Security Solutions for IBM i

The security and availability of your IBM i and iSeries servers is essential to your business. Sensitive information and business-critical files housed on your IBM i servers must be closely monitored—and access to them audited—in order to help ensure that you meet compliance requirements and demonstrate security best practices. Security Solutions for IBM i provide you a simple, integrated, and powerful solution to enhance the security of your IBM i and iSeries servers and improve auditing and reporting of access and events.

Security Solutions for IBM i at a Glance
Protect data and demonstrate compliance by securing and monitoring IBM i and iSeries servers.

Solution

Security Management

Product

Security Solutions for IBM i

Product Overview

While good security is an inherent capability of the IBM i platform, additional protection is needed to maximize its security. With multiple access points to your system, tracking and controlling access to your servers and their business-critical data is more important—and more difficult—than ever. NetIQ Security Solutions for IBM i enable you to more proactively and easily protect your sensitive data and applications, to improve the performance and availability of services run from IBM i platforms, as well as to extend productivity through secure and streamlined user administration.

Capabilities

Security Solutions for IBM i provide:

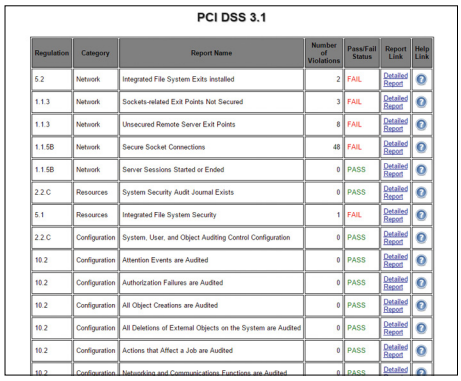
- **Streamlined compliance**—quickly identify and archive obsolete and inactive users, easily produce audit reports, and track privileged user activity to help meet requirements such as the PCI DSS, HIPAA and EU Privacy Directive.
- **Proactive protection for IBM i platforms**—quickly and effectively lock down your OS/400 and i5/OS systems through the application of strong access controls at both the network and object security levels.
- **Security enforcement through time-based privileged management**—implement the least-privilege model to reduce risk and protect sensitive data.
- **Real-time intrusion protection**—respond to both attacks and policy violations with real-time intrusion protection.
- **Simplified user administration**—reduce the time spent synchronizing user profiles and passwords with secure user administration across multiple servers.
- **Simplified reporting on compliance with policies and standards**—allow security analysts and auditors to automatically evaluate and report on your servers with NetIQ Secure Configuration Manager templates.

Features

Security Solutions for IBM i provide extensive and powerful auditing and security capabilities to streamline compliance reporting and reduce the risk to sensitive data. Key features include:

- Easy-to-understand reports that are run on a scheduled basis or on demand, automating and simplifying the process of identifying security vulnerabilities.
- Secure, time-based delegation and management of privileges through Privilege Manager.
- Scored System Checkup Report to quickly analyze your system's health.
- More than 200 reports on changes to the operating system, user profiles, security violations, exit points, and object authority changes.

- Detailed field and record-level auditing, with the ability to use filters for exception reporting.
- Tracking and documentation of user activities and access to systems, including sign-on and sign-off times.
- Establishment of a security baseline to quickly identify changes to system values, libraries, user profiles, device configurations, PTFs and more.
- “Exit point” management to track, monitor and control who, when and how access is allowed to your systems.
- Object authority templates to simplify resource (object-level) management and compliance.
- Synchronization of profiles and passwords across multiple IBM i servers.



PCI DSS 3.1

Regulation	Category	Report Name	Number of Violations	Pass/Fail Status	Report Link	Help Link
5.2	Network	Integrated File System Exits Installed	2	FAIL	Detailed Report	
1.1.3	Network	Sockets-related Exit Points Not Secured	3	FAIL	Detailed Report	
1.1.3	Network	Unsecured Remote Server Exit Points	8	FAIL	Detailed Report	
1.1.5B	Network	Secure Socket Connections	48	FAIL	Detailed Report	
1.1.5B	Network	Server Sessions Started or Ended	0	PASS	Detailed Report	
2.2.C	Resources	System Security Audit Journal Exists	0	PASS	Detailed Report	
5.1	Resources	Integrated File System Security	1	FAIL	Detailed Report	
2.2.C	Configuration	System, User, and Object Auditing Control Configuration	0	PASS	Detailed Report	
10.2	Configuration	Attention Events are Audited	0	PASS	Detailed Report	
10.2	Configuration	Authorization Failures are Audited	0	PASS	Detailed Report	
10.2	Configuration	All Object Creations are Audited	0	PASS	Detailed Report	
10.2	Configuration	All Deletions of External Objects on the System are Audited	0	PASS	Detailed Report	
10.2	Configuration	Actions that Affect a Job are Audited	0	PASS	Detailed Report	
10.2	Configuration	Networking and Communications Functions are Audited	0	PASS	Detailed Report	

Figure 1. Security Solutions for IBM i systems reduce risk to critical data and improve compliance reporting.

- Disabling or deletion of unused user profiles and ability to automatically terminate inactive user sessions.
- Detailed audit log of file alterations.
- Simplified password policy definitions, and assurance of their continual enforcement.
- Real-time protection against unauthorized access attempts or policy violations.
- Monitoring of any Message Queue, including QSYSOPR.
- Field level database file change auditing, which can save hundreds of hours of tracking and documenting critical and sensitive database file updates.

Key Differentiators

Your IBM i systems represent the heart of your business, and NetIQ solutions can help provide you the ability to close existing security gaps and clearly demonstrate to your auditors that you are meeting policy and compliance goals.

- Security Solutions for IBMi provide highly granular and tunable controls to reduce unnecessary privilege and access for users or systems, helping meet compliance mandates and reducing the risk to your sensitive information and business-critical applications.
- NetIQ is the only vendor that provides security reporting, auditing, and monitoring across the entire IBM i and Power Systems platforms—including i5/OS (OS/400), AIX, Linux and Microsoft Windows. Only NetIQ can help you protect the critical data and applications on these important platforms.
- The solutions are also integrated with NetIQ enterprise security solutions to provide comprehensive event correlation and reporting across heterogeneous platforms, as well as configuration assessment and reporting to help ensure complete coverage and the ability to respond to threats to data—wherever it resides.

About NetIQ

NetIQ provides security solutions that help organizations with workforce and consumer identity and access management at enterprise-scale. By providing secure access, effective governance, scalable automation, and actionable insight, NetIQ customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the NetIQ homepage at **www.cyberres.com/netiq** to learn more. Watch video demos on our NetIQ Unplugged YouTube channel at **www.youtube.com/c/NetIQUnplugged**.

NetIQ is part of CyberRes, a Micro Focus line of business.

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes
A Micro Focus Line of Business