

# NetIQ Security Solutions for IBM iSeries

## Die Lösung für sichere Business Continuity auf allen iSeries-Servern

### Im Überblick

NetIQ® Security Solutions for IBM iSeries trägt dazu bei, Sicherheitsrisiken zu vermeiden und eine betriebliche Kontinuität im Umfeld der iSeries-Systeme durch vereinfachte Prüfungsabläufe, Schutz gegen Eindringversuche, Schwachstellenermittlung und sichere Benutzerverwaltung für iSeries/i5- und AS/400-Systeme zu gewährleisten.

Der kombinierte Einsatz mit NetIQ® Security Manager™ und NetIQ® Secure Configuration Manager™ gewährleistet über sämtliche iSeries-Server eines Unternehmens hinweg ein hohes Maß an Sicherheit und Compliance für alle Betriebssysteme und Dienste, die auf der iSeries/i5-Plattform unterstützt werden.

### Zeitgemäße Lösungen

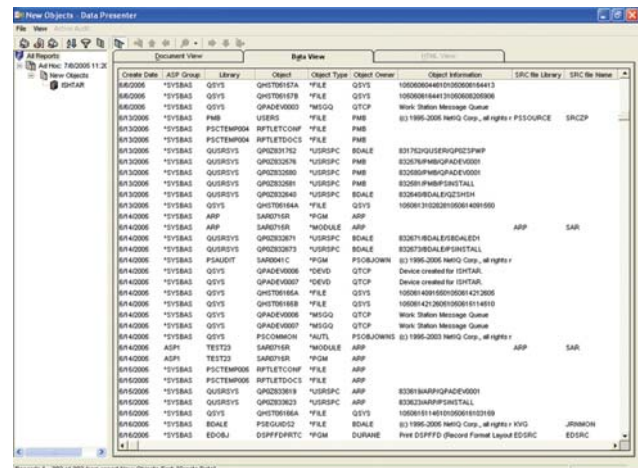
Obschon die iSeries-Plattform bereits von Haus aus mit einem hohen Maß an Sicherheit ausgestattet ist, wird das maximal mögliche Sicherheitspotenzial in den Standardkonfigurationen doch nicht ausgeschöpft. Weil komplexe Systeme zahlreiche Zugangspunkte aufweisen, ist die Rückverfolgung und Kontrolle des Zugriffs auf die iSeries-Server und auf die darauf befindlichen geschäftswichtigen Daten wichtiger denn je. NetIQ Security Solutions for iSeries ermöglicht es, die iSeries-Plattformen aktiv und vergleichsweise einfach zu schützen, um die Leistung und Verfügbarkeit der ausgeführten Dienste zu gewährleisten und die Produktivität durch eine sichere und übersichtliche Benutzerverwaltung zu verbessern.

### Entscheidende Vorteile

**Aktiver Schutz für die iSeries-Plattformen** – Rigide Zugriffskontrollen gleichermaßen auf Netzwerk- wie auf Objektebene ermöglichen es, Systeme unter OS/400 und i5/OS schnell und effektiv zu schützen, indem bewährte Verfahren von NetIQ für die Überwachung der Sicherheit und die Erkennung von Konfigurationsproblemen und Schwachstellen herangezogen werden.

**Sicherheit durch verbesserte Rechteverwaltung** – Administratoren können auf sämtlichen Systemen das "Minimalrechteprinzip" für Benutzer durchsetzen, um Risiken zu mindern und sensible Daten zu schützen, indem Zugriff und Rechte anhand von aufgaben- und zeitspezifischen Parametern gesteuert werden.

**Übereinstimmung mit Richtlinien, Standards und Sicherheitsauflagen** – Die enge Integration mit NetIQ Secure Configuration Manager versetzt Sicherheitsspezialisten und Auditoren in die Lage, eine automatische Prüfung der betreffenden iSeries-Server anhand umfangreicher Vorlagen für Konfigurationsrichtlinien durchzuführen und auszuwerten.



Create Date	ASP Group	Library	Object	Object Type	Object Owner	Object Information	SRG File Library	SRG File Name
08/02/06	*SYSBAS	QSYS	QSTW151A	FILE	QSYS	10000044010100000000000000000000		
08/02/06	*SYSBAS	QSYS	QSTW151B	FILE	QSYS	10000044010100000000000000000000		
08/02/06	*SYSBAS	QSYS	QPADE0000	MSGQ	QTCP	Work Status Message Queue		
08/30/06	*SYSBAS	PMB	USERS	FILE	PMB	03 1996-2006 NetIQ Corp., all rights reserved		SRCP
08/30/06	*SYSBAS	PSCSTEM004	RFLTE0C05	FILE	PMB			
08/30/06	*SYSBAS	QUSRQSYS	QPR23072	USRSPC	BDAL	831762QUERENQPR23072		
08/30/06	*SYSBAS	QUSRQSYS	QPR23078	USRSPC	PMB	832078MHPQPR23078		
08/30/06	*SYSBAS	QUSRQSYS	QPR23080	USRSPC	PMB	832080MHPQPR23080		
08/30/06	*SYSBAS	QUSRQSYS	QPR23081	USRSPC	PMB	832081MHPQPR23081		
08/30/06	*SYSBAS	QUSRQSYS	QPR23082	USRSPC	BDAL	832082MHPQPR23082		
08/30/06	*SYSBAS	QSYS	QSTW161AA	FILE	QSYS	10000130200100000000000000000000		
08/40/06	*SYSBAS	APP	SARV1SR	PGM	APP			SAR
08/40/06	*SYSBAS	APP	SARV1SR	MODULE	APP			SAR
08/40/06	*SYSBAS	QUSRQSYS	QPR23071	USRSPC	BDAL	832071MHPQPR23071		
08/40/06	*SYSBAS	QUSRQSYS	QPR23073	USRSPC	BDAL	832073MHPQPR23073		
08/40/06	*SYSBAS	PSADGIT	SARV01C	PGM	PSJOBOWN	03 1996-2006 NetIQ Corp., all rights reserved		
08/40/06	*SYSBAS	QSYS	QPADE0006	DEVQ	QTCP	Device created for ISPTAR.		
08/40/06	*SYSBAS	QSYS	QPADE0007	DEVQ	QTCP	Device created for ISPTAR.		
08/40/06	*SYSBAS	QSYS	QSTW161AA	FILE	QSYS	10000140100100000000000000000000		
08/40/06	*SYSBAS	QSYS	QSTW161BB	FILE	QSYS	10000142100100000000000000000000		
08/40/06	*SYSBAS	QSYS	QPADE0007	MSGQ	QTCP	Work Status Message Queue		
08/40/06	*SYSBAS	QSYS	PSCSTEM004	FILE	QSYS	10000130200100000000000000000000		
08/40/06	ASPI	TEST23	SARV1SR	MODULE	APP			SAR
08/40/06	ASPI	TEST23	SARV1SR	PGM	APP			SAR
08/30/06	*SYSBAS	PSCSTEM006	RFLTE0C05	FILE	APP			
08/30/06	*SYSBAS	PSCSTEM006	RFLTE0C05	FILE	APP			
08/30/06	*SYSBAS	QUSRQSYS	QPR230819	USRSPC	APP	8320819MHPQPR230819		
08/30/06	*SYSBAS	QUSRQSYS	QPR230823	USRSPC	APP	8320823MHPQPR230823		
08/30/06	*SYSBAS	QSYS	QSTW161AA	FILE	QSYS	10000114010100000000000000000000		
08/30/06	*SYSBAS	BDAL	PSCJMSD2	FILE	BDAL	03 1996-2006 NetIQ Corp., all rights reserved		JRM000
08/30/06	*SYSBAS	ED06J	DSPPFDSPFC	PGM	DURANE	Free DSPPFD (Personal Format) Layout ED06C		ED06C

NetIQ Security Solutions for iSeries überzeugt mit detaillierten Prüfungs- und Reporting-Funktionen auf allen iSeries-Plattformen.

**Echtzeitschutz gegen Eindringversuche** – Böswillige Angriffe und Verstöße gegen Sicherheitsrichtlinien werden unverzüglich erkannt und in Echtzeit gemeldet. Die vom System erzeugten Antworten werden an das zentrale Alarm- und Ereignismanagement von NetIQ Security Manager weitergeleitet, um Nutzung, Analyse und Reporting miteinander zu korrelieren.

**Einhaltung der gesetzlichen Bestimmungen an das Log-Managementsystem** – Durch Integration mit NetIQ Security Manager besteht Zugang zu leistungsstarken Analyse- und Reporting-Funktionen, die ein lückenloses Audit durch regelmäßige Prüfung und Dokumentation anhand unternehmensweiter Sicherheitsprotokolle und Ereignisinformationen ermöglichen.

**Synchronisierung von Benutzerprofilen und Kennwörtern** – Für die Synchronisierung der Benutzerprofile und Kennwörter fällt weniger Zeitaufwand an, was einer sicheren und effizienten Benutzerverwaltung über mehrere iSeries-Server zugute kommt. Alte und inaktive Benutzerkonten werden schnell erkannt und archiviert, um die Risiken durch Missbrauch verwaister Konten zu reduzieren.

# NetIQ Security Solutions for IBM iSeries

## Technische Merkmale

### PSAudit™

PSAudit automatisiert und vereinfacht die Erkennung von Sicherheitschwachstellen der iSeries-Plattform anhand leicht verständlicher Berichte, die entweder regelmäßig oder nach Bedarf erstellt werden können.

- Nach Prioritäten gegliederter System Checkup Report zur umgehenden Analyse der Systemintegrität
- Über 200 Berichte zu Änderungen an Betriebssystem, Benutzerprofilen und Objektbefugnissen sowie über Sicherheitsverstöße und die Nutzung von Exit-Points
- Detaillierte Prüfung auf Feld- und Datensatzebene mit der Möglichkeit, Filter für Ausnahmeberichte zu nutzen
- Rückverfolgung und Dokumentation von Benutzeraktivitäten und Systemzugriff, inkl. An- und Abmeldezeiten
- Erstellung einer Sicherheits-Baseline, um Änderungen an Systemwerten, Bibliotheken, Benutzerprofilen, Gerätekonfigurationen, PTFs usw. schnell zu erkennen
- SQL/Query-Auditing zur Einsichtnahme in ausgeführte SQL- und Query-Anweisungen (QRY)
- 

### PSSecure™

Mit PSSecure lässt sich die Sicherheit der iSeries-Server schnell und einfach herstellen.

- "Exit-Point"-Management zur Rückverfolgung, Überwachung und Kontrolle, wem, wann und wie Zugriff auf ein iSeries-System erlaubt wird
- Sichere Delegation und Verwaltung von Rechten über "Privilege Manager".
- Vereinfachte Ressourcenverwaltung (auf Objektebene) und Compliance durch Nutzung von Vorlagen für Objektbefugnisse
- Synchronisation von Profilen und Kennwörtern über mehrere iSeries-Server hinweg

- Deaktivieren und Löschen verwaister Benutzerprofile
- Automatisches Beenden inaktiver Benutzersitzungen
- Erstellen detaillierter Prüfprotokolle von Datenänderungen
- Erstellung sicherer Menüs für neue und vorhandene Anwendungen
- Einfachere Definition von Kennwortrichtlinien zur strikten Durchsetzung der Sicherheitsregeln.

### PSDetect™

PSDetect bietet Schutz in Echtzeit gegen unbefugte Zugriffsversuche oder Sicherheitsverletzungen und warnt bei Problemen, die die Verfügbarkeit und Leistung des Systems beeinträchtigen könnten.

- Überwachung jeder Nachrichtenwarteschlange, inkl. QSYSOPR
- Überwachung zahlreicher Ereignisse, u.a.:
  - Änderungen an Systemwerten und Konfigurationen
  - Speicheralarme (z.B. bei nahezu erschöpfter Plattenkapazität)
  - Ungültige Anmeldeversuche
  - QSECOFR-Profilaktivität
  - Ablehnung von Anfragen zu Remote-Transaktionen (bei Einsatz von Remote Request Management [RRM] zur Absicherung der Exit-Points)
- Mehrere Möglichkeiten der Reaktion oder Benachrichtigung, u.a.:
  - Protokollieren von Ereignissen in PSDetect oder Meldung in NetIQ Security Manager
  - Ausführung eines OS/400- oder i5/OS-Befehls oder -Programms
  - Meldung an Pager, Mobiltelefon oder per E-Mail
  - Absenden von SNMP-Traps, z.B. an NetIQ AppManager®

## Systemvoraussetzungen

- OS/400 V5R1 oder neuer
- 415 MB Speicherkapazität für die Produktbibliotheken für NetIQ Security Solutions for iSeries
- 150 MB freie QTEMP-Speicherkapazität

## Kontakt

### Internationaler Sitz

#### NetIQ, An Attachmate

#### Business

1233 West Loop South

Suite 1800

Houston, TX 77027, USA

713.548.1700

713.548.1771 Fax

888.323.6768 Verkauf

### NetIQ Deutschland GmbH

+49 (0)89 99351-0

infoDE@Netiq.com

www.netiq.de

### NetIQ Schweiz

+41 43399 3090

infoCH@Netiq.com

www.netiq.de

### NetIQ Österreich

+43 15954335

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)

NetIQ, das NetIQ-Zeichen, NetIQ Security Solutions for iSeries, PSAudit, PSDetect, PSSecure, NetIQ Secure Configuration Manager, NetIQ Security Manager und NetIQ AppManager sind Marken oder eingetragene Marken der NetIQ Corporation oder ihrer Tochtergesellschaften in den Vereinigten Staaten oder anderen Gerichtsbarkeiten. Alle sonstigen Firmen- und Produktnamen sind möglicherweise Marken oder eingetragene Marken der jeweiligen Gesellschaften.

© 2008 NetIQ Corporation, alle Rechte vorbehalten.

SS107ISER PS 1908

