threat protection through our dynamic, stateful desktop firewall

Unlike traditional system firewalls that rely on specific rules, McAfee Host Intrusion Prevention for Desktop has integrated McAfee Global Threat Intelligence™ network connection reputation to secure desktops and laptops 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. Additional firewall features, such as application and location policies, further safeguard laptops and desktops especially when they are not on the corporate network.

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 Desktop 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 Desktop protects against an average of 97 percent of exploits[1]. Protection is provided 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; NetWare networks require TCP/IP
- NIC: Network interface card; 10 mbps or higher

Supported operating systems

Microsoft Windows XP SP2, SP3 (32-bit only)

- Professional Edition

Microsoft Windows Vista, Vista SP1 (32- and 64-bit)

- Business Edition
- Enterprise Edition
- Ultimate Edition

Microsoft Windows 7 (32- and 64-bit)

- Professional Edition
- Enterprise Edition
- Ultimate Edition

Endpoints are no longer vulnerable during startup

Laptops and desktops are vulnerable during startup because the security policies have not yet been enforced. During this vulnerable startup time, endpoints could be subject to network-based attacks and security services could be disabled. McAfee Host Intrusion Prevention for Desktop 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 Desktop policy and IPS catalogs streamline that process, allowing you to create and maintain multiple firewall and IPS policies that can be applied to different groups of users and reused as needed.

Optimize and simplify management further with McAfee ePolicy Orchestrator® (McAfee ePO™) software, our single, centralized console that helps you oversee and administer all your protection. Complete 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 Desktop 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 & 4.00	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		

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