McAfee Network Security Platform

A comprehensive, intelligent approach to network security

McAfee® Network Security Platform (McAfee NSP) is a next-generation intrusion prevention system (IPS) that discovers and blocks sophisticated malware threats across the network. It utilizes advanced detection and emulation techniques, moving beyond mere pattern matching to defend against stealthy attacks with a high degree of accuracy. To meet the needs of demanding networks, the platform can scale to more than 40 Gbps with a single device. The integrated McAfee solution portfolio streamlines security operations by combining real-time McAfee Global Threat Intelligence feeds with rich contextual data about users, devices, and applications for fast, accurate response to network-borne attacks.

Protection Against Today's Stealthy Threats

Your network faces advanced stealthy attacks that can evade traditional detection methods, leaving applications and data exposed to crippling breaches and downtime. Unfortunately, most organizations lack the financial and operational resources to implement and manage the combination of tools and technologies required to provide an adequate defense.

McAfee NSP combines intelligent threat prevention with intuitive security management to improve detection accuracy and streamline security operations. No single malware detection technology can prevent all attacks—which is why McAfee NSP layers multiple signature and signature-less detection engines to help prevent unwanted malware from wreaking havoc on your network. It performs deep inspection of network traffic by using a combination of advanced technologies, including full protocol analysis, threat reputation, and behavior analysis to detect and protect against malware callbacks, denial-of-service (DoS), zero-day attacks, and other advanced threats.

Integrated Security

McAfee Network Security Platform integrates with McAfee Advanced Threat Defense, which combines in-depth static code analysis, dynamic analysis (malware sandboxing), and machine learning to detect zero-day threats, including threats that use evasion techniques and ransomware. McAfee NSP also combines file reputation from McAfee Global Threat Intelligence and offers integration with McAfee® ePolicy Orchestrator® software and McAfee

Key Advantages

- Quickly detects and blocks threats to protect applications and data
- High-performance, scalable solution for dynamic environments
- Centralized management for visibility and control
- Advanced detection, including signature-less malware analysis
- Inbound and outbound SSL decryption to inspect network traffic
- High-availability and disaster recovery protection
- Virtual appliance models also available
- Integrates with McAfee solution portfolio for device-to-cloud security

Connect With Us

Enterprise Security Manager for real-time correlation of network events across all relevant sources. The combined solution incorporates device details, user information, endpoint security posture, vulnerability assessments, and other rich information to help organizations better understand threat severity and business risk factors.

Performance and Availability

McAfee Network Security Platform offers the best of both worlds—security and high performance. It combines a single-pass, protocol-based inspection architecture with purpose-built, carrier-class hardware to achieve real-world inspection of more than 40 Gbps with a single device. Its efficient architecture preserves performance regardless of security settings, while other IPS solutions can experience up to a 50% reduction in throughput with security-over-performance policies.

McAfee NSP also provides active-active and active-passive with stateful failover, enabling you to meet high availability SLAs, while avoiding the bottlenecks of slower performing appliances or over-burdened stand-alone solutions.

Visibility and Control

Make informed decisions about the applications and protocols on your network. McAfee Network Security Platform is the first and only IPS solution to combine advanced threat prevention and application awareness into a single security decision engine. We correlate threat activity with application usage, including Layer 7 visibility of more than 1,500 applications and protocols, enabling you to make more informed decisions about which applications you allow on your network.

In addition to application identification, McAfee NSP provides user and device visibility. It prioritizes risky hosts and users, including active botnets, through the identification of anomalous network behavior.

Intelligent, Scalable Security Management

Make the most of your security investment through intelligent network security management. McAfee Network Security Manager provides scalable web-based management from two to several hundred network security appliances. It offers intuitive, progressive disclosure workflows that guide administrators to relevant alerts, along with easy-to-use security dashboards that automatically prioritize events based on alert severity and relevancy.

Additional Features

Advanced threat prevention

- Inbound Secure Sockets Layer (SSL) decryption supports Diffie-Hellman (DH) and Elliptic-Curve Diffie–Hellman (ECDH) ciphers using an agent-based, shared key solution with no impact on sensor performance (patent pending, for NS-series)
- Outbound SSL decryption (NS-series)
- McAfee Gateway Anti-Malware Emulation engine
- PDF JavaScript emulation engine
- Adobe Flash behavioral analysis engine
- Advanced evasion protection
- Mobile threat reputation and cloud analysis

Botnet and malware callback protection

- DNS/DGA fast flux callback detection
- DNS sinkholing
- Heuristic bot detection
- Multiple attack correlation
- Command and control database

Advanced intrusion prevention

- IP defragmentation and TCP stream reassembly
- McAfee, user-defined, and open-source signatures
- Native support for Snort signatures (NS-series)
- Whitelist/blacklist enhancements in support of Structured Threat Information eXpression (STIX) (NS-series)
- Host quarantine and rate limiting
- Inspection of virtual environments
- Integration with McAfee Advanced Threat Defense
- HTTP response decompression support

DoS and DDoS prevention

- Threshold and heuristic-based detection
- Host-based connection limiting
- Self-learning, profile-based detection

McAfee Global Threat Intelligence

- File and IP reputation
- Application and protocol reputation
- Geo-location
- Whitelisting based on McAfee Global Threat Intelligence categories

High availability

- Active-active and active-passive with stateful failover
- External fail-open (active)
- Built-in fail-open

Protocol tunneling support

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

McAfee Network Security Manager

- Tiered management (up to 1,000 sensors)
- User authentication (RADIUS and LDAP)
- Automated failover and fail-back
- Disaster recovery of critical configuration data
- Centralized, hierarchical policy management
- Ability to integrate with McAfee Cloud Threat Detection to submit unknown files
- Memory dashboard details memory utilization by device

Learn More

For more details and physical appliance options, please see the **McAfee Network Security Platform Specifications Sheet**.

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com