



Protect what you value.

McAfee Host Intrusion Prevention *for desktop*

Proactively secure endpoints, data, and applications

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 less urgently

Simplified compliance

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

The Challenge

Managing security and controlling connectivity for the desktop and laptop computers across your organization can be a huge headache. Because of the growing number of active, profit-driven cybercriminals, there were more new threats in the first half of January 2008 than all of 2007!¹ IT security teams are under intense pressure to protect all endpoints from the rapidly growing number of complex threats. And with over 32 percent of exploits released within three days of vulnerability disclosure;² organizations are at risk as it can take upwards of 30 days or more to deploy patches to endpoints. Enterprises need zero-day threat protection to grant them the security and time to properly prioritize, plan, test, and deploy patches.

A top challenge for IT managers is to successfully protect endpoints that support their business from known and unknown attacks before real damage is done. Anti-virus alone is not enough, as attacks and vulnerability exploits are being released faster and 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 managers can ensure that all endpoints and confidential data are protected, and business continuity is preserved.

McAfee Host Intrusion Prevention for desktop

As an integral part of McAfee® Total Protection (ToPS) for Endpoint, McAfee Host Intrusion Prevention (Host IPS) for desktop protects endpoints from known and unknown, zero-day threats by combining signature and behavioral intrusion prevention system (IPS) protection with a stateful desktop firewall and application control. McAfee Host IPS reduces patch frequency and urgency, preserves business continuity and employee productivity, protects data confidentiality, and simplifies regulatory compliance.

Enterprise Manageability

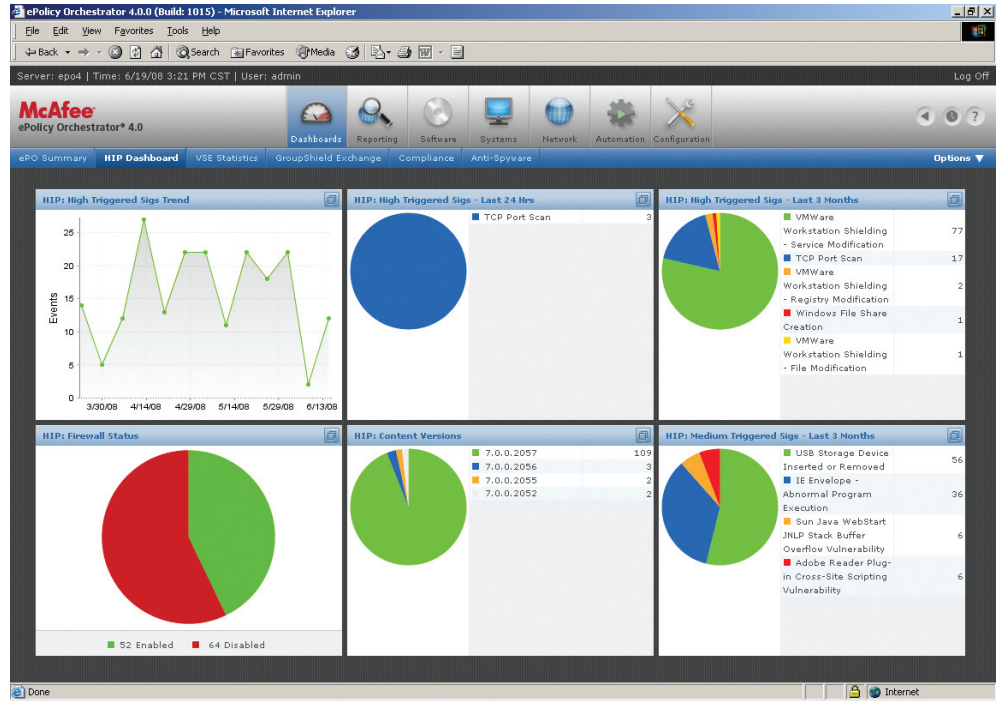
McAfee ePolicy Orchestrator® (ePO™) is the industry-leading security management platform that delivers a coordinated, proactive defense against malicious threats and attacks for the enterprise. With ePO at the hub of McAfee security risk management (SRM) solutions, administrators can mitigate the risk of rogue, noncompliant systems; keep protection up to date; configure and enforce protection policies; and monitor security status 24/7 from one centralized, web-based console. Deploy ePO and manage all of your new security solutions or extend your investment in enterprise security management by adding Host IPS to your existing ePO infrastructure. Using a single agent, endpoint security is easy to deploy, configure, and manage. Consolidation of security management not only means fewer headaches, but also substantial IT cost savings.

¹ McAfee Avert® Labs
² McAfee Avert Labs

SYSTEM REQUIREMENTS

Microsoft Windows (English, French, German, Spanish, Japanese, Korean, Traditional Chinese)

- Windows XP Home with Service Pack 2 or 3
- Windows XP Professional with Service Pack 2 or 3
- Windows XP Tablet PC
- Windows Vista, 32-bit and 64-bit



ePO dashboards make viewing Host IPS data easy.

Features and Benefits

Multi-layered protection provides broad, comprehensive coverage

With the rapid growth of profit-motivated cybercrime rings, organizations need layered protection to defend endpoints against known and unknown zero-day threats and to prevent loss of confidential data.

- **Signature protection** accurately identifies and blocks known attacks
- **Behavioral protection** secures endpoints against new, zero-day threats, such as buffer overflow attacks
- **Stateful firewall** blocks unsolicited inbound traffic, controls outbound traffic, and applies policy rules based on traffic, ports, applications, and locations
- **Application control** helps you create whitelists and blacklists to specify which applications can or cannot run

Secure mobile laptops and keep noncompliant systems from infecting your network

More and more employees—and their PCs—are on the go, making organizations more susceptible to the introduction of new threats. Host IPS safeguards laptops when they are not connected to the corporate network and prevents noncompliant systems from infecting the network.

- Protect laptops even when they are off the corporate network to ensure that attempted exploits do not threaten the corporate network
- **Connection-aware protection** applies different levels of protection rules based on the endpoint's connection—on the corporate network, over a VPN, or from a public network
- **Quarantine mode** blocks remote users that fail security checks from accessing network resources

Your IT team patches less frequently, less urgently, and on its own schedule

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

- **Vulnerability shielding** automatically updates signatures to protect endpoints against attacks resulting from exploited vulnerabilities
- **Out-of-the-box protection** boasts a superior track record: Host IPS protected 97 percent of all Microsoft vulnerabilities disclosed in 2007³
- **Signature updates** are automatically and regularly downloaded in a similar manner to .DAT file updates for protection assurance

ePO consolidates and centralizes management for all McAfee products

Companies struggle with the costs and effort required to manage separate security technologies deployed on their endpoints and network. By using a single, integrated security console, companies reduce the number of IT managers needed to manage endpoint security with multiple consoles by 44 percent.⁴

- Access centralized event monitoring, reports, dashboard, and workflow through a single web-based, management console
- Deploy, manage, and update agents and policies from one management platform

Spend less time collecting data needed to achieve, report, and prove compliance

Maintaining and proving compliance can consume a huge amount of IT resources. Host IPS helps organizations obtain greater visibility and control to simplify their compliance efforts and make reporting and audits less painstaking.

- Gather attack details such as type, vector, source, severity, timestamp, and more—all in clear and easy-to-understand language—for prompt reporting, audit, investigation, and response
- Produce compliance reports for auditors and other stakeholders
- Customize dashboards for real-time compliance status

McAfee Host IPS is an integral part of McAfee ToPS for Endpoint, McAfee's comprehensive endpoint security solution. ToPS for Endpoint is fully integrated with McAfee ePO, the unified SRM platform that saves enterprises money and time with unprecedented operational efficiencies. To learn more about ToPS for Endpoint, please visit: http://www.mcafee.com/us/enterprise/products/security_suite_solutions/total_protection_solutions.

³ McAfee Avert Labs

⁴ Insight Express, 2007