

McAfee Network Security Platform

The industry's most advanced and proven intrusion prevention solution

Faster time to protection. Faster time to resolution. Faster time to confidence.

McAfee® Network Security Platform delivers knowledge-driven security that's integrated, automated, and actionable. Only Network Security Platform combines network and system security infrastructure, providing class-leading threat protection from 100 megabits (Mb) to beyond 10 gigabits (Gb). Install the appliance and start blocking threats immediately. Get full visibility of events through the Network Security Manager dashboard, and integration with McAfee ePolicy Orchestrator® (ePO™) and McAfee Vulnerability Manager lets you manage risk and enforce compliance with less effort.

Key Advantages

Enterprise-wide coverage

- A single industry-proven device provides comprehensive, proactive network and system security

More visibility and enforcement through integration

- Integrates with McAfee Vulnerability Manager and ePO to give you on-demand visibility to critical host details, threats, and risk relevance

Fast, accurate decisions

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

Reliable, network-class platforms; next-generation network protection

- Performance from 100 Mbps to beyond 10 Gbps
- Highest port density

Operational efficiency

- Collaboration between McAfee network, system, risk, and management products saves time and IT resources

Ease of deployment

- Using the Network Security Manager appliance and built-in installation wizards, installing the Network Security Platform takes a few minutes. The ports on the appliance are configured as in line by default with a well-tuned default policy applied that is ready to block critical threats.

Comprehensive support for packet encapsulation decoding

- IPv6
- V4-in-V4, V4-in-V6, V6-in-V4, and V6-in-V6 tunnels
- MPLS
- GRE
- Q-in-Q Double VLAN

High availability

- Layer two fail-open
- Hardware fail-open
- Failover

Reliable protection for every networked device

How intelligent is your network security?

Traditional intrusion prevention systems (IPS) are point products fraught with false positives and overwhelming alert logs. Their lack of coordination means valuable hours are lost to redundant management processes. Many PC-based solutions don't scale under attack, and few offer the control to mitigate patch pressures.

That's why more than 4,500 of the most demanding enterprises and service providers have selected McAfee Network Security Platform to protect their networks and network-connected devices.

Integrated network and system security

McAfee Network Security Platform is the perfect fit for enterprises that need real-time security confidence with multi-gigabit performance and integrated, enterprise-wide network and system security. Network Security Platform's knowledge-driven security empowers you to automatically manage risk and meet compliance—while enhancing operational efficiency and reducing IT effort.

Network Security Platform collaborates with McAfee Vulnerability Manager (*formerly McAfee Foundstone®*), McAfee ePolicy Orchestrator, and

McAfee Host Intrusion Prevention. It is also a key component of the McAfee network access control (NAC) solution, McAfee Unified Secure Access. Network Security Platform gives you more of the things that matter to your business—protection, visibility, efficiency, enforcement, and value.

Absolute security confidence

Network Security Platform protects all network-connected devices with a combination of IPS and internal firewall that overlaps and integrates protection and extends firewall defenses to the internal network. It correlates signatures, anomalies, denial of service (DoS), and distributed denial of service (DDoS) information to accurately block attacks before they reach their intended targets. Dynamic threat and vulnerability updates ensure continuous protection.

Network-class platform with multi-gigabit performance

Network Security Platform's quality and performance exceed carrier-class standards and make it the only IPS to hold the NSS Group's 10-Gbps IPS certification. And you get carrier class reliability with the M-Series, offering beyond 10-Gbps performance with the highest port density on the market.



McAfee Network Security Platform

Real-time business protection

- Prevent attacks while reducing costs and downtime
- Protect your data and infrastructure
- Meet compliance initiatives

Protect your systems

- Proactive protection for unpatched systems
- Proactive protection for zero-day attacks
- System-aware intrusion prevention system (IPS) with McAfee ePO integration
- Host IPS/virus/spyware event visibility

Protect your network

- Next-generation 10-gigabit Ethernet
- IPv6 protection
- Adaptive rate limiting
- Comprehensive infrastructure protection

Regulatory and policy compliance

- Real-time vulnerability awareness and compliance reporting
- Risk-aware IPS with McAfee Vulnerability Manager integration
- Behavior-driven host quarantine
- Enforce internal and regulatory policy

Mitigate patch anxieties and enforce your policies

You are in control. With Network Security Platform, you insulate systems from risk while you validate and deploy patches. You can control traffic and apply unique policies and protections to a network segment, a collection of hosts, or even a single system. It's flexible, too, so that you can deploy patches when you are ready and set up policy enforcement to meet your organization's needs.

Add the optional NAC add-on software, and turn your IPS into a NAC device that offers both pre- and post-admission control and identity based-access control, along with host quarantine and enforceable access policies.

Industry-proven network security device

Surround your enterprise with proven McAfee security, backed by 24/7 research at McAfee Avert® Labs. Scale up your protection to carrier-class performance with one integrated network security solution.

Accurate, enterprise-wide threat prevention

- Protect your enterprise from known, zero-day, denial of service (DoS), distributed denial of service (DDoS), SYN flood (which sends TCP connections requests faster than a machine can process them), and encrypted attacks, and threats like spyware, Voice over IP (VoIP) vulnerabilities, botnets, malware, worms, Trojans, phishing, and peer-to-peer tunneling
- Improve accuracy through use of multiple advanced detection methods, including signature, application, and protocol anomaly; shell-code detection algorithms; and next-generation DoS and DDoS prevention
- Parse more than 100 protocols and review more than 3,000 high-quality, multi-token, multi-trigger signatures with stateful traffic inspection
- Get proactive blocking for hundreds of attacks straight out of the box with pre-configured policies
- Receive continuous threat updates 24/7 from the global research team at McAfee Avert Labs

McAfee ePolicy Orchestrator (ePO) integration

- Get real-time visibility of actionable system host details, including host name, user name, OS, patch level, media access control (MAC) address, last scan date, protection details, and the top host IPS, anti-virus, and anti-spyware events
- Synthesize and filter data from multiple tools to create custom reports

Real-time risk-aware network security platform

- Integration with McAfee Vulnerability Manager provides auto-import of multiple vulnerability data points and regular or on-demand scans to accurately determine threat relevance

Adaptive rate limiting

- Network Security Platform uses real-time, protocol-based rate limiting to apply application, protocol type, and port-based bandwidth controls and improve quality of service
- Prioritize business-critical traffic and block unwanted and risky applications

Certification by NSS Group

- Network Security Platform is the only network IPS solution that has received the NSS Group's IPS certification for more 10-Gbps

Proven manageability and availability

Simple, centralized, web-based management of Network Security Platform appliances and policies includes:

- Fourteen ready-to-use, predefined IPS security policy rule templates
- Integrated user authentication support to external databases, including Radius, LDAP, and TACACS
- McAfee Network Security Manager offers always-on management, automated failover and fail-back, and disaster recovery of critical configuration data
- Network Security Manager software is provided at no cost for managing up to two Network Security Platform appliances
- Network Security Central Manager provides hierarchical management for centralized control of policy viewing, modification, and distribution to support large or geographically dispersed sensor deployments
- High-availability configuration allows transparent Layer 7 stateful failover, avoiding a single point of failure

Network Security Platform Specifications

10 Gigabit Ethernet Connectivity



Sensor Hardware Components	M-8000	M-6050	M-4050	M-3050	M-2750	M-1450	M-1250
Network location	Core	Core	Core	Core	Perimeter	Branch office / perimeter	Branch office
Performance throughput	Up to 10 Gbps	Up to 5 Gbps	Up to 3 Gbps	Up to 1.5 Gbps	Up to 600 Mbps	Up to 200 Mbps	Up to 100 Mbps
Maximum concurrent connections	4,000,000	2,000,000	1,500,000	750,000	250,000	80,000	40,000
Ports							
Gigabit Ethernet detection ports	16	8	8	8	20	8 (Copper Only)	8 (Copper Only)
10 Gigabit Ethernet	12	8	4	4	—	—	—
Dedicated response ports (GigE)	1	1	1	1	1	1	1
Dedicated management ports (GigE)	1	1	1	1	1	1	1
External fail-open control ports	14	8	6	6	10	—	—
Console and aux ports	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fail-open	Optional	Optional	Optional	Optional	Optional	Yes	Yes
Fail-close	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mode of operation							
Span port monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tap mode	Optional	Optional	Optional	Optional	Optional	Optional	Optional
In-line mode	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Port clustering	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10-Gbps-plus solution	Yes	Yes	—	—	—	—	—
Number of virtual IPS systems	1,000	1,000	1,000	1,000	100	32	16
Traffic monitoring on active-active links	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Traffic monitoring on active-passive links	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Monitoring of asymmetric traffic routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
High availability							
Redundant power	Yes (optional)	Yes (optional)	Yes (optional)	Yes (optional)	Yes (optional)	No	No
Device failure detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Link failure detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Physical							
Dimensions	2x 2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D) each	2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D)	2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D)	2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D)	2RU Rack mountable 15.88(W) x 3.3(H) x 24.5(D)	1RU Rack mountable 17.37 (W) x 1.65(H) x 13.5 (D)	1RU Rack mountable 17.37 (W) x 1.65(H) x 13.5(D)
Weight	94 lbs. (2x47)	47 lbs.	47 lbs.	47 lbs.	40 lbs.	12 lbs.	12 lbs.
Power consumption	900w (2x450w)	450w	450w	450w	450w	120w	120w
DC power available	Optional	Optional	Optional	Optional	Optional	No	No
Power	100–240VAC (50/60Hz)						
Temperature	0° to 35° C (operating) –40° to 70° C (non-operating)				0° to 40° C (operating) –40° to 70° C (non-operating)		
Relative humidity (non-condensing)	Operational: 10 percent to 90 percent Non-operational: 5 percent to 95 percent						
Altitude	0 to 10,000 feet						
Safety certification	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, IEC 60825, 21CFR1040 CB license and report covering all national country deviations.						
EMI certification	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)						

Sensor Software Components

		M-8000	M-6050	M-4050	M-3050	M-2750	M-1450	M-1250
Stateful traffic inspection	IP defragmentation and TCP stream reassembly	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Detailed protocol analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Asymmetric traffic monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Protocol normalization	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Advanced evasion protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Forensic data collection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Protocol tunneling	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Protocol discovery	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Stacked VLAN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Signature detection	User-defined signatures	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Real-time signature updates	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Anomaly detection	Statistical anomaly	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Protocol anomaly	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Application anomaly	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DoS detection	Threshold-based detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Self-learning profile-based detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Maximum DoS profiles	5,000	5,000	5,000	5,000	300	120	100
Intrusion prevention	Stop attacks in progress in real time	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Drop attack packets/sessions	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Host quarantine	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Initiate TCP reset, ICMP unreachable	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Packet logging	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Automated and user-initiated prevention	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Internal firewall	Blocks unwanted and nuisance traffic	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Granular security policy enforcement	Yes	Yes	Yes	Yes	Yes	Yes	Yes
High availability	Stateful failover	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management	Command line interface (console)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Manager communication	Secure channel	Secure channel	Secure channel	Secure channel	Same for all models	Same for all models	Same for all models

