

NetIQ Security Manager™

Delivers comprehensive, centralized security management in real time

Overview

NetIQ Security Manager is a comprehensive, security incident management solution for your enterprise. Designed specifically to protect your confidential data in an increasingly complex and insecure business world, it is the only product that provides a single solution for protecting against intrusions, managing and correlating security events, and performing advanced forensics and trending.

Solutions for Today

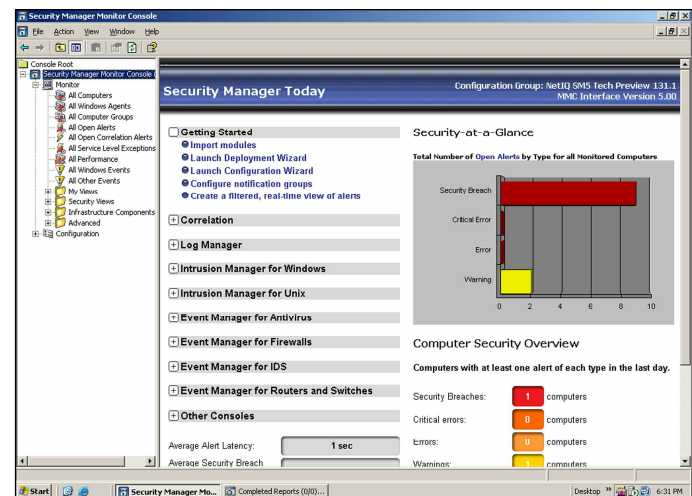
In an attempt to meet the connectivity needs of the business while maintaining the security of an enterprise, organizations continue to invest in a wide variety of security-point solutions, such as firewalls, antivirus products and intrusion detection systems. These technologies generate incredibly high volumes of security data that, especially with limited resources, present an enormous challenge for organizations in achieving real-time detection of security breaches and the later analysis of that data.

NetIQ Security Manager delivers security incident management across the event lifecycle by leveraging powerful correlation, intrusion protection, reporting, forensics and trending capabilities. It is the most comprehensive security incident management solution available today. The product enables organizations to increase the overall level of enterprise security by dramatically helping to reduce exposure times, increasing security knowledge and leveraging the investments already made in existing and future point-security solutions. NetIQ Security Manager assists customers in knowing that they are in compliance, knowing that they are effectively managing their risk and knowing that their assets are secure.

Assuring compliance – NetIQ Security Manager helps you assure customers, business partners, regulators—even the courts, if necessary—that you have proactively enforced security of your IT infrastructure. Specifically, NetIQ Security Manager monitors implementations of your technical security policies, assesses compliance with those policies, identifies vulnerabilities and provides an effective security-incident detection and management capability.

Managing risk – Your business cannot completely eliminate risk, but NetIQ Security Manager can assist in intelligently and cost-effectively managing that risk. Through its ability to correlate real-time and archived security information from multiple point-security solutions throughout the enterprise architecture, NetIQ Security Manager enables you to effectively monitor your organization's IT security via a "single pane of glass." When security incidents do occur, NetIQ Security Manager aids incident response teams to quickly resolve those incidents by providing up-to-date security knowledge and enables them to perform root-cause analysis through its comprehensive forensics capabilities.

Securing assets – Keeping your IT systems secure in the face of constant changes in hardware, software, threats and regulations may seem impossible. Through its multi-layered approach to intrusion defense, NetIQ Security Manager balances the needs of managing security with the demands of managing performance and availability. By proactively discovering, detecting and preventing intrusive activities, NetIQ Security Manager maximizes the security posture of the enterprise.



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

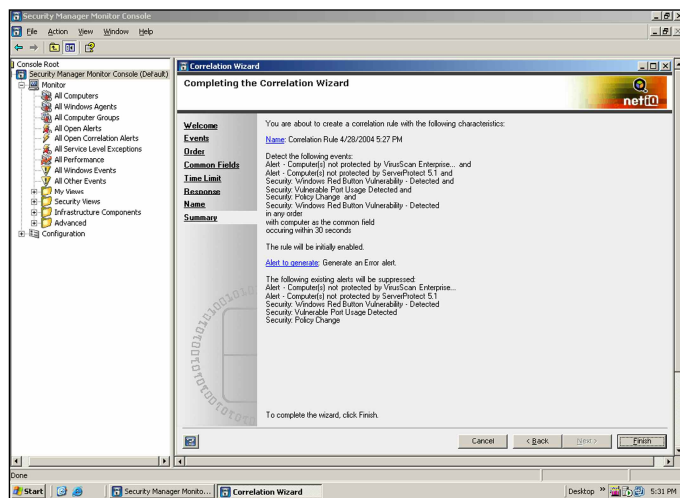
Key Benefits

Reduces exposure time – Protects against downtime and loss of confidential data. NetIQ Security Manager reduces detection times through its real-time monitoring for security breaches and policy violations, as well as its extensive notification capabilities. It also optimizes reaction times with automated responses and security knowledge.

Improves security knowledge – Delivers an automated infrastructure that builds internal security knowledge for deployment and customization. You can quickly resolve issues by combining the out-of-the-box NetIQ Knowledge Base with security knowledge specific to your company.

Increases protection levels – Ensures layered defenses are in place to maximize your security posture. With NetIQ Security Manager, you can integrate real-time and archived data from all security systems and processes, including correlation, to achieve true incident lifecycle management.

Boosts operational performance – Improves ROI by centralizing your best-of-breed security products into a central security console, enabling real-time notification and automated response to suspicious activity. NetIQ Security Manager ensures compliance from all of your security sensors and tools and alerts you of important issues, such as non-compliant firewall configurations or outdated virus signatures and vulnerability test libraries. The product also provides audit reporting and enforces policies and best practices across the enterprise for security mandates, such as HIPAA and GLBA.



A built-in customizable security knowledge base centralizes monitoring and response to security alerts generated anywhere in the organization by security sensors placed across the enterprise.

Modules

NetIQ Security Manager's various modules enable you to manage your security information and identify and respond quickly to a wide range of security threats. NetIQ Security Manager modules include:

Log Manager for NetIQ Security Manager

Log Manager for NetIQ Security Manager enables you to meet audit and legal requirements, as well as identify hidden threats, with powerful real-time security log consolidation, forensics and trending analysis. This module:

Provides ability to meet legal and business log-retention requirements – Supplies a powerful, yet simple solution that enables you to meet audit requirements. With instant event collection, assured delivery and relational database storage and data access, Log Manager can be customized to collect any log event or log data.

Reduces security threat exposure times – Provides real-time collection of events and enables notification for critical events. Log Manager helps you record, retain and disseminate event-specific company knowledge.

Identifies source and extent of security breaches and policy violations – Delivers centralized analysis and forensics capabilities through real-time, highly scalable event collection and consolidation. Log Manager helps you meet legal irrefutability standards and allows you to analyze data through specialized views and customizable reporting.

Ensures security audit policies are enforced across your organization – Enables the centralized definition and enforcement of audit settings that should be set and enforced across all distributed computers. This automated and totally hands-free audit setting enforcement guarantees that object access, account changes, service activity, logons and other security-sensitive events are logged accordingly.

Improves staff productivity, effectiveness and security expertise – Eases the burdens associated with the collection of, and access to, logs from distributed servers, applications and network devices by consolidating events into a single SQL database. Pre-built report templates make the data simple to digest and analyze.

Intrusion Manager for NetIQ Security Manager

Intrusion Manager for NetIQ Security Manager improves server and application availability and protects intellectual property with real-time, host-based intrusion detection and response. This module:

Minimizes security threat exposure times – Delivers immediate notification of security breaches and policy violations with real-time alerting and notification tools. These powerful capabilities enable you to react quickly enough to prevent damage resulting from suspicious activity when it is happening. Automated response actions react to events instantaneously to stop attacks in progress. This also serves to maximize availability by avoiding downtime.

Automatically stops security breaches and policy violations – Detects and responds to breaches and violations with guaranteed delivery and priority handling of critical security alerts, as well as customizes automated response actions.

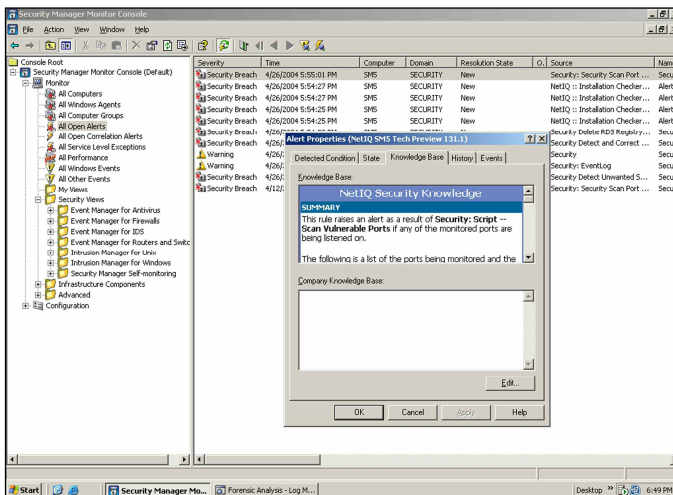
Enforces internal security policies – Enforces acceptable use policies and identifies permission escalations, enabling you to automatically respond and notify key personnel of misuse or unauthorized activity. This capability prevents potential integrity and confidentiality compromises that would impact overall availability.

Protects against external intrusions – Detects and automatically terminates unauthorized or unknown services and processes, such as worms, viruses or rogue applications. Blended threats can be identified and quarantined through event-correlation capabilities.

Event Manager for NetIQ Security Manager

Event Manager for NetIQ Security Manager centralizes the management of security devices across the event lifecycle, including real-time monitoring, advanced correlation, analysis, automated response and reporting. This module:

Enables corporate security teams to prevent outbreaks – Optimizes your defenses and countermeasures through a centralized security operations center that collects, correlates, analyzes and responds to events from key security systems and point products. This complete coverage enables you to effectively protect against complex blended threats.



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

Maximizes the value of your security infrastructure

– Monitors the operations, performance and configuration of your security point products to assure that you achieve maximum results and value. These NetIQ Security Manager components sort through the massive volume of events produced, notify you of critical issues and automatically respond so your defenses are optimized.

Identifies and responds to breach attempts and policy violations in real time – Prevents security breaches and policy violations in real time to avoid loss of confidential data, reduce data integrity risks and improve availability. Automated response actions react to events instantaneously to stop attacks in progress. Other actions, such as instant detection of administrator actions, changing audit settings or attempts to clear an event log, allow you to take immediate action.

Isolates breach origination and assesses damages

– Centralizes forensics, trending and audit analysis and offers both pre-configured and customizable views to meet your specific needs.

Technical Features

Centralized Management

- Single management console, presenting the security state of the enterprise “at a glance”
- Aggregation, normalization and consolidation of security data from across the enterprise

Incident Identification and Management

- Advanced correlation to identify blended threats and reduce false positives
- Ability to receive alerts from NetIQ Vulnerability Manager and NetIQ AppManager
- NetIQ Knowledge Base incorporated for alert resolution information (including links to security services such as SANS)
- Incident tracking system to manage alerts from origination to resolution

Intrusion Protection

- Identifies policy violations
 - Out-of-date anti-virus DAT/signature files
 - Unauthorized applications, (e.g., I0phtcrack, NetBus) or services, (e.g., SNMP, IIS, RAS)
- Extensive response capabilities
 - Notification via pager or email
 - Ability to execute a program, command, or script, or kill a service or process

Advanced Reporting and Investigatory Capabilities

- Pre-built and extendable report templates
- Extensive reporting and trending analysis tools
- Powerful forensics investigation capabilities

Architectural Scalability and Stability

- Agent or agent-less capabilities
- Enterprise-class data warehousing
 - Architected for high volumes of security data
 - Flexible archival capabilities
- Ensures high availability
 - Fault tolerant capabilities
 - Agent heartbeat monitoring

System Requirements

Database Computer Requirements:

- 500 MHz Intel Pentium II or equivalent (1.5 GHz Intel Pentium or better recommended in environments expecting more than one million total events)
- 1.7GB + free disk space (fast disk access, multiple physical devices and RAID arrays recommended for most environments)
- 256MB RAM (1GB recommended)
- Windows 2000 Server

Central Computer Requirements:

- 500 MHz Intel Pentium II or equivalent (1.5 GHz Intel Pentium or better recommended in environments expecting more than one million total events)
- 1.7GB free disk space (fast disk access, multiple physical devices and RAID arrays recommended for most environments)
- 256MB RAM (1GB recommended)
- 256 color display with resolution of at least 1024 x 768

Supported Systems & Devices

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

- **Servers and workstations** – including Microsoft, Linux, Unix and iSeries platforms
- **Antivirus products**
- **Firewall products**
- **Intrusion Detection Systems**
- **Routers and Switches**

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.

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.com/japan

NetIQ Australia & New Zealand

61 (0) 2 9959 2313
www.netiq.com/au

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