

The McAfee Network Security Platform: Bridging Network and System Security

Enterprise-wide network security platform

McAfee Network Security Platform delivers unprecedented knowledge-driven security. Together with McAfee's security risk management (SRM) framework, Network Security Platform collaborates with McAfee Foundstone®, McAfee ePolicy Orchestrator® (ePO™), and McAfee Network Access Control (NAC) to provide intelligent and real-time security that's exponentially more accurate and efficient than traditional point products.

Key Advantages

McAfee SRM

- Integration with McAfee Foundstone and McAfee ePO goes beyond intrusion detection and intrusion prevention to provide critical host details, on-demand threat and risk relevance, and host quarantine.

McAfee collaborative security infrastructure

- McAfee's collaborative SRM framework bridges network and system security to help you leverage the benefits of your existing security ecosystem to do more with less.

McAfee opens a world of integration benefits and value to leverage your security investment. The integration of network (Network Security Platform) and system (ePO) security infrastructure results in the only System-Aware IPS, delivering efficient security collaboration for visibility of system and network threats. Breakthrough ePolicy Orchestrator® Integration provides real-time visibility of actionable system host details, as well as the top Host IPS and AV/Spyware events.

Integration with McAfee Foundstone provides real-time threat relevancy, on-demand. Highly accurate risk relevancy and visibility provides actionable security intelligence to empower real-time security decisions.

Integration with McAfee NAC extends the reach and depth of network enforcement by delivering dynamic, zero-day access control. Combined with Network Security Platform (NSP) on-board host quarantine capability, Dynamic NAC provides continuous pre and post admission control for managed, un-managed and un-manageable hosts.

Knowledge-Driven Network Security

Smart network and system security integration delivers real-time security that's not just automated, but actionable. With the click of a mouse, you've got intelligent IPS that provides critical host details, top host intrusion and spyware attacks, and accurate threat and risk relevance, on demand. A real-time security solution empowers real-time security decisions, giving you a faster time to protection and confidence.



Integration with ePO

Faster time-to-protection/time-to-resolution with real-time visibility of system host details, top Host IPS attacks and AV/spyware events

Integration with Foundstone

Real-time Risk-Aware IPS with on-demand threat relevancy and Foundstone "scan now" functionality

Integration with McAfee NAC

Behavior-driven host quarantine and Dynamic NAC for real-time post admission control of managed and un-managed hosts

Real-time intelligence. Real-time security action

Real-time relevancy, visibility and control capabilities empower efficient, real-time security decisions to give you faster time-to-protection and time-to-compliance.

Security knowledge that's actionable

Integrated network and system security leverages all points of visibility—including McAfee Foundstone, ePO and NAC—to provide knowledge-driven security that's exponentially more actionable and accurate than IPS point products.

Faster time-to-confidence

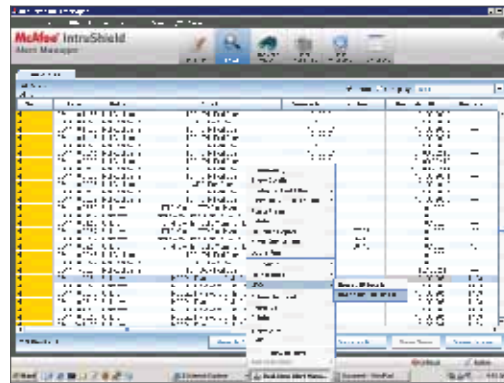
McAfee has integrated multiple products and technologies to allow you to distinguish between noise and relevant information in real-time. That's security confidence only McAfee Network Security Platform can provide.

Integration with ePO: Real-Time System-Aware IPS

By doing a simple right click within the Network Security Platform manager, you can get specific visibility to details of a source host or a destination host. You get visibility to things like the host name, user name, current protection on that host, and the top 10 Host Intrusions events that have occurred on that host.

This gives the Network Administrator direct, actionable information that was never available to a network admin before McAfee's integration of Network Security Platform and ePO.

SRM Framework Integration—McAfee ePO Real-time system-aware IPS for enterprise-wide visibility



System-Aware IPS with ePO Host Data

- Simple right-click provides real-time details of Source or Destination IPs
- Provides host name, user name, OS, patch level, MAC address, last scan date and other protection policies Top 10 Host Intrusion events

System-Aware IPS Benefits

- Faster time-to-confidence
- Visibility, efficiency, relevancy
- Leverages ePO investment

How Does it Work?

Integrating Network Security Platform and ePO enables you to query the ePO database for the details of your network hosts right from the Alert Manager. The details that are fetched from the ePO database include the host type, host name, user name, operating system details, and the details of system security products installed on the host. If you have installed McAfee Host Intrusion

Prevention as part of your ePO installation, then you can also view the last 10 HIPS events for a specific host. These details provide increased visibility and relevance for security administrators performing forensic investigation of security events seen on the network.

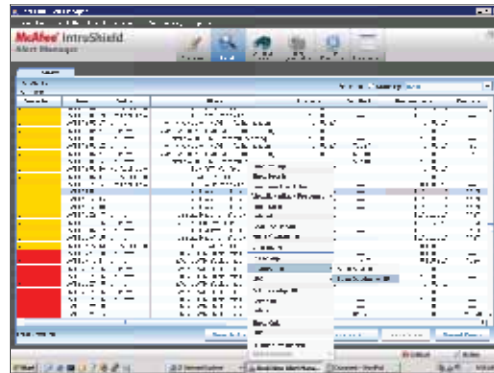
Consider the following scenario to understand how Network Security Platform-ePO integration works: You notice in the Alert Manager that a host in your network is port scanning the other hosts. You want to know more details about the source of these attacks. So, you right-click on an alert and see the details of the source IP. NSP queries the ePO database and displays the details of the host in the Alert Manager. From these details, you realize that VirusScan (McAfee's antivirus application) is outdated. Looking at the host name, you also realize that it is the server that was taken off the network sometime back. Therefore, the VirusScan was not updated during this period.

Integration with Foundstone: Real-Time Risk-Aware IPS

Vulnerability assessment is the automated process of pro-actively identifying vulnerabilities of computing systems in a network, to determine security threats in the network. Network Security Platform provides integration Foundstone Enterprise. You can request remote scans, and use the vulnerability assessment reports from the scanners to determine the relevance of attacks on the hosts.

Network Security Platform has been integrated with Foundstone Enterprise vulnerability scanner. There are two main components to this enhanced integration. First, users can schedule the import of Foundstone scan data into Network Security Platform, to provide automated updating of IPS-event data relevancy. Second, users can initiate a Foundstone on-demand scan of a single or group of IP addresses directly from the NSP Alert Manager console. This provides a simple way for security administrators to access near real-time updates of host vulnerability details, and improved focus on critical events.

**SRM Framework Integration—
McAfee Foundstone
Real-time risk-aware IPS**



**Real-Time Risk-Aware
IPS Features**

- Auto import of Foundstone scan reports
- “Scan no” provides on-demand Foundstone relevancy on a per-host(s) basis

**Real-Time Risk-Aware
IPS Benefits**

- Improved focus on critical events
- Automated, accurate relevance
- Real-time update of vulnerability details for specific host(s)

How Does it Work?

On-demand scan. You can request a Foundstone scan from NSP Alert Manager, The FoundScan engine scans the host, and provides the vulnerability assessment data to Network Security Platform. This data is processed and stored in the NSP database. The vulnerability data is also updated in the cache maintained in Alert Manager client, so that all open alert managers have visibility to the recently invoked on-demand scans.

Automatic or manual import of Foundstone reports. The vulnerability report from Foundstone database can be imported via the Foundstone Scheduler in Network Security Platform. Reports can be scheduled on a daily or weekly basis. Imported vulnerability data will be stored in the NSP database, and also updated in the cache used for relevance analysis of attacks.

You can manually import reports from Foundstone, and store them in your local machine. NSP client passes the imported vulnerability data into the vulnerability assessment module in the NSP server. This data is processed and stored in the NSP database in Network Security Platform format.

Relevance analysis of attacks. Once you have imported vulnerability reports into the Network Security Platform (NSP) database, you can determine the vulnerability relevance for real-time alerts.

Integration with NAC: Post Admission Control

McAfee NAC detects and assesses systems attempting to enter your network and can enforce policy compliance on the systems before allowing them on to the network. However, network security is not complete with only pre-admission control. For comprehensive and continuous network security, you need effective post-admission control as well, such as the one provided by Network Security Platform. Network Security Platform can alert you in real-time about post-admission threats and exploit attempts such as a system generating malicious traffic. You can then use McAfee NAC and Network Security Platform (NSP) collaboratively to handle the offending system. For example, using NSP you can quarantine the system and re-direct all HTTP traffic from the system to the remediation portal until remediation is complete.

How Does it Work?

Step 1: Define system compliance policies and Network IPS policies.

Step 2: Network Security Platform sensor detects anomalous traffic or malicious activity from a badly behaving host.

Step 3 and 4: Network Security Platform blocks the attack and either informs the MNCAC for managed host or quarantine the source of attack if unmanaged host through “quarantine” feature.

Step 5: Again for managed host, it goes through auto remediation, and unmanaged host is redirected to a remediation portal.

Real-Time Security Confidence

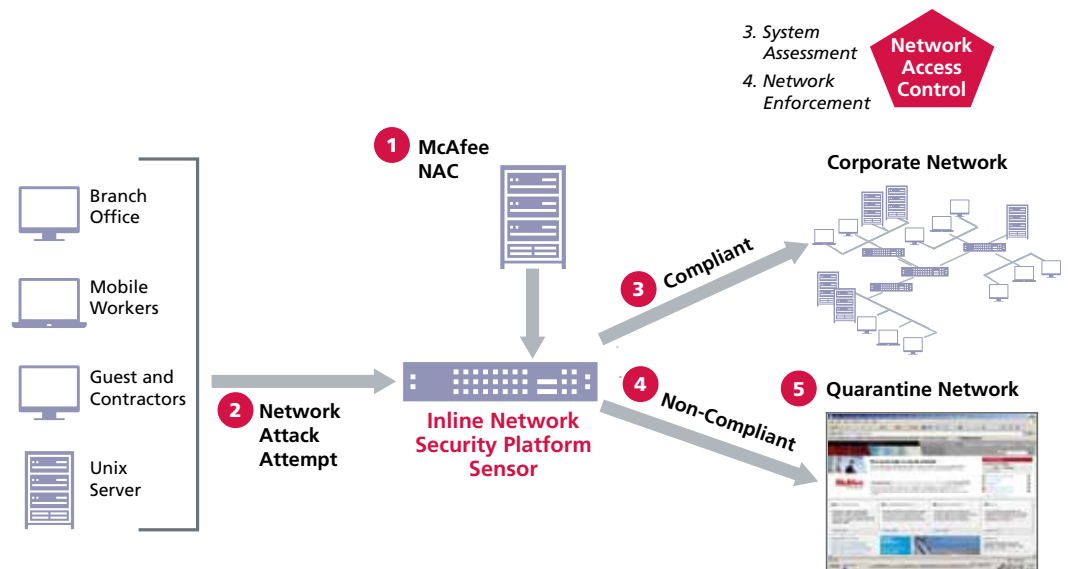
Smart network and system security integration delivers real-time security that’s not just automated, but actionable. With the click of a mouse, you’ve got intelligent IPS that provides critical host details, top host intrusion and spyware attacks, and accurate threat and risk relevance, on demand. A real-time security solution empowers real-time security decisions, giving you:

- Faster time-to-protection with system-aware IPS through ePO integration
- Faster time-to-confidence with real-time Risk-Aware IPS through Foundstone vulnerability scanning integration
- Comprehensive and continuous network security with pre and post admission control through NAC Integration

Traditional intrusion prevention systems (IPS) are point solutions 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.

Only Network Security Platform combines network and system security infrastructure for proactive enterprise-wide protection. It's exponentially more accurate and efficient than traditional point products. You can manage risk and meet compliance—with less effort. Network Security Platform's intelligent security and reliable network-class platforms give you absolute confidence in your security.



1	2	3	4	5
Define Define system compliance policies and Network IPS policies	Detect Network Security Platform sensor detects network traffic from "badly behaving host"	Assess Network Security Platform blocks the attacks and evaluates whether the device is managed or unmanaged using MNAC database	Enforce Network Security Platform quarantines unmanaged infected host using IPS policies	Remediate Quarantined system is redirected to a remediation portal for unmanaged

McAfee NAC and Network Security Platform integration—Post admission control

