Using NetIQ Secure Configuration Manager for Unix Assessments

January 2007

Contents

A 'Unified Compliance' Approach................................ 3

Implementing Unified Compliance with NetIQ 5

Support for Enterprise-Level Compliance & Risk Management........................... 7

Meeting Compliance Requirements on Unix Systems with NetIQ Secure Configuration Manager 9

NetIQ Brings Compliance Solutions to Customers 12

About NetIQ......................... 14

NetIQ Secure Configuration Manager helps you protect your IT infrastructure and meet compliance requirements in the IT controls areas of entitlement reporting and segregation of duties. This holds across many different platforms, none more important than Unix and Linux.

With NetIQ Secure Configuration Manager, companies can implement and manage controls, which make compliance programs sustainable and repeatable, while gaining visibility into sources of vulnerability and risk exposure on Unix systems.

NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense [DOD] acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, Provider-1, SiteManager-1, and VPN-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveReporting, ADcheck, AppAnalyzer, AppManager, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, IntelliPolicy, Knowing is Everything, Knowledge Scripts, Mission Critical Software for E-Business, MP3check, NetConnect, NetIQ, the NetIQ logo, NetIQ Change Administrator, NetIQ Change Guardian, NetIQ Compliance Suite, NetIQ Group Policy Administrator, NetIQ Group Policy Guardian, NetIQ Group Policy Suite, the NetIQ Partner Network design, NetIQ Patch Manager, NetIQ Risk and Compliance Center, NetIQ Secure Configuration Manager, NetIQ Security Administration Suite, NetIQ Security Analyzer, NetIQ Security Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Server Consolidator, VigilEnt, Vivinet, Work Smarter, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

A ‘Unified Compliance’ Approach

There are several information security control frameworks available to help you get started in creating IT controls for assessment and reporting to meet compliance requirements: ISO17799 from the International Standards Organization in Europe, CobiT from the Information Systems Assurance and Control Association (ISACA) and the IT Infrastructure Library.

However, because these are attempts at universal control sets for organizations of all sizes, locations, and industries, it will still be necessary to customize to meet your unique needs. The major challenges that customers face in these efforts include those listed in the following sections.

Breaking Down Regulations into Standards and Best Practices

Most regulations today provide general overviews without providing detailed instructions on requirements and checklists. For example, the Gramm-Leach-Bliley Act states that financial institutions must ensure the confidentiality and integrity of consumer information, but provides no specifics on how to achieve this. Customers need solutions that break down regulations into standards, best practices, and policies. Administrators look for guidelines and best practices that add bulk and definition to vague regulation requirements.

The frameworks mentioned above can provide assistance in this area, as well as guidance provided by regulatory agencies, industry associations, and consultants. To drill down even further and provide specific guidance on recommended system configurations, organizations such as Center for Internet Security (CIS) and National Institute of Science and Technology’s Computer Security Resource Center (NIST CSRC) provide more detail.

Automating the Compliance Process to Make it Sustainable

Organizations have spent huge amounts of money in meeting initial compliance requirements for Sarbanes-Oxley and other regulations. In order to make the whole compliance process repeatable and sustainable, companies need solutions that can automate IT control areas that when performed manually are time-consuming and error-prone.

Implementing, Managing, and Documenting Controls

A compliance architecture supports the integration of controls into an organization by centralizing many IT controls and using technology to help enforce process controls. While there are areas of commonality across various standards and guidelines, the major controls can be grouped under three main categories.

Organizational Controls

Organizational controls can be thought of as *activities* such as budget processes, business strategy, organization charts, legal processes, and policies and procedures. These controls are part of the structure of the entire organization, not just part of IT and are often explicitly required by the regulations.

Management Controls

Management controls can be thought of as security *processes* such as risk assessment, continuity planning, incident response, and auditing/compliance reporting. They are more specific to IT than Organizational Controls, but apply to the governance of the entire IT environment. Most IT regulations will specify at least some of these controls.

Technical Controls

Technical controls can be thought of as specific IT procedures that ensure an organization’s information is secure. They are very specific to the world of IT and often require specialized training to perform. Rarely are technical controls explicit within a regulation – organizations and practitioners usually are left to interpret what procedures to implement to achieve compliance. Examples of technical controls include encryption levels and key management, audit log management, identification and authentication, service level agreements, change control, intrusion detection, antivirus, and many others.

Implementing Unified Compliance with NetIQ

IT compliance programs cover disciplines ranging from physical security to HR processes, and from system continuity planning to identification and authentication. Most information security controls frameworks have somewhere between 8 and 12 distinct domains, with some as high as 32. These domains can break down in to hundreds of controls – an impossible range of coverage for any one vendor. Indeed, many of the controls are process-oriented, requiring no additional technology. However, some controls are extremely labor-intensive, and almost impossible to perform manually. NetIQ offers the broadest range of automated compliance solutions. Some specific examples of controls we can help you implement and automate are explored below:

Policy Management

It is important that all areas have documented policies and procedures. In addition, organizations need to ensure that policies are approved by management, and communicated to appropriate employees. And for the auditors and lawyers, you need to be able to prove that employees received and understood the policies and procedures that apply to them.

With NetIQ VigilEnt Policy Center, organizations can easily document and distribute policies and procedures through your intranet. More than 1,400 security policies and standards will help you create new or update existing policies In addition, tracking and reporting ensures that the required individuals have reviewed and approved the documentation. Finally, electronic signatures and quizzes ensure that employees have been properly trained.

IT Compliance Reporting

It is not enough to perform all of these activities, processes, and procedures, of course. You must also coherently report your results to management, internal and external auditors, and other applicable third parties. At the highest levels, management will want to know simply, “Are we in compliance”? Yet, of course, others will want more detail about compliance levels for particular sections of the regulation or compliance across different regulations. This is where the concept of unified compliance becomes critical in building and sustaining a cost-effective compliance program.

The NetIQ Risk and Compliance Center solution aligns security metrics gathered from your IT systems to demonstrate compliance with one or more IT-related policies and regulations. It displays those metrics in a powerful yet easy-to-understand, web-based dashboard for compliance management. This solution also analyzes IT risk factors such as compliance exceptions and vulnerabilities across the key areas of your business.

Segregation of Duties

IT managers need to meet a key regulation that requires the separation of job functions to ensure that no one can commit and cover up fraud or a security breach. For example, it is important to establish checks and balances that would deter a person from designating himself or herself as the signing authority when generating a purchase order.

With NetIQ products, IT managers can segregate key functions such as configuration management, configuration policy setting, system auditing, and vulnerability assessment. NetIQ can help ensure that users and administrators have only the privileges they need to do their jobs. Administrators can segregate the duties of configuration assessment, policy writing, compliance reporting, and remediation by performing these tasks within NetIQ Secure Configuration Manager and relying on its granular access control.

Log Management

All IT regulations mandate directly or indirectly the collection, review, and storage of audit logs to have a record of system events, user activities, and transaction processing. Log consolidation and analysis is a must in today's regulated, litigated, risky world.

By consolidating and analyzing event logs to a central repository**,** administrators can ease the burdens associated with log management across heterogeneous environments. NetIQ solutions ensure that proper audit log settings are enabled throughout. With NetIQ Secure Configuration Manager, IT managers can schedule regular assessments to check that the appropriate audit log settings are enabled across all major server platforms in one report, and automatically distribute the report to the appropriate individuals.

Entitlement Reporting

IT organizations have controls on entitlement reports, which are lists of who has access to what resources. These reports are extremely difficult and time-consuming to produce manually. In addition, most organizations don't have an up-to-date repository of personnel reporting structures that can be used in an automated way.

By automating key functions with NetIQ solutions, IT managers can easily manage entitlement reports and electronically distribute them to management, and disable stale and suspicious accounts. NetIQ solutions enable customers to regularly review users with advanced privileges across all systems in a single report. With NetIQ Secure Configuration Manager, IT organizations get a single report of administrator accounts across UNIX, Linux and Oracle databases, as well as other leading platforms.

Change Control

IT organizations are required to record and manage all the changes to a computing and business environment. While most organizations are at least documenting and routing change requests through a Help Desk ticketing system, they usually limit their definition to software and hardware upgrades. Often not part of the formal change control process are important sections like Group Policies, User Access Privileges, and Configuration Settings.

NetIQ Change Control & Audit solutions assure that you can authorize, verify, audit and monitor changes across your IT environments. Through an automated approach, IT change management processes are reinforced with the knowledge and confidence that only authorized and intended changes have been implemented. With support for best practices, such as ITIL and CobiT, NetIQ Change Control & Audit solutions enable you to more easily comply with leading regulations such as Sarbanes-Oxley and HIPAA.

NetIQ Security Solutions enable managers to monitor for configuration changes and unauthorized access attempts. NetIQ Secure Configuration Manager allows IT organizations to regularly run reports on system configurations. The solution performs a vulnerability assessment and policy scan on a system before it is placed into production, and schedules regular scans to detect unauthorized changes. This can be linked to NetIQ Security Manager for real-time alerting on system changes or to monitor certain files for unauthorized changes.

Support for Enterprise-Level Compliance & Risk Management

The NetIQ Secure Configuration Manager solution provides the features and support for an enterprise-level compliance program.

Risk and Compliance Metrics

NetIQ Secure Configuration Manager performs assessments using either out-of-the-box or custom policy checks. In doing so, it returns detailed information about the compliance of a given asset (e.g., server) to the technical policy (or baseline) of an organization. These reports provide ample detail to enable an administrator to bring the system back into compliance or to remediate a vulnerability. Specifically, it provides detailed reports on policy exceptions such as which accounts violate a given policy check or which patches have not been applied. It also provides instructions for remediation, often including highly detailed instructions from a security intelligence service called IntelliShield.

However, those details provide little value at the enterprise-level. At that level, metrics are paramount. Without proper high-level metrics, it is virtually impossible to manage an organization’s compliance and perform effective risk management. Fortunately, these metrics are provided by NetIQ Secure Configuration Manager.

NetIQ Secure Configuration Manager grades the technical compliance of systems using a risk-weighted score. The score is a factor of the number of policy exceptions, vulnerabilities and exploits discovered during assessments as well as the importance of the asset to the business. Different checks may be scored differently, depending on the needs of the organization. Also, different assets are prioritized in the scored results according to their business value; two servers with the same policy exceptions and vulnerabilities, for example, score differently depending on their business value.

These scores are summarized for each assessment and further broken down by group (e.g., business unit, geography) and by platform (e.g., Windows vs. UNIX). These quickly highlight areas of concern, making it easier for compliance and risk management professionals to focus their efforts.

Broad Platform and Application Support

While systems administrators often look for “best of breed” tools for homogeneous environments, security officers and compliance personnel are generally responsible for ensuring the security of a broad list of technologies and platforms. Consequently, NetIQ offers the broadest coverage of vulnerability and configuration management solutions on the market.

For starters, NetIQ Secure Configuration Manager supports numerous distinct operating systems, covering everything from enterprise class servers, clusters and midrange platforms to critical workstations. Specifically, NetIQ Secure Configuration Manager helps secure and manage the following platforms:

Windows Platforms	**Unix Platforms**
Windows 2000 Professional	Sun Solaris 7, 8, 9, 10
Windows XP Professional	HP-UX 11.00, 11i, 11i v2
Windows Server 2003	IBM-AIX 4.3.3, 5.1, 5.2, 5.3
Windows Domains	Compaq Tru64 UNIX 4.0f & HP Tru64 5.1b
Active Directory	Silicon Graphics IRIX 6.5.x
Microsoft SQL Server 2000	Oracle 9i, 10g
Internet Information Services 5.0, 5.1, 6.0	Sybase Adaptive Server Enterprise (ASE) 11.5 - 11.92
	Sybase System 11 - 11.92
Linux Platforms	**iSeries Platforms**
Red Hat AS/ES 2.1, 3.0, 4.0	OS/400 V5R2 and later
SuSE Linux Enterprise Server 8.0 on POWER (including iSeries)	i5/OS
SuSE Linux Enterprise Server 8, 9	SuSE Linux Enterprise Server 8.0 on POWER
	IBM-AIX 4.3.3, 5.1, and 5.2

Meeting Compliance Requirements on Unix Systems with NetIQ Secure Configuration Manager

Specific to the controls areas of entitlement reporting and segregation of duties, NetIQ has built-in knowledge to help you audit your Unix servers to ensure implementation and automation for best practices such as developing and enforcing secure passwords, ensuring appropriate privilege on Unix hosts, enforcing secure logins on Unix hosts and enforcing consistent Unix file and directory permissions.

Developing and Enforcing Secure Passwords

Because passwords help control who can access what, password security is the cornerstone of your security structure. You should ensure passwords cannot be cracked through brute force attacks on individual host computers or through inappropriate access to sensitive data and system files. Securing passwords involves developing and enforcing password complexity, encryption and policy.

Secure Configuration Manager provides several reports and security checks to help you audit password security and identify weak passwords. For example, if a security check discovers a password-related vulnerability, you can take the appropriate action, such as changing the root password. The following Unix reports and security checks in Secure Configuration Manager can help you assess and enforce password policy.

Reports	***Security Checks***
Active Users	Accounts with password length problems
Detect Changes to Root	Accounts with weak passwords
Password Lifetimes	Accounts without a password
User Records with Unmatched Password File Entry	Accounts where the user name is also the password
Users with Duplicate UIDs	NIS is active
Users with Duplicate Name in Password File	Protected password database check

Ensuring Appropriate Privilege on Unix Hosts

To ensure appropriate privilege on your Unix computers, you must secure super user (root) and other privileged accounts. Secure Configuration Manager provides multiple reports and security checks to help you audit privilege and identify inappropriate access, such as those shown below.

Reports	***Security Checks***
Detect Changes to Root	Last access date for accounts
Groups with GID=0	Powerful group accounts
Guest and Command Accounts	Powerful user accounts
Root Login Activity	Privileged group accounts
Users with UID=0	Privileged user and pseudo-user accounts
Users with Duplicate UIDs in the Password File	Switch user to root command statistics

Enforcing Secure Logins on Unix Hosts

Establishing and enforcing secure logins ensures your Unix host computers and resources are protected against malicious attacks, and demonstrate effective segregations have been established. For example, you can protect remote hosts by avoiding login configurations that bypass authentication such as **r** commands (**rlogin, rsh**) that provide open access to explicitly trusted systems.

Secure Configuration Manager provides multiple reports and security checks to help you audit logins and identify inappropriate access, including those below.

Reports	***Security Checks***
All User Profile Information	Contents and permissions of ~/.rhosts
Startup Profile Files	Default inactive login timeouts
User Logon Shell File Ownership	Dormant user accounts
Users Home .rhosts Problems	Login failures

Enforcing Consistent Unix File and Directory Permissions

Enforcing consistent Unix file and directory permissions help you establish and enforce permissions standards across your company. Secure Configuration Manager provides multiple reports and security checks to help you audit file system permissions and identify inappropriate access such as those below.

Reports	***Security Checks***
Directories with Uneven Privileges	Files and directories without ownership
Files with Uneven Privileges	File ownership verification
Files Which are SUID/SGID and World Writeable	Inadequate umask values
Mounted File Systems	System files with non-root ownership
Startup Files that are World Writeable	World writeable directories that are not sticky

NetIQ Brings Compliance Solutions to Customers

The use case scenarios listed below are just a few examples of how organizations are using NetIQ Secure Configuration Manager (SCM) to meet ongoing compliance and risk management requirements for various regulations across different industries.

Financial Services

Secure Configuration Manager helps organizations in the financial services industry comply with the following:

- FFIEC Examination Handbook, Information Security Booklet (December 2002, p.7): "Financial institutions must maintain an ongoing information security risk assessment program that effectively ... prioritizes the risks present due to threats and vulnerabilities."
- PCI Data Security Standard (12.1.2): "Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment."

For example, an international bank purchased Secure Configuration Manager. This bank aimed to displace several incumbent products (network-based vulnerability scanning and file auditing products). The key business driver was compliance reporting for Sarbanes-Oxley, and NetIQ's capabilities in the areas of delta reporting and host vulnerability assessment were critical to the customer.

Health Care

Secure Configuration Manager helps health care companies with the following requirements:

- HIPAA Security Rule (164.308(a)(1)): "Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities."
- CMS Information Security Acceptable Risk Safeguards (p.18): "Document the risk and safeguards of the system according to the CMS Information Security RA Methodology."
- PCI Data Security Standard (12.1.2): "Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment."

At a health care organization based in North America, NetIQ replaced products from two competing vendors with Secure Configuration Manager and Security Manager (SM). The key driver for SCM was compliance reporting. The fact that we were able to generate the audit reports they needed (last physical log-on, acceptable usage, and entitlements) figured greatly into their decision. Also the fact that NetIQ can integrate SCM into SM, then into AppManager (for viewing all events) was an enormous plus for this organization.

Federal Government

Secure Configuration Manager helps federal organizations meet the following FISMA-related control recommendations:

NIST 800-53: Page 86: “The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.”

In a recent purchase decision, Secure Configuration Manager was selected by an agency of the U.S. Department of Commerce to comply with FISMA regulations. FISMA compliance is tied closely to the NIST 800-53 risk management framework, and the fact that SCM has policy templates corresponding to NIST guidelines helped the customer immensely with their auditing needs.

Retail

Risk management programs help companies comply while focusing resources on what's important. SCM can help by:

- Providing metrics based not only on vulnerabilities but also compliance exceptions, weighed according to their business value.
- Highlighting which systems represent the highest business risks and show them where to focus remediation efforts.

A manufacturing/retail corporation selected Secure Configuration Manager to help prepare for an upcoming audit. There were several features of SCM that made the difference in the company’s final selection. These included custom checks, the audit-by-proxy feature, database auditing, and the ability to run templates across multiple platforms.

About NetIQ

NetIQ is a leading provider of integrated systems and security management solutions. Our compelling, best-of-breed solutions for Performance & Availability Management, Security Management, Configuration & Secure Configuration Management, and Operational Change Control empower IT organizations and ensure operational integrity, better managed services and risk, and policy compliance. With a history of innovation and leadership, NetIQ provides a broad range of easy-to-deploy cross-platform products.

NetIQ counts more than 3,000 of the world’s leading enterprises as key customers. In addition, our partnerships with industry leaders such as Microsoft, IBM, HP, and Dell give NetIQ a unique advantage in the global marketplace. With customer-proven solutions and strong relationships, NetIQ delivers the tools you need to reduce your risk and deliver value from day 1.

In June 2006, NetIQ Corporation joined the Attachmate family of companies. Attachmate, owned by an investment group led by Francisco Partners, Golden Gate Capital and Thoma Cressey Equity Partners, enables IT organizations to extend mission critical services and assures they are managed, secure, and compliant. Our goal is to empower IT organizations to deliver trusted applications, manage service levels, and ensure compliance by leveraging knowledge, automation and secured connectivity.

For more information about:

- ☑ Attachmate, visit http://www.attachmate.com
- ☑ NetIQ, visit http://www.netiq.com