

# NetIQ Security Manager

## Sicherheitsmanagement mit integrierter Ereignisbehandlung zum Schutz wichtiger Daten

### Einleitung

Mit dem Ziel, die Anforderungen an Sicherheit und Verfügbarkeit zu erfüllen, investieren Unternehmen oft in eine Vielzahl punktueller Sicherheitslösungen, wie beispielsweise Firewalls, Antivirenprogramme und Systeme zur Erkennung von Eindringversuchen. Diese Technologien erzeugen sehr große Datenmengen, wodurch es schwer wird, diese Daten auf einen Blick zu prüfen und zu analysieren, um Sicherheitsverstöße in Echtzeit zu erkennen.

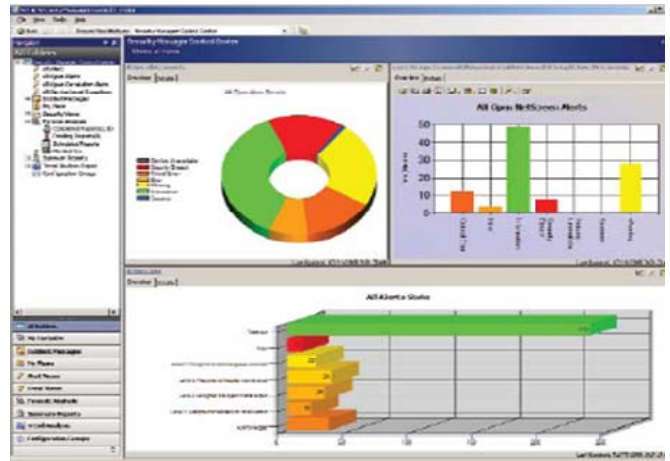
NetIQ® Security Manager™ nutzt die vorhandene Sicherheitsinfrastruktur, indem Log- und Ereignisdaten unternehmensweit in einer zentralen Managementkonsole und Datenbank zusammengeführt werden. So wird es möglich, sich auf Anhieb ein klares Bild über die Informationssicherheit zu verschaffen, auf Bedrohungen zu reagieren und Richtlinien und Vorschriften zu erfüllen.

### Überblick

NetIQ Security Manager überwacht Systemveränderungen und Benutzeraktivitäten in Echtzeit, erkennt Bedrohungen und Eindringversuche, verwaltet und korreliert sicherheitsrelevante Ereignisse, führt ein Log-Management durch und reagiert automatisch auf Vorfälle - und das alles innerhalb einer integrierten und skalierbaren Infrastruktur.

Durch die netzwerkweite Konsolidierung und Archivierung von Log- und Ereignisdaten stellt die Lösung eine umfassende Wissensdatenbank für Analyse- und Abhilfemaßnahmen zur Verfügung und trägt gleichzeitig dazu bei, die gesetzlichen Vorschriften zur Aufzeichnung und Speicherung von Daten einzuhalten. Standardmäßig unterstützt NetIQ Security Manager bereits ein breites Spektrum von heterogenen Endgeräten und Anwendungen, u.a.:

- **Server und Workstations** - inkl. Microsoft, Linux, Unix und IBM iSeries.
- **Wichtige Dienste** - inkl. Datenbanken, Microsoft Active Directory und VoIP-Infrastruktur.
- **Punktuelle Sicherheitslösungen** - inkl. Antivirensoftware, Firewalls, Systeme zur Erkennung und Abwehr von Eindringversuchen.
- **Netzwerkgeräte** - inkl. Router und Switches.
- **NetIQ Lösungen** - inkl. NetIQ® Secure Configuration Manager™, NetIQ® Aegis®, NetIQ® Change Guardian™ for Windows, NetIQ Change Guardian for Active Directory, NetIQ Change Guardian for Group Policy und NetIQ Change Guardian for Databases.



NetIQ Security Manager ist eine einheitliche Lösung zum Schutz gegen unbefugte Benutzeraktivitäten, zur Verwaltung und Korrelation von sicherheitsrelevanten Ereignissen und zur Durchführung weitreichender forensischer Untersuchungen und Trendanalysen.

### Funktionalität

Mit NetIQ Security Manager sind Unternehmen in der Lage, ihre Informationssicherheitsinfrastruktur effektiv zu verwalten. Hierzu werden Ereignisse unternehmensweit über eine zentrale Sicherheitskonsole erfasst, korreliert und analysiert, um schnell und gezielt reagieren zu können. Die Funktionalität in Stichpunkten:

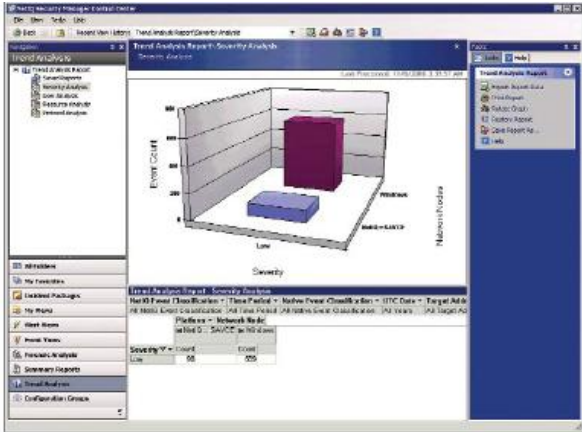
**Höherer Schutz und geringeres Risiko** - Korrelation der Daten über mehrere Endpunkte und Anwendungen hinweg. So gehen keine wichtigen Informationen verloren.

**Risikominimierung** - Schnelle Reaktion auf Echtzeitmeldungen oder automatische Behandlung von Ereignissen zur Reduzierung des Risikos von Datenverlusten.

**Darstellung der Gesamt- und Detailansicht** - Filter- und Reporting-Werkzeuge zur Einholung genauer Daten für sicherheitstechnische Trendanalysen und forensische Untersuchungen.

**Einhaltung geltender Vorschriften** - Durchsetzen von Sicherheitsrichtlinien und bewährten Verfahren in Echtzeit unter Beachtung der Vorschriften für Datenaufzeichnung und Berichtswesen.

# NetIQ Security Manager



Leistungsstarke Analyseinstrumente eröffnen mehrere Ansichten auf sicherheitsrelevante Daten des Unternehmens, um Trends zu ermitteln, Anomalien zu erkennen und potenzielle Bedrohungen abzuwenden.

## Leistungsmerkmale

NetIQ Security Manager versetzt Systemadministratoren und Information-Security-Manager in die Lage, eine zentrale Konsole zur effektiven Verwaltung der drei kritischen Funktionen zu verwenden: Log-Management und Forensik; Zugriffskontrolle und Benutzerüberwachung; Korrelation und Analyse von Sicherheitsereignissen. Das System zeichnet sich u.a. durch folgende Merkmale aus:

- Die Konsole für vereinheitlichte Sicherheitsoperationen ermöglicht eine schnelle und einfache Verwaltung mehrerer Sicherheitsfunktionen.
- Die regelbasierte Correlation-Engine vermittelt netzwerkweit ein klares Bild der maßgeblichen Sicherheitsereignisse und sorgt gleichzeitig für weniger unnötige Meldungen und Fehlalarme.
- Der Workflow zur Nachverfolgung interner Vorfälle ermöglicht es, Vorfälle unverzüglich und mit Priorität zu behandeln und deren Status jederzeit nachzuverfolgen. Sicherheitsrelevante Vorfälle können nicht mehr übersehen oder außer Acht gelassen werden.
- Das sichere und kosteneffiziente Log-Management mit der TRACE™-Technologie (Trend Reporting, Analytics, and Centralized Examination) ermöglicht eine schnelle forensische Analyse der Logs, effiziente Log-Reviews, unverzügliche Reaktionen auf Sicherheitsvorfälle und ein mehrdimensionales Berichtswesen.

## Kontakt

**Internationaler Sitz**  
**NetIQ, An Attachmate**  
**Business**  
1233 West Loop South  
Suite 1800  
Houston, TX 77027, USA  
713.548.1700  
713.548.1771 Fax

**NetIQ Deutschland**  
+49 (0)89 99351-0  
infoDE@netiq.com  
www.netiq.de

**NetIQ Schweiz**  
+41 43399 2090  
infoCH@netiq.com  
www.netiq.de

**NetIQ Österreich**  
+43 1 595 4335  
infoDE@netiq.com  
www.netiq.de

Informationen über weitere Geschäftsstellen, Partner und Wiederverkäufer finden Sie auf unserer Website unter [www.netiq.com/contacts](http://www.netiq.com/contacts)

- Die agentengestützte und agentenlose Überwachung und Erhebung von Daten ermöglicht die Überwachung der Benutzer und die Erkennung von Änderungen auf lokaler und Serverebene.
- Änderungen auf Systemebene, beispielsweise Änderungen an Dateien, Änderungen an Benutzerrechten, Löschen von Log-Files, Installieren von Software, Änderungen an der Registry und an Objekten, werden zum Schutz gegen böswillige oder versehentliche Änderungen in Echtzeit überwacht.
- Übergeordnetes oder detailliertes Reporting mit ausgefeilten Data-Mining-Funktionen unterstützt durch lückenlose Nachverfolgung die Einhaltung aufsichtsrechtlicher Vorgaben, ermöglicht sicherheitsrelevante Trendanalysen und liefert Informationen für forensische Untersuchungen.
- Sicherheitsmeldungen in Echtzeit ermöglichen eine schnelle Reaktion auf Vorfälle und mindern die Gefahr von Verlusten oder Schäden.
- Eine integrierte Wissensdatenbank liefert Informationen zu möglichen Ursachen von Warnmeldungen und fördert so die effiziente Arbeitsweise und Qualifizierung der Mitarbeiter.
- Die NetIQ AutoSync-Technologie sorgt für eine unkomplizierte Bereitstellung und Installation der neuesten Updates der Sicherheitsdatenbank.

## Wesentliche Unterscheidungsmerkmale

### Log-Management mit maximaler Leistung

NetIQ Security Manager nutzt die TRACE™-Technologie, ein System, das auf einer eigenen, dateigestützten, verteilten Speicherung beruht, die das Log-Management gegenüber herkömmlichen relationalen Datenbanken erheblich verbessert und den Funktionsumfang eines integrierten Systems deutlich vergrößert.

### Höherer Schutz durch mehr Daten aus mehreren Quellen

Andere Sicherheitslösungen versprechen zwar einen hohen Schutz, sind aber oft auf wenige Geräte beschränkt. NetIQ Security Manager schützt wesentlich umfassender, weil die Lösung eine Vielzahl von Endgeräten und Anwendungen unterstützt und so dafür sorgt, dass alle Informationsressourcen abgedeckt werden.

### Überall und jederzeit ein leistungsstarker Datenschutz

Die Überwachungs- und Schutzfunktionen von NetIQ Security Manager gehen über den Server hinaus und erstrecken sich auch auf Hostsystem und Benutzer. So liegen stets alle Echtzeitdaten und detaillierten Analysen vor, die für eine initiale Erkennung und Abwendung potenzieller Gefahren

NetIQ, das NetIQ-Zeichen, NetIQ Security Manager, NetIQ Secure Configuration Manager, NetIQ Aegis, NetIQ Change Guardian und TRACE sind Marken oder eingetragene Marken der NetIQ Corporation in den Vereinigten Staaten. Alle sonstigen Firmen- und Produktnamen sind möglicherweise Marken oder eingetragene Marken der jeweiligen Inhaber.

© 2010 NetIQ Corporation, alle Rechte vorbehalten.

DS10259SMGR PS 01/10

