NetIQ Security Manager

Integrated security and event management for critical data protection

Introduction

To meet 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 – making it difficult to easily review and analyze that data.

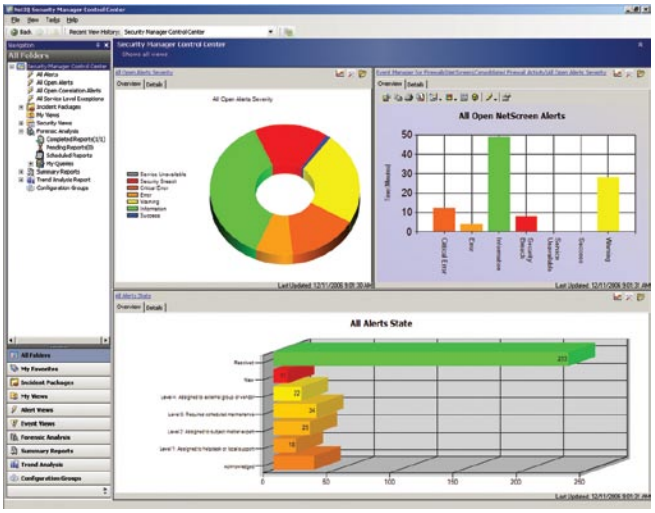
NetIQ® Security Manager™ enhances the value of your existing security infrastructure by pulling log and event data from across your organization into one central management console and database, enabling you to quickly and easily gain a clear picture of your overall information security levels, respond to threats, and satisfy regulatory compliance requirements.

Product Overview

NetIQ Security Manager provides real-time monitoring of system changes and user activity, detection of threats and intrusions, security event management and correlation, log management, and incident response automation – all with a single, integrated, and scalable infrastructure.

By consolidating and archiving log and event data from across the network, the solution provides a comprehensive knowledge base for analysis and remediation, while also helping satisfy legal log-retention requirements. NetIQ Security Manager provides out-of-the-box support for a broad range of heterogeneous endpoints and applications including:

- **Servers and workstations** – including Microsoft, Linux, Unix and IBM iSeries.
- **Critical services** – including databases, Microsoft Active Directory, and VoIP infrastructure.
- **Security point solutions** – including antivirus products, firewalls, and intrusion detection and protection systems.
- **Network devices** – including routers and switches.
- **NetIQ solutions** – including NetIQ® Secure Configuration Manager™, NetIQ® Aegis®, NetIQ® Change Guardian™ for Windows, NetIQ Change Guardian for Active Directory, NetIQ Change Guardian for Group Policy, and NetIQ Change Guardian for Databases.



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

Capabilities

NetIQ Security Manager enables you to effectively manage your information security infrastructure by giving you the unique ability to capture, correlate, analyze, and respond to events throughout the organization from one centralized security console. This allows you to:

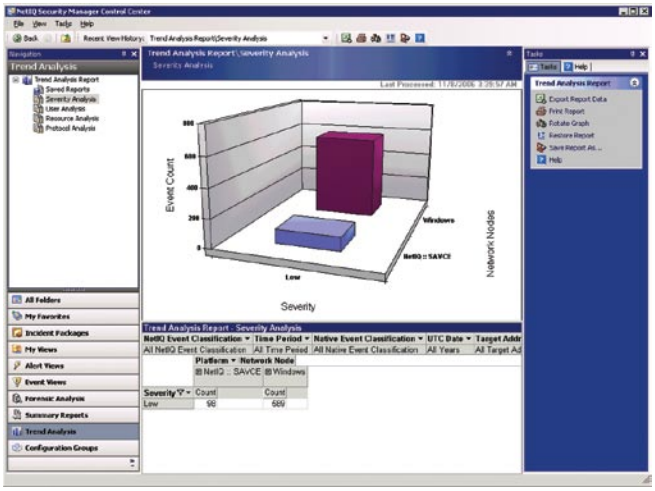
Increase protection and reduce risk – correlate data from multiple endpoints and applications, so you don't miss a thing.

Reduce exposure time – respond quickly to real-time alerts or set up automated responses in order to reduce risks of data leakage or other losses.

Get the big picture and the smallest details – use powerful filtering and reporting tools to obtain the exact data you need, from security trend analysis to forensic investigations.

Satisfy your need for compliance – enforce your security policies and best practices in real time, while meeting log-retention, review, and reporting requirements of today's regulations.

NetIQ Security Manager



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

Features

NetIQ Security Manager enables system administrators and information security managers to use one central console to effectively manage three critical functions: log management and forensics, access control and user monitoring, and security event correlation and analysis. Features include:

- Unified security operations console enables you to manage multiple security functions quickly and easily.
- Rules-based correlation engine gives you a clear picture of related security events across the network, while reducing event noise and false positives.
- Internal incident tracking workflow allows organizations to immediately prioritize incidents and track their status at any time, preventing security incidents from being lost or forgotten.
- Secure and cost-effective log management using TRACE™ (Trend Reporting, Analytics, and Centralized Examination) technology provides high-speed log forensics, streamlined log reviews, expedited security incident response, and multidimensional reporting.
- Agents and agent-less monitoring and collection allow for user monitoring and change detection at both the server and local level.
- System-level changes, such as file modifications, user privilege changes, log file clearing, software installation, registry changes, and object changes, can be monitored in real time to protect against malicious or accidental changes.
- Summarized and detailed reporting, including advanced data mining capabilities, provides audit trail data for regulatory compliance, security trend analysis, and forensic investigation needs.
- Real-time security alerts facilitate rapid response to incidents, reducing risk of loss or damage.
- A built-in security knowledge base publishes information on possible causes for alerts, improving staff effectiveness and security knowledge.
- Easy delivery and installation of latest updates to security database, using NetIQ Autosync technology.

Key differentiators

Maximum log management performance
NetIQ Security Manager leverages TRACE™ technology, which utilizes proprietary, file-based distributed storage that radically improves log management over traditional relational databases, enabling you to do more with one integrated system.

More data from more sources equals greater protection
While other security solutions may promise protection, their coverage is often limited to a small number of devices. With NetIQ Security Manager's comprehensive support of a wide variety of endpoints and applications, you can be confident knowing your information assets are covered.

Powerful data protection anytime, anywhere
NetIQ Security Manager's monitoring and protection extends beyond the server to the host and user – meaning you get the real-time information and detailed analysis you need to help proactively identify and resolve potential data breaches and compliance failures.

Contacts

Worldwide Headquarters
NetIQ
An Attachmate Business
1233 West Loop South
Suite 810
Houston, TX 77027
713.548.1700
713.548.1771 fax
888.323.6768 sales
info@netiq.com
www.netiq.com

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

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

NetIQ Australia & New Zealand
+61 3 9825 2300
www.netiq.com.au

For additional office locations, partners and resellers, please visit our web site at www.netiq.com/contacts.

PB10259SMGR PS 01/10

netIQ An Attachmate® Business