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 more 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.

The Challenge

Antivirus 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 a 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 (McAfee GTI) 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.

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.

With the increase in advanced threats, McAfee GTI offers one of the most sophisticated protection services 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.

- McAfee Host Intrusion Prevention for Desktop defends against zero-day exploits and unpatched vulnerabilities. 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.

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 intrusion prevention system (IPS) startup protection.

- Startup firewall protection allows only outbound traffic during startup until the complete firewall policy has been enforced.
- Startup IPS protection prevents our 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.

System Requirements

Supported operating systems

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1, 32 or 64-bit: Business, Enterprise, Ultimate
- Windows Embedded Standard 7 SP1, 32 or 64-bit
- Windows Vista 32 or 64-bit: Business, Enterprise, Ultimate
- Windows XP Professional 32-bit
- Windows XP Professional for Embedded Systems 32-bit
- Windows XP Embedded 32-bit

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.

Compatibility with major virtualization platforms

Virtualization offers you lower costs, flexibility, and easier product maintenance. McAfee Host Intrusion Prevention for Desktop is compatible with many major virtualization platforms including VMware, Citrix, and Microsoft.

For more information, visit **http://www.mcafee.com/us/products/host-ips-for-desktop.aspx**.

System Requirements

Supported virtualization platforms

- Citrix XenServer: 5.0, 5.5
- Citrix XenDesktop: 3.0, 4.0, 7.5, 7.6
- Citrix XenApp: 5.0, 6.0, 6.5
- Citrix Provisioning Services 6.1
- Microsoft App-V: 4.5, 4.6
- Microsoft Hyper-V Server: 2008, 2008 R2
- Microsoft Windows Server: 2008, Hyper-V 2008, 2008 R2, 2012 R2
- Microsoft VDI (Bundle)
- MED-V: 1.0, 1.0 SP1
- SCVMM: 2008, 2008 R2
- SCCM: 2007 SP2, 2007 R2
- SCOM: 2007, 2007 R2
- VMware ACE: 2.5, 2.6
- VMware ESX: 3.5, 4.0, 5.0
- VMware ESXi 5.1
- VMware Player: 2.5, 3.0, 5.0
- VMware Server: 1.0, 2.0
- VMware Thin App: 4.0, 4.5
- VMware Vsphere 4.0
- VMware View: 4 3.1, 4.0
- VMware Workstation: 6.5, 7.0, 8.0, 9.0
- XP Mode Windows 7: 32 and 64-bit

McAfee
Together is power.

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

62140ds_hips-desktop_1015
OCTOBER 2015