NetIQ Security Manager™

Delivers comprehensive, centralized security information management and advanced log analysis and forensics

Overview

NetIQ Security Manager provides comprehensive security management for your heterogeneous enterprise, centralizing your ability to collect, view, analyze, archive and report on security information from across your organization. With real-time intrusion response capabilities, it is the only single product that encapsulates security information management and correlation, log management, intrusion protection and advanced analysis and reporting.

Solutions for Today

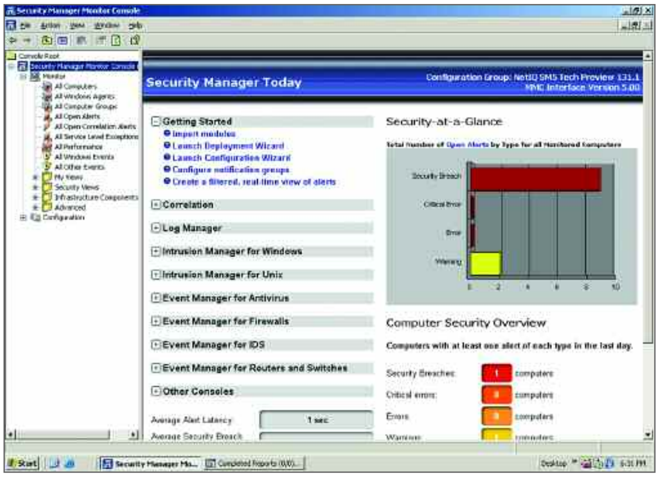
To meet the security and availability needs of the business, organizations continue to invest in a wide variety of security-point solutions, such as firewalls, antivirus products and intrusion detection systems. These technologies generate incredibly high volumes of security data that present an enormous challenge in achieving real-time detection of security breaches—much less being able to easily review and analyze that data.

NetIQ Security Manager enhances the value of your existing security infrastructure by consolidating and archiving log and event data from across the organization. The solution provides a comprehensive built-in security Knowledge Base, delivering powerful correlation and analysis tools, and enabling in-depth reporting to dramatically reduce the risks associated with your operation.

Key Benefits

Reduces exposure time - Optimizes reaction times with real-time monitoring for security incidents, extensive notification and information capabilities and automated responses.

Improves security knowledge - Delivers a comprehensive Knowledge Base that automatically builds security knowledge and internalizes new and updated information. This helps you ensure that the knowledge needed to understand and respond to incidents is available when needed.


Security Manager Monitor Console
File
Action
View
Window
Help
Console Root
Security Manager Monitor Console
Monitor
All Computers
All Windows Agents
All Computer Groups
All Open Alerts
All Open Correlation Alerts
All Service Level Exceptions
All Performance
All Windows Events
All Other Events
My Views
Security Views
Infrastructure Components
Advanced
Configuration
Security Manager Today
Configuration Group: NetIQ SMS Tech Preview 131.1
MMC Interface Version 5.00
Getting Started
Import modules
Launch Deployment Wizard
Launch Configuration Wizard
Configure notification groups
Create a filtered, real-time view of alerts
Correlation
Log Manager
Intrusion Manager for Windows
Intrusion Manager for Unix
Event Manager for Antivirus
Event Manager for Firewalls
Event Manager for IDS
Event Manager for Routers and Switches
Other Consoles
Security-at-a-Glance
Total Number of Open Alerts by Type for all Monitored Computers
Security Breach
Critical Error
Error
Warning
0
2
4
6
8
10
Computer Security Overview
Start
Security Manager Mo...
Completed Reports (0/0)...
Desktop
6:31 PM

Computers with at least one alert of each type in the last day.

Security Breaches: 1 computers
Critical errors: 3 computers
Errors: 3 computers
Warnings: 1 computers

Average Alert Latency: 1 sec
Average Security Breach

NetIQ Security Manager provides a single solution for protecting against intrusions, managing and correlating security events, and performing advanced forensics and trending.

Increases protection levels - Integrates and correlates real-time and archived data from all security systems and processes. By tracking incidents to ensure they are handled correctly and on time, you can achieve true incident lifecycle management for optimal protection.

Boosts operational performance - Improves ROI by consolidating security information from across your organization into a central location, filtering out noise and false positives, and presenting real incidents. This enables you to provide a focused monitoring and response capability.

Assures compliance - Facilitates regular review and reporting on enterprise security information, monitors security controls to validate their effectiveness and provides real-time enforcement of policies and best practices. This helps you satisfy the security requirements of today's regulations.

NetIQ Security Manager™

Key Features

Log Management

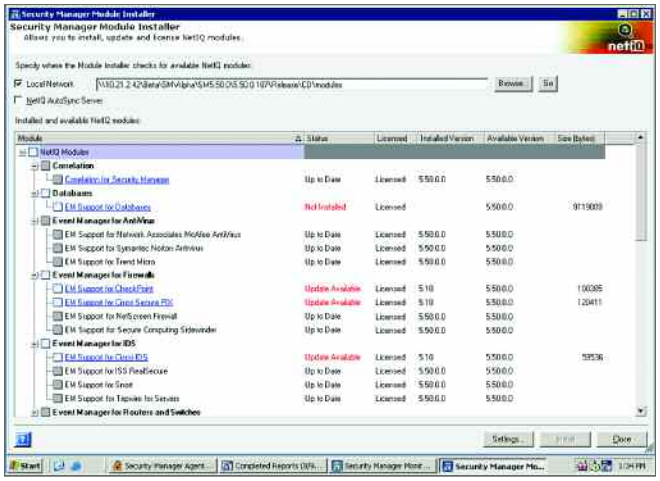
Quickly identify hidden threats while meeting audit and regulatory requirements with scaleable and centralized log and event consolidation, combined with powerful archival, forensics and trending analysis tools.

Helps satisfy legal log-retention requirements - Supplies a powerful, yet simple solution that enables you to meet audit and regulatory requirements that mandate security log and event information be collected and retained for extended periods of time.

Facilitates regular and easy review of security information - Provides reports, based on summarized security data, that present key security information, (e.g., failed log-on attempts), and which allow more in-depth analysis by clicking down into the report to reveal more detailed information. Updated daily, these reports facilitate regular reviews of security information, helping to meet both security best practice and regulatory requirements.

Enables the analysis of security trends - Enables baseline security activity to be visualized, as well as provide for the faster identification of anomalies through detailed and flexible trend analysis reports. With charts and data manipulation capabilities, you can show different visual representations of security event information.

Provides powerful forensics investigation capabilities - Dramatically reduces the time to find the root-cause behind an incident or anomaly through powerful forensics queries. With a forensics reporting interface, your alerts can be easily filtered, grouped and sorted for improved data mining.


Security Manager Module Installer
Start
Security Manager Agent...
Completed Reports (0/8...
Security Manager Moni...
Security Manager Mo...
1:34 PM

Security Manager Module Installer
Allows you to install, update and license NetIQ modules.

Specify where the Module Installer checks for available NetIQ modules:

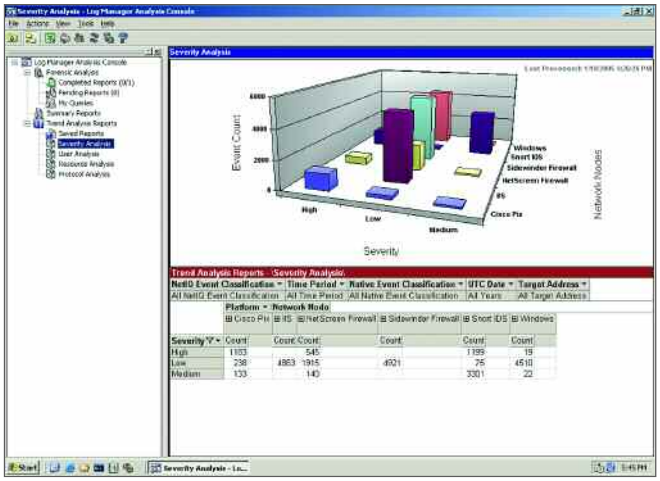
☑ Local Network \\10.21.2.42\beta\SMAlpha\SM5.50.0\5.50.0.107\Release\CD\modules [Browse...] [Go]
☐ NetIQ AutoSync Server

Installed and available NetIQ modules:

Module	Status	Licensed	Installed Version	Available Version	Size (bytes)
NetIQ Modules					
Correlation					
Correlation for Security Manager	Up to Date	Licensed	5.50.0.0	5.50.0.0	
Databases					
EM Support for Databases	Not Installed	Licensed		5.50.0.0	9119009
Event Manager for AntiVirus					
EM Support for Network Associates McAfee AntiVirus	Up to Date	Licensed	5.50.0.0	5.50.0.0	
EM Support for Symantec Norton Antivirus	Up to Date	Licensed	5.50.0.0	5.50.0.0	
EM Support for Trend Micro	Up to Date	Licensed	5.50.0.0	5.50.0.0	
Event Manager for Firewalls					
EM Support for CheckPoint	Update Available	Licensed	5.10	5.50.0.0	100385
EM Support for Cisco Secure PIX	Update Available	Licensed	5.10	5.50.0.0	120411
EM Support for NetScreen Firewall	Up to Date	Licensed	5.50.0.0	5.50.0.0	
EM Support for Secure Computing Sidewinder	Up to Date	Licensed	5.50.0.0	5.50.0.0	
Event Manager for IDS					
EM Support for Cisco IDS	Update Available	Licensed	5.10	5.50.0.0	59536
EM Support for ISS RealSecure	Up to Date	Licensed	5.50.0.0	5.50.0.0	
EM Support for Snort	Up to Date	Licensed	5.50.0.0	5.50.0.0	
EM Support for Tripwire for Servers	Up to Date	Licensed	5.50.0.0	5.50.0.0	
Event Manager for Routers and Switches					

[Settings...] [Install] [Done]

NetIQ AutoSync technology displays newly available security knowledge and product updates and facilitates their automatic upload and installation at runtime.

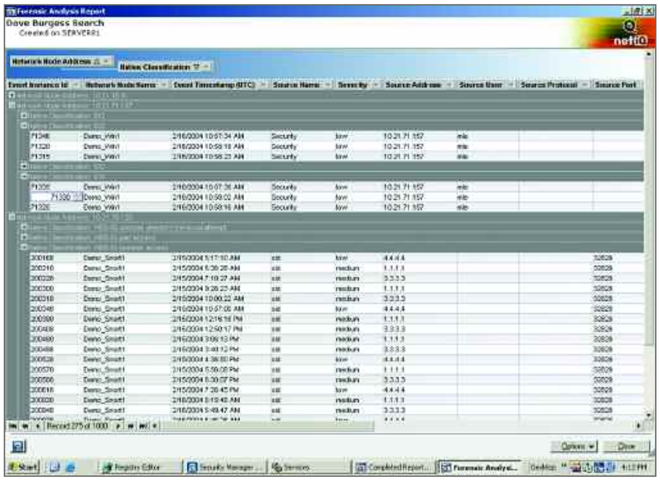


Trend Analysis Reports - Severity Analysis

NetIQ Event Classification	Time Period	Native Event Classification	UTC Date	Target Address
All NetIQ Event Classification	All Time Period	All Native Event Classification	All Years	All Target Address

	Platform - Network Node					
	Cisco Pix	IIS	NetScreen Firewall	Sidewinder Firewall	Snort IDS	Windows
Severity	Count	Count	Count	Count	Count	Count
High	1153		545		1199	19
Low	238	4863	1915	4921	75	4510
Medium	133		140		3301	22

Powerful analysis tools present multiple views of your enterprise security data to help identify trends, as well as detect anomalies and potential threats.



Dave Burgess Search
Created on SERVER01

Event Instance Id	Network Node Name	Event Timestamp (UTC)	Source Name	Severity	Source Address	Source User	Source Protocol	Source Port
71346	Demo_Win1	2/16/2004 10:57:34 AM	Security	low	10.21.71.157	n/a		
71320	Demo_Win1	2/16/2004 10:58:18 AM	Security	low	10.21.71.157	n/a		
71315	Demo_Win1	2/16/2004 10:58:23 AM	Security	low	10.21.71.157	n/a		
71305	Demo_Win1	2/16/2004 10:57:36 AM	Security	low	10.21.71.157	n/a		
71330	Demo_Win1	2/16/2004 10:58:02 AM	Security	low	10.21.71.157	n/a		
71326	Demo_Win1	2/16/2004 10:58:16 AM	Security	low	10.21.71.157	n/a		
200168	Demo_Snort1	2/15/2004 5:17:10 AM	snt	low	4.4.4.4			32828
200210	Demo_Snort1	2/15/2004 6:39:28 AM	snt	medium	1.1.1.1			32828
200226	Demo_Snort1	2/15/2004 7:10:27 AM	snt	medium	3.3.3.3			32828
200300	Demo_Snort1	2/15/2004 9:26:23 AM	snt	medium	1.1.1.1			32828
200318	Demo_Snort1	2/15/2004 10:00:22 AM	snt	medium	3.3.3.3			32828
200348	Demo_Snort1	2/16/2004 10:57:00 AM	snt	low	4.4.4.4			32829
200380	Demo_Snort1	2/16/2004 12:18:18 PM	snt	medium	1.1.1.1			32829
200408	Demo_Snort1	2/16/2004 12:50:17 PM	snt	medium	3.3.3.3			32829
200480	Demo_Snort1	2/16/2004 3:06:13 PM	snt	medium	1.1.1.1			32829
200488	Demo_Snort1	2/16/2004 3:40:12 PM	snt	medium	3.3.3.3			32829
200528	Demo_Snort1	2/16/2004 4:36:00 PM	snt	low	4.4.4.4			32829
200570	Demo_Snort1	2/15/2004 5:59:08 PM	snt	medium	1.1.1.1			32829
200586	Demo_Snort1	2/15/2004 6:30:07 PM	snt	medium	3.3.3.3			32829
200616	Demo_Snort1	2/15/2004 7:26:45 PM	snt	low	4.4.4.4			32829
200020	Demo_Snort1	2/16/2004 0:19:48 AM	snt	medium	1.1.1.1			32828
200040	Demo_Snort1	2/16/2004 5:49:47 AM	snt	medium	3.3.3.3			32828

Record 275 of 1000

[Options ▾] [Close]

Forensics reports provide comprehensive data mining capabilities, including filtering, sorting and grouping of data elements, enabling the fast identification of the root causes of incidents.

Intrusion Detection & Response

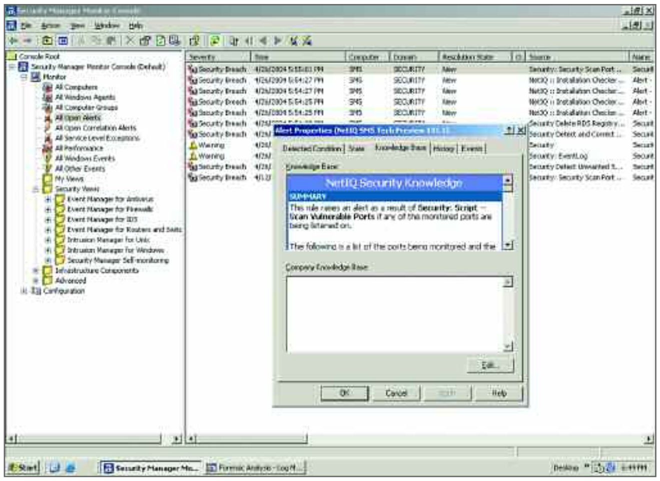
Improves system availability, service assurance and protects intellectual property with real-time intrusion detection and protection, along with a comprehensive security knowledge base to aid incident interpretation and response.

Facilitates rapid response to incidents - Delivers immediate notification of security breaches and policy violations with real-time alerting and notification, enabling you to react quickly and minimize the risk of any damage.

Minimizes security threat exposure times - Responds in real time to detected incidents, providing immediate protection by automatically stopping attacks in progress. The wizard-driven interface allows responses to be easily created and customized without requiring any programming knowledge.

Protects against intrusions - Detects and automatically terminates unauthorized or unknown user actions, services and processes; effectively blocking unauthorized activities, worms, viruses and rogue applications.

Improves staff effectiveness and security knowledge - Built-in security Knowledge Base contains detailed information on possible causes for alerts. This internalized knowledge can be extended with organizational-specific information such as incident-handling procedures. You can then ensure that knowledge gained can be reused by others and not walk out the door with the employee.


Security Manager Monitor Console
File Action View Window Help
Console Root
Security Manager Monitor Console (Default)
Monitor
All Computers
All Windows Agents
All Computer Groups
All Open Alerts
All Open Correlation Alerts
All Service Level Exceptions
All Performance
All Windows Events
All Other Events
My Views
Security Views
Event Manager for Antivirus
Event Manager for Firewalls
Event Manager for IDS
Event Manager for Routers and Switches
Intrusion Manager for Unix
Intrusion Manager for Windows
Security Manager Self-monitoring
Infrastructure Components
Advanced
Configuration
Alert Properties (NetIQ SMS Tech Preview 131.1)
Detected Condition
State
Knowledge Base
History
Events
Edit...
OK
Cancel
Apply
Help
Start
Security Manager Mo...
Forensic Analysis - Log M...
Desktop
4:49 PM

Severity	Time	Computer	Domain	Resolution State		Source	Name
Security Breach	4/26/2004 5:55:01 PM	SMS	SECURITY	New		Security: Security Scan Port ...	Securi
Security Breach	4/26/2004 5:54:27 PM	SMS	SECURITY	New		NetIQ :: Installation Checker ...	Alert -
Security Breach	4/26/2004 5:54:27 PM	SMS	SECURITY	New		NetIQ :: Installation Checker ...	Alert -
Security Breach	4/26/2004 5:54:25 PM	SMS	SECURITY	New		NetIQ :: Installation Checker ...	Alert -
Security Breach	4/26/2004 5:54:25 PM	SMS	SECURITY	New		NetIQ :: Installation Checker ...	Alert -
Security Breach	4/26/					Security Delete RDS Registry ...	Securi
Security Breach	4/26/					Security Detect and Correct ...	Securi
Warning	4/26/					Security	Securi
Warning	4/26/					Security: EventLog	Securi
Security Breach	4/26/					Security Detect Unwanted S...	Securi
Security Breach	4/1/2					Security: Security Scan Port ...	Securi

Knowledge Base:

NetIQ Security Knowledge

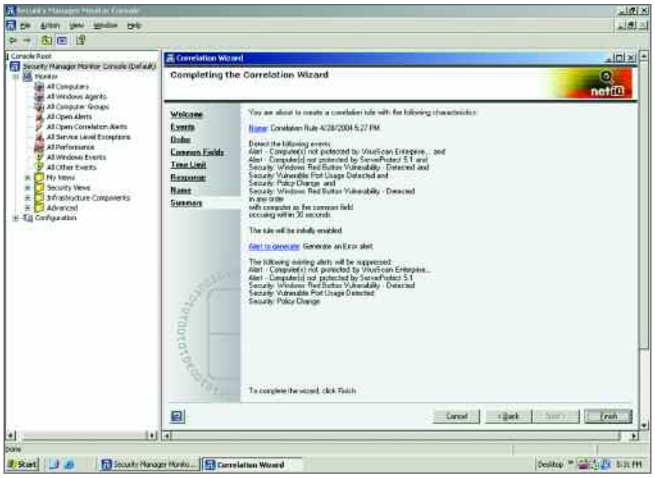
SUMMARY

This rule raises an alert as a result of **Security: Script -- Scan Vulnerable Ports** if any of the monitored ports are being listened on.

The following is a list of the ports being monitored and the

Company Knowledge Base:

A built-in extendable security Knowledge Base centralizes monitoring and response to security alerts generated anywhere in the organization.



Completing the Correlation Wizard

You are about to create a correlation rule with the following characteristics:

Name: Correlation Rule 4/28/2004 5:27 PM

Detect the following events:
Alert - Computer(s) not protected by VirusScan Enterprise... and
Alert - Computer(s) not protected by ServerProtect 5.1 and
Security: Windows Red Button Vulnerability - Detected and
Security: Vulnerable Port Usage Detected and
Security: Policy Change and
Security: Windows Red Button Vulnerability - Detected
in any order
with computer as the common field
occuring within 30 seconds

The rule will be initially enabled

Alert to generate: Generate an Error alert

The following existing alerts will be suppressed:
Alert - Computer(s) not protected by VirusScan Enterprise...
Alert - Computer(s) not protected by ServerProtect 5.1
Security: Windows Red Button Vulnerability - Detected
Security: Vulnerable Port Usage Detected
Security: Policy Change

To complete the wizard, click Finish

Reduces noise and false positives by correlating events from various security sensors and accurately identifying critical security incidents.

Security Information Management & Correlation

Presents meaningful and real-time security information that represents the true security state of your organization by identifying real incidents from amongst event noise and false positive alerts. This facilitates a prioritized and tracked response.

Maximizes the value of your security infrastructure - Optimizes your defenses and countermeasures through a centralized security operations center that securely collects, correlates, analyzes and responds to events from key assets, security point products and network devices.

Reduces event noise and false positives - Powerful real-time correlation engine minimizes irrelevant information, removing the need to sort through the deluge of security events and allowing security teams to see and focus on the real incidents. A correlation wizard enables new correlation rules to be quickly created and take immediate effect.

Assures that security incidents are not lost or forgotten - Internal incident tracking workflow allows organizations to immediately prioritize incidents and track their status at any time. Response activity information can be added to provide an audit trail of how incidents are handled.

Ensures that the latest updates are available - Provides an easy-to-use, dynamic mechanism to receive update notifications to product functionality and knowledge. It also facilitate painless delivery and installation of those updates, using NetIQ's AutoSync technology.

NetIQ Security Manager™

Technical Summary

Centralized Management

- Single and centralized management console
- Consolidates and normalizes security event and log data from across the enterprise
- Advanced correlation to identify blended threats and reduce false positives

Incident Identification and Management

- Security Knowledge Base for information on alerts and guidelines for incident resolution
- Internal incident tracking system
- Extensive and customizable response capabilities—including notification, script execution, or service termination

Advanced Reporting and Analysis

- Flexible and scalable log archiving infrastructure
- Pre-built and extendable report templates
- Trending analysis reports and tools
- Powerful forensics investigation capabilities
- Report scheduling to automate when reports are run

Architectural Scalability and Stability

- Designed to handle the high event volumes
- Agent and agent-less capabilities
- Dynamically update knowledge, reports, and supported endpoints via AutoSync
- Fault tolerant design
- Agent heartbeat monitoring

Supported Systems & Devices

NetIQ Security Manager provides out-of-the-box support for a broad range of heterogeneous endpoints and applications, including support for:

- Servers and workstations - including Microsoft, Linux, Unix and iSeries
- Critical services – including databases, Active Directory, and VoIP infrastructure
- Security point solutions – including antivirus products, firewall products, intrusion detection and protection systems
- Network devices – including routers and switches
- NetIQ solutions – including NetIQ Vulnerability Manager™, NetIQ AppManager®, NetIQ Change Guardian™ for Active Directory, NetIQ Group Policy Guardian™

Through its AutoSync capability, NetIQ Security Manager can be easily extended to monitor other products, systems and devices. Please contact your NetIQ representative for more information on how NetIQ can assist in supporting your environment and specific requirements.

Minimum System Requirements

- 1.5GHz Intel Pentium, with 1GB RAM
- Windows 2000/2003 Server
- Microsoft SQL Server 2000 (for Database Server)
- Microsoft SQL Server 2000 SP3a Analysis Services (for Trend Analysis Server)
- IIS 5.0+ (for Web Console Server)

Contacts

Worldwide Headquarters
NetIQ Corporation
3553 North First Street
San Jose, CA 95134
713.548.1700
713.548.1771 fax
888.323.6768 sales
info@netiq.com
www.netiq.com

NetIQ EMEA
+44 (0) 1784 454500
info@netiq.com

NetIQ Japan
+81 3 5909 5400
info-japan@netiq.com
www.netiq.co.jp

NetIQ Australia
& New Zealand
+61 2 9925 2100
www.netiq.com.au

For our offices in Latin America & Asia Pacific,
please visit our web site at www.netiq.com/contacts