NetIQ® Secure Configuration Manager

Demonstrate compliance and protect sensitive assets from internal and external attack with automated configuration assessment of critical systems in accordance with regulatory requirements and security policies.

SOLUTION
Security Management

PRODUCT
NetIQ® Secure Configuration Manager™

NetIQ Secure Configuration Manager helps you to enforce compliance with evolving security regulations and internal policies.

Introduction

Your organization faces increased security risks and compliance challenges when it loses visibility and control of sensitive data due to evolving and complex threat and regulatory environments. NetIQ® Secure Configuration Manager™ helps to protect sensitive data by enabling you to enforce security policy across critical systems. The solution proactively assesses system configurations in light of regulatory requirements and your organization's security policies, alerting teams to instances in which system configurations drift from policy, helping them to remediate misconfigurations before they result in security breaches or failed audits.

Product Overview

NetIQ Secure Configuration Manager is an award-winning security configuration assessment and compliance monitoring solution. The automated solution helps security teams build a continuous process for identifying and alerting on instances in which critical system configurations drift from policy. Intuitive reporting gives teams the security information they need to rapidly identify and remediate poor configurations before real damage can occur. By delivering configuration and vulnerability assessments, user entitlement reporting, baselining and delta reporting, a security and compliance dashboard, and exception management, Secure Configuration Manager enables you to demonstrate compliance with organizational policies and manage information security risk.

Capabilities

NetIQ Secure Configuration Manager provides the comprehensive configuration assessment and reporting capabilities necessary for compliance with the Sarbanes Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Federal Information Security Management Act (FISMA), North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) and more. Extensive automation for assessment and reporting not only reduces the strain on IT resources but also helps ensure that critical systems routinely meet compliance standards. NetIQ Secure Configuration Manager helps organizations meet their security and compliance goals by delivering:

- **Configuration assessment** – provides customizable policy templates that align with regulations and standards; audits system configurations and compares them against best practices; and reports on total and managed risk.

- **Vulnerability assessment** – identifies host flaws by assessing them against security intelligence delivered by an automated service and reports on the frequency and location of vulnerabilities.

- **User entitlement reporting** – assesses user permissions for access to critical information, providing answers to your questions about who has access to what level of critical information.

- **Baselining and delta reporting** – reports changes to system and user configurations; highlights instances in which configurations drift from policy; provides the security information your team needs to quickly remediate poor configurations.

- **Security and Compliance Dashboard** – displays security and compliance posture quickly and intuitively, meeting the needs of multiple stakeholders while enabling improved decision making.

- **Business exception management** – ensures that the risk from excluded systems or checks is properly understood, managed and documented by security teams.

Features

We've designed NetIQ Secure Configuration Manager to protect sensitive data and avoid non-compliance with corporate and regulatory policies. Key features include:

- Out-of-the-box compliance and best practices knowledge to simplify the process of setting appropriate system configurations.

- Broad platform and application support, including Microsoft Windows, UNIX, Linux, IBM iSeries and System i, Oracle, and Microsoft SQL Server and Internet Information Services (IIS). Expanded support for network devices from Cisco Systems and Juniper Networks.

- Automated delivery of the latest vulnerability, threat and patch information.

- Report scheduling to automate when and how often NetIQ Secure Configuration Manager performs assessments.

- Agent or agentless operating system, database and application assessments.

- Flexible asset-importance weighting and comprehensive risk scoring.

The Security and Compliance Dashboard delivers greater risk visibility to senior stakeholders, helping them make faster, better informed business-risk decisions.

- Built-in exception management capabilities to manage information security risks associated with known exceptions.

- Security Content Automation Protocol (SCAP) validation to ensure your compliance assessment solution is in compliance with federal requirements.

- Integration with IT GRC solutions using the UCF*interchange* to ensure a common language helps teams provide automated, continuous monitoring and reporting to key stakeholders.

Key Differentiators

- **Out-of-the-box security intelligence** – Keep content on regulations, standards and security vulnerabilities relevant and up-to-date with Autosync, an automated security content update service within

NetIQ Secure Configuration Manager. You can download new information and automatically turn it into policy checks. A wizard-based system can help you create new or modify existing policies to help you make the most of the IT resources you have.

- **Broad cross-platform support** – NetIQ Secure Configuration Manager provides support for heterogeneous environments that include multiple servers, network devices, operating systems and applications. This enables a comprehensive view of your entire IT infrastructure's security and compliance posture.

- **Superior reporting and risk management** – NetIQ Secure Configuration Manager has powerful reporting capabilities that allow you to schedule proactive configuration assessments and use a comprehensive risk scoring methodology to help prioritize potential vulnerabilities within your IT

When stakeholders say "show me," you can. Our solution streamlines risk and compliance reporting, enabling you to proactively produce assessments that prove you are working with the business to mitigate risks.

NetIQ.

infrastructure. Integration with IT GRC platforms further enhances your ability to continuously and efficiently monitor and report on information security risk and compliance within your infrastructure. With this security knowledge in hand, your security team can take immediate action before a security breach or compliance gap occurs.

- **Identity-Powered Security** – NetIQ Secure Configuration Manager is part of a security management solution that, when integrated with identity information from identity and access management solutions, gives security teams the ability to identify user activity that is abnormal or not business-appropriate. The additional "identity context" provided by identity and access management solutions transforms typical security monitoring

data into truly actionable security intelligence that teams can use to detect and address threats, before damage is done. NetIQ calls this approach to information protection, Identity-Powered Security. As part of this approach, Secure Configuration Manager provides the ability to assess user permissions for access to critical information, offers answers to "who" has access and "what" is their level of access to critical information, helps teams to maintain up-to-date access privileges, and assists security professionals in demonstrating compliance to security regulations, policies, and best practices.

To learn more about NetIQ Secure Configuration Manager, or to start a trial, go to **www.netiq.com/scm.**