

Full Spectrum Network Defense—McAfee Network Security Platform (I-Series)

Advanced intrusion prevention technology protects against malware and unauthorized access while enforcing policy

Product Overview

McAfee® Network Security Platform is an advanced, comprehensive network intrusion prevention system (IPS). Its action-oriented security allows you to automatically manage risk and meet compliance while reducing IT resource dependency. This network-class platform is designed for any enterprise that needs absolute security confidence, 100 megabits (Mb) to beyond 10 gigabits (Gb) performance, and collaborative security for integrated and intelligent enterprise-wide protection that prevents attacks and secures your infrastructure.

McAfee Network Security Platform accurately detects and protects against all kinds of intrusions. It correlates signatures and other anomalies and protects your enterprise from known, zero-day, denial of service (DoS), distributed denial of service (DDoS), and encrypted attacks. It also protects against threats like spyware, voice over IP (VoIP) vulnerabilities, botnets, malware, worms, Trojans, phishing, and peer-to-peer tunnelling.

McAfee Network Security Platform delivers knowledge-driven security that is integrated, automated, and actionable. McAfee Network Security Platform's Network Security Manager dashboard provides full visibility of events. Integration with the McAfee® ePolicy Orchestrator® (McAfee ePO™) software and McAfee Vulnerability Manager software helps you manage and enforce compliance with minimal effort.

Key Benefits

Comprehensive enterprise-wide threat prevention

- Blocks attacks and prevents intrusion
- Reduces blind spots and provides enterprise-wide visibility

- Protects every device connected to the network
- Safeguards extensive networks accurately and efficiently
- Defends against most vulnerabilities—including zero-day, malware, DoS and DDOS attacks, phishing, and peer-to-peer tunneling

Operational efficiency and real-time business protection

- Prevents attacks while reducing costs and downtime
- Protects your data and infrastructure
- Meets compliance initiatives
- Saves time and IT resources with collaboration among McAfee network, system, risk, and management products

Enhanced competitive advantage

- Prevents network threats and exploits from interrupting business operations
- Delivers enterprise-level performance and ensures reliability
- Promotes availability of network bandwidth
- Simplifies operations concerning threat and signature management
- Accelerates network performance, scalability, and flexibility

Enables fast, accurate decisions

- Improves time to protection and time to confidence with real-time security that's not just automated but actionable

Features That Set McAfee Network Security Platform Apart

Network-class platform with multigigabit performance

- Offers carrier-class reliability with the highest port density

- Delivers multigigabit performance reliability for all company locations, from branch offices to the network core, with purpose-built platforms
- Offers an easy-to-set-up and easy-to-use network security platform
- Provides easy setup and management of policy templates and updates through a centralized, browser-based console
- Addresses today's evolving security and network needs
- Provides affordable and reliable network-class performance
- Protects all enterprise locations—from the network core to branch offices, with purpose-built platforms

Industry-proven network security with NSS Group Certification

- The only network intrusion prevention system to hold the NSS Group's Multigigabit IPS Certification¹
- Acts both as an intrusion detection system (IDS) and an IPS
- Safeguards all network-connected devices with a combination of IPS and internal firewall, providing overlapping and integrated protection
- Defends against current and future threats with dynamic threat and vulnerability updates
- Includes behavior and anomaly, signature, and DoS/DDoS detection; also protects against encrypted attacks
- Offers the best zero-day vulnerability coverage; includes vulnerabilities in applications from Adobe, Oracle, Cisco, and Microsoft

Greater visibility and policy enforcement through integration

- Integrates with McAfee Vulnerability Manager software, McAfee ePO software, and other devices, saving time and IT resources
- Provides on-demand visibility on critical host details, threats, and risk relevance to ensure actionable security
- Limits bandwidth to low-priority traffic and provides high-priority traffic with the required throughput
- Safeguards unpatched systems up to patch process initiation

Dynamic network access control integration

- Provides pre- and post-admission control and identity-based access control when integrated with the optional McAfee Network Access Control add-on
- Extends the reach and depth of network enforcement with the ability to control access to managed, unmanaged, and unmanageable hosts
- Offers host quarantine and enforces access policies; blocks a badly behaving host and quarantines it until remediation

Policy enforcement and regulatory compliance

- Offers real-time vulnerability awareness and compliance reporting and behavior-driven host quarantine

Why McAfee

Managing security and controlling connectivity for the desktop and laptop computers across the organization is nothing short of an IT nightmare. Employees inadvertently introduce worms, spyware, and other threats into the network through their desktops and laptops. These systems also are commonly targeted by hackers for use in attacking other internal servers, databases, and information. The corporate servers house an organization's most valuable information assets and keep the business alive. One of the top challenges for an organization is to successfully protect these desktops, laptops, servers, and applications from known and unknown attacks that threaten to disrupt the business. To accomplish this, you must aggressively deploy security technologies throughout your network

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, you ensure that confidential data is protected and business continuity is preserved.

McAfee Network Security Platform is a combination of network appliances and software that implements network access control (NAC) as well as accurately detects and prevents intrusions, denial of service (DoS) and distributed denial of service (DDoS) attacks, and network misuse. McAfee Network Security Platform combines real-time intrusion detection and prevention for the most comprehensive and effective network security system.

McAfee Network Security Platform protects your assets with proven methods that include signature and behavioral intrusion prevention, application-blocking control, and a stateful system firewall. Automatic signature updates and zero-day protection give you the advanced vulnerability-shielding capabilities you require. It also reduces the requirement for frequent patching, and improves compliance with regulations.

System Requirements

McAfee Network Security Manager consists of hardware and software resources that are used to configure and manage your Network Security Platform deployment.

The following are the system requirements for a McAfee Network Security Manager server running with a MySQL database:

	Minimum	Recommended
OS	Microsoft Windows Server 2003 Standard Edition, SP2 English OS (32-bit or 64-bit) Note: For 64-bit, only X64 architecture is supported. Windows Server 2003 R2 (Standard Edition), Japanese OS (32-bit)	Same
Memory	2 GB or higher	Same
CPU	2 GHz Pentium 4 processor	Dual 2 GHz processors
Disk Space	40 GB	80 GB disk with 8 MB memory cache
Network	100 Mbps card	Same
Monitor	32-bit color, 1024 x 768 display setting	Same

The following are the system requirements for hosting the McAfee Network Security Manager server on a VMware platform. Note that the supported VMware version is ESX 3.02:

	Minimum	Recommended
OS	Microsoft Windows Server 2003 (Standard Edition) SP2 (32-bit or 64-bit), English OS	Same as the minimum requirement
Memory	2 GB	2 GB or higher
Virtual CPUs	2	2 or more
Disk Space	40 GB	80 GB

The following are the system requirements for client systems connecting to the McAfee Network Security Manager application:

	Minimum
OS	Microsoft Windows XP (Standard Edition) SP2
Memory	512 MB
Browser	Internet Explorer 6.0 or 7.0
Monitor	32-bit color, 1024 x 768 display

About McAfee

McAfee, Inc., headquartered in Santa Clara, California, is the world’s largest dedicated security technology company. McAfee is relentlessly committed to tackling the world’s toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. <http://www.mcafee.com>.

