



Proactive Security Policy Enforcement: A Practical Approach

September 2003

Contents

| | |
|---|----------|
| Why Enforcing Security Policy Is Critical | 1 |
| Policy Enforcement Challenges | 2 |
| Proactive Enforcement via Policy Management Lifecycle4 | |
| NetIQ Proactive Policy Enforcement Solutions | 5 |
| Key Policy Enforcement Advantages | 8 |
| Conclusion | 9 |

Battling a constant barrage of worms, viruses and attacks on enterprise systems, IT and security administrators are seeking more efficient and effective ways to protect information assets. Worm-weary security professionals seem to be constantly reacting to the latest assault on vulnerable systems, “putting out fires” on a weekly basis.

A proactive approach to security policy and compliance offers a more effective means of managing these challenges. By understanding the Policy Enforcement Lifecycle and implementing configuration standards, acceptable use policies, and information classification and handling procedures, enterprises can significantly reduce their risk and their workload.

This White Paper explains why policy enforcement is so important, how to manage the process, and how to apply solutions from NetIQ to help implement a proactive and practical approach to enterprise security policy compliance.

Besides reviewing the information in this paper, NetIQ encourages you to visit our website at www.netiq.com for more details.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, 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.

© 1995-2003 NetIQ Corporation, all rights reserved.

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

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveKnowledge, ActiveReporting, ADcheck, AppAnalyzer, Application Scanner, AppManager, AuditTrack, AutoSync, Chariot, ClusterTrends, CommerceTrends, Configuration Assessor, ConfigurationManager, the cube logo design, DBTrends, DiagnosticManager, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, End2End, Exchange Administrator, Exchange Migrator, Extended Management Pack, FastTrends, File Security Administrator, Firewall Appliance Analyzer, Firewall Reporting Center, Firewall Suite, Ganymede, the Ganymede logo, Ganymede Software, Group Policy Administrator, Intergreat, Knowledge Scripts, Migrate.Monitor.Manage, Mission Critical Software, Mission Critical Software for E-Business, the Mission Critical Software logo, MP3check, NetIQ, the NetIQ logo, the NetIQ Partner Network design, NetWare Migrator, OnePoint, the OnePoint logo, Operations Manager, PentaSafe, PSAudit, PSDetect, PSPasswordManager, PSSecure, Qcheck, RecoveryManager, Security Analyzer, Security Manager, Server Consolidator, SQLcheck, VigilEnt, Visitor Mean Business, Vivinet, W logo, WebTrends, WebTrends Analysis Suite, WebTrends for Content Management Systems, WebTrends Intelligence Suite, WebTrends Live, WebTrends Log Analyzer, WebTrends Network, WebTrends OLAP Manager, WebTrends Report Designer, WebTrends Reporting Center, WebTrends Warehouse, Work Smarter, WWWorld, 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.

Why Enforcing Security Policy Is Critical

Virtually every organization is subject to policies of one form or another and must enforce those policies. Yet far too many policies tend to be expressed in a voluminous printed binder that gathers dust on a shelf rather than guide daily practice and workplace behavior. Security policies are no exception.

Organizations today, however, are recognizing that enforcing security policies is no longer an option but a critical component for managing productivity, protecting one's image and assets, and minimizing liability. Several trends are driving this recognition.

- ❑ **Growth of Incidents:** The sophistication and cost of security incidents from worms, viruses and attacks (both inside and outside the organization) continue to escalate. The latest version of the SoBig virus, for example, hit the Internet August 18, 2003 and created more than a million copies of itself in 24 hours. In addition, normal human and organizational behavior often exposes organizations to risks. Workers often act in ways that put their organizations at risk without even being aware of the consequences. Improper use of corporate technologies exposes the company to harassment-related lawsuits, accidental discloses private or sensitive information, increases vulnerabilities, and reduces productivity.
- ❑ **Regulatory Compliance:** Regulations and standards in many industries require compliance with and enforcement of information security policies. Examples include Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability & Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), Sarbanes-Oxley, European Communities (Data Protection) Regulations, and EU Privacy Directive. Penalties for non-compliance can be severe. A mistaken placement of email addresses among Prozac users by Eli Lilly Company, for example, generated nationwide negative press and triggered an FTC investigation. Under Sarbanes-Oxley, a corporate officer can be fined up to \$1 million and/or face 10 years in prison for signing a false financial report.
- ❑ **Audit Scrutiny:** IT audits and other audits of internal controls typically highlight deviations from corporate policies, regulations, and industry best practices. Lack of critical security policies is often an audit finding as well. Many different types of auditors conduct audits: internal auditors, independent financial statement auditors (who review internal controls), regulators (e.g., OCC, FDIC, FDA, etc.), and customers and business partners (who rely on the organization's controls). IT managers and security officers are very sensitive to audit issues and tend to seek immediate resolution to audit findings.

Moreover, it is no longer viewed as acceptable to simply have policies. For example, one large energy company recently lost a multi-million harassment-related lawsuit. The cause of the suit stemmed from inappropriate e-mail (a joke). While the company had a policy against offensive workplace behavior, including e-mails, it was argued that because the company had not routinely *educated* employees on that policy and had not *enforced* the policy the company had not taken reasonable measures to prevent a hostile work environment.

Independent of the drivers behind policy enforcement, most security professionals recognize that policy enforcement is simply good business since sound policies often encourage efficiency and help reduce risk.

Policy Enforcement Challenges

Organizations commonly treat policy enforcement as a project rather than an ongoing business process. For example, an organization may review and develop policies once every few years, launch a security awareness campaign once a year, conduct sexual harassment policy training every year, and perform a security audit every six months. Treating security policy and compliance as a series of projects can be very inefficient – like balancing your checkbook every six months. It is much more time-consuming than enforcing security policies as a routine way of doing business.

To make policy management an ongoing process that is practical and effective, policy enforcement should be automated, repeatable and measurable. To do so, organizations must overcome hurdles related to the establishment of metrics, organization of security resources, limitations of existing technologies, sheer scale of the enterprise and scarcity of required expertise.

Metrics

Most managers understand that “you can’t manage what you don’t measure.” Security policies are often difficult to enforce because organizations rarely generate metrics for policy compliance. Key security policy metrics must include:

- ☑ **Policy awareness:** Most organizations are unable to tell the degree to which workers know their security policies. In fact, many treat it like advertising, with little ability to tell how effective security training is. Metrics should include the percentage of workers that have signed compliance statements for key policies within the last year and quiz results based on key policies and security topics.
- ☑ **Technical compliance:** Organizations often lack metrics on how well their mission critical technologies (e.g., operating systems, databases, and web servers) comply with policies and standards regarding security configuration and patch levels. Metrics should illustrate compliance levels of key technologies based on risk.
- ☑ **User compliance:** Organizations rarely can tell how many workers have agreed to abide by policies or how well they abide by key policies such as acceptable use policies and information classification and handling policies. Metrics should include the number of times acceptable use policies for e-mail and web are being violated or violations are attempted.

Only with the right metrics can security officers quickly hone in on critical problems and spend resources where they have the greatest benefit.

Organization

In many cases, organizations also create a policy compliance group as part of the internal audit and/or information security team. Unfortunately, these groups often do not include participants at the business unit level or in the IT department to ensure enforcement of security policies. While a central compliance group is generally recommended, it should develop and specify procedures for administrators to use in implementing and enforcing policies.

Policy enforcement processes should also be integrated with other business processes to ensure consistent and continuous application of policies. For example, technical compliance procedures should feed change management procedures to make sure policies adapt to reflect a changing business environment.

Technology

Because many fundamental technologies such as operating systems, databases and web servers are not designed to adequately *enforce* key security policies, it is essential that technology issues be addressed through:

- ☑ **Acceptable use restrictions:** Users should be prevented from browsing illicit web sites, downloading or uploading inappropriate files, and engaging in other dangerous web and instant messenger activities.
- ☑ **Information classification controls:** Users should be prohibited from sending sensitive or classified materials, such as those labeled “Company Confidential,” outside the company via e-mail or instant messenger.
- ☑ **System configuration:** Organizations should be able to determine which systems are out of compliance with their official security policies and standards and take action to correct exposures.

Only by implementing procedures and tools for enforcing policies through technology can an organization effectively and efficiently protect itself.

Large Enterprise Environments

Larger enterprises with diverse, highly complex and distributed systems face special enforcement challenges such as:

- ☑ **Large, complex networks:** Large enterprise may manage thousands of systems distributed around the globe. Naturally, the size and distribution of the network has a direct impact on the ability to enforce policy. Systems are often very difficult to access and review due to their physical location and/or network access controls (e.g., firewall rules).
- ☑ **Large numbers of workers:** Large organizations may have thousands or even tens of thousands of workers, including full-time employees, consultants, contractors and vendors. This makes it very difficult to ensure every employee has read the policies, standards and understands those that apply to them.
- ☑ **Heterogeneity:** Chief security officers, IT directors and managers are usually responsible for enforcing compliance across a heterogeneous environment – different operating systems, database management systems, web servers and other technologies.

In large enterprises, security officers must establish processes and technologies that provide leverage – the ability to address the enterprise with few resources.

In-house Expertise

Many organizations lack the required expertise for policy enforcement, especially on a scale large enough to perform the work necessary. As a result, they may have to hire expensive consultants to develop and facilitate the process. Key areas of expertise include:

- ☑ **Policy and standards development:** It is difficult to create realistic and effective policies and standards without experience and in-depth knowledge. Developing policies from scratch can be very time-consuming and frustrating. Moreover, it is a highly political process that involves numerous stakeholders – executive (read *CEO*) sponsorship, careful wordsmithing, thorough review and approval, and aggressive “promotion” of policies are keys to success.

- ☑ **IT security assessments:** Performing detailed security assessments with native tools, open source or cheap utilities, or vulnerability assessment products typically require a significant amount of security expertise that may not be available or affordable from in-house staff.
- ☑ **Securing systems:** Whether hardening a Unix server or configuring a firewall to prohibit unauthorized web use, securing systems requires significant technical expertise.

Organization should seek solutions that minimize the amount of knowledge required for the task. Tools should include knowledge and features that facilitate quick deployments and are based on existing industry standards such as ISO17799.

Proactive Enforcement via Policy Management Lifecycle

By viewing policy enforcement from the perspective of a continuous life cycle, companies can organize their efforts based on four key areas: policy **establishment**, **education**, **enforcement** and **evaluation**. Known as the four E's of the policy enforcement lifecycle, these stages provide a mature policy management process that can be automated, repeatable and measurable.

- 1. Establish policies:** Companies need the capability to establish policies that drive efficiency and limit risk. Since many companies do not have policy expertise internally, solutions should include “best practices” content that can be easily implemented by novice users. Solutions should also offer content that is specific to “policy rich” industries such as financial services and healthcare.
- 2. Educate workers:** Organizations need to communicate policies and standards to the people responsible for enforcing and complying with them. Once communicated, it is important to certify that users understand and accept the policies that govern them. Solutions should be able to educate workers on a large scale, without overwhelming each worker with content. Key to success includes making policies role specific – a staff accountant should read a different set of policies than a Windows administrator, although there may be some overlap.
- 3. Enforce policies:** Organizations need to enforce policies for both people and technology. People behavior must be monitored and restricted in some cases such as controlling web browsing, e-mail and instant messaging to ensure users are not violating acceptable use, information classification and handling, and other policies. Technology enforcement focuses on technical security settings on key platforms such as Windows, Unix, NetWare, and iSeries as well as mission critical applications such as databases and web servers.
- 4. Evaluate compliance:** Organizations need to assess compliance with security policies for people and technology as well. All personnel must read and agreed to abide by security policies and standards that apply to them. There must also be some kind of system that alerts operators when workers attempt to bypass acceptable usage, information classification and related policies. Technologies, in turn, must be routinely evaluated for compliance with corporate security policies and standards. Compliance assessment is used to evaluate current effectiveness and may lead to changes or improvements in procedures that help to enforce policies.

While each of these stages is described separately, they should not be viewed as distinct. Each is dependent on the others. Establishing policies is senseless without educating and enforcing them. Doing so would be a waste of paper. Moreover, policies (along with standards and guidelines) should be “living breathing” documents, which are maintained based on routine evaluations for both compliance and effectiveness.

NetIQ Proactive Policy Enforcement Solutions

NetIQ’s Policy Enforcement Solutions increases efficiency and reduces risk by providing products that implement and manage across the four key areas of the Policy Management Lifecycle: **establishment**, **education**, and **enforcement** and **evaluation**. As shown below, NetIQ views the lifecycle as a repeatable process that results in continuous improvement in compliance, risk reduction and efficiency.



NetIQ provides three primary product suites that help fulfill the policy management lifecycle: VigilEnt Policy Center, the Marshal products, and VigilEnt Security Manager. The table shown below illustrates how each of the NetIQ products fits within the Policy Lifecycle and positions them according to the key policy deliverable necessary to assure proactive and practical enforcement across the enterprise. In the following section, NetIQ solution capabilities are explained for each of the four phases of the policy enforcement lifecycle.

| Key Deliverables | Policy Lifecycle Stage | | | |
|------------------------------|--|--|---|---|
| | Establish | Educate | Enforce | Evaluate |
| Acceptable Use of Internet | <input checked="" type="checkbox"/> VigilEnt Policy Center | <input checked="" type="checkbox"/> VigilEnt Policy Center | <input checked="" type="checkbox"/> Marshal products <input checked="" type="checkbox"/> VigilEnt Security Manager | <input checked="" type="checkbox"/> Marshal products <input checked="" type="checkbox"/> VigilEnt Security Manager |
| Information Classification | <input checked="" type="checkbox"/> VigilEnt Policy Center | <input checked="" type="checkbox"/> VigilEnt Policy Center | <input checked="" type="checkbox"/> Marshal products | <input checked="" type="checkbox"/> Marshal products |
| Technical Security Standards | <input checked="" type="checkbox"/> VigilEnt Policy Center | <input checked="" type="checkbox"/> VigilEnt Policy Center | <input checked="" type="checkbox"/> VigilEnt Security Manager | <input checked="" type="checkbox"/> VigilEnt Security Manager |

1. Establish policies: For security officers, establishing policies means more than just technical configuration standards. They must include business rules that guide both human behavior and machine settings. VigilEnt Policy Center from NetIQ provides a complete enterprise-class solution for creating policies, distributing them for review, tracking comments and approvals, and publishing them online for easy access. These policies may include, but are not limited to:

- ☑ Security configuration standards to properly secure the technology infrastructure including Windows, Unix, iSeries, web servers and databases
- ☑ Acceptable use policies aimed at prohibiting illicit web browsing, downloading or uploading inappropriate files, and other dangerous web and instant messenger activities
- ☑ Information classification and handling designed to prohibit the transmission of sensitive corporate information such as trade secrets, business plans and others

VigilEnt Policy Center improves efficiency by speeding the creation of policies with the content libraries that incorporate the latest in leading practice standards and wording. Not only does VigilEnt Policy Center ship with extensive policy content from Charles Cresson Wood¹, CISSP, organized by ISO 17799, but also content modules for GLBA, HIPAA and FDA 21 CFR Part 11.

VigilEnt Policy Center also provides a facility for distributing policies for review, obtaining comments and approvals, and publishing the final version. All versions are archived and tracked, providing a complete audit trail of all policies and other content ever issued.

2. Educate workers: Once policies are established, it is essential that all stakeholders connected with the enterprise understand and accept the policies that govern them and the systems they use. VigilEnt Policy Center communicates policies to employees, business partners, and others according to their roles and responsibilities via an Internet browser. VigilEnt Policy Center provides a straightforward but highly effective approach for communicating policies and verifying users have read and agreed to abide by them.

Don't just take our word for it...

NetIQ is not the only one advocating a multi-pronged approach for managing and enforcing security policies.

Charles Cresson Wood, author of Information Security Policies Made Easy, agrees that policy management should be treated as a process where organizations “move away from viewing policy development and/or update as a project.” According to Wood, the process should include periodically assessing of compliance and routine policy-based education.

Michel R. Overly, author of E-Policy: How to Develop Computer, E-Policy, and Internet Guidelines to Protect Your Company and Its Assets, argues for a 3-step process that includes (1) establishing policies that are very specific on the rights and obligations of employees, (2) training and awareness seminars for employees and (3) enforcement via technical means such as monitoring and filtering software.

- ☑ Workers login to the VigilEnt Policy Center through a web browser using (in most organizations) their corporate network user accounts (e.g. Active Directory user accounts).
- ☑ VigilEnt Policy Center presents users with policies that apply only to their specific roles. For example, VigilEnt Policy Center may present a system administrator with the Windows security configuration standards and the acceptable use policy.

¹ Author of Information Security Policies Made Easy.

- ☑ Users read the appropriate policies and check a box that indicates their agreement. This digital signature satisfies due diligence for accountability and compliance.
- ☑ Users can also be made to take quizzes on selected policies to ensure they have read and understand them providing additional evidence of accountability and compliance.

Thus, VigilEnt Policy Center not only saves considerable time and effort in the development and communication of policies, it also tracks compliance in terms of securing agreements to abide by policies. This helps limit security and legal risks while ensuring compliance with regulations required of key stakeholders.

3. Enforce policies: VigilEnt Security Manager and Marshal products from NetIQ provide an effective and efficient means to enforce many policies and standards such as:

- ☑ Security configuration standards are enabled with VigilEnt Security Manager’s built in knowledge base to manage Windows, Unix, Linux, NetWare, iSeries (AS/400s), web servers and databases.
- ☑ Acceptable use policies are enforced with NetIQ MailMarshal², WebMarshal, and imMarshal products that prevent illicit web browsing, downloading or uploading inappropriate files, and other dangerous activities.
- ☑ Information classification controls are enforced by preventing the transmission of sensitive corporate information such as trade secrets, business plans and others based on key words, phrases and labels (e.g., “Company Sensitive” or “Top Secret”).

VigilEnt Security Manager and the Marshal products improve efficiency by centralizing the management of system configurations, enforcing content security in real-time, saving employee time by reducing spam, and conserving network bandwidth and system-processing power by limiting the non-business use. VigilEnt Security Manager and the Marshal products also limit risk by ensuring that systems are configured in a way that limits security exposure and controlling employee use of tools like email, web and instant messenger in a manner that results in legal or security exposure.

4. Evaluate compliance: VigilEnt Policy Center, VigilEnt Security Manager and the Marshal products provide powerful and rapid report creation to continuously evaluate the effectiveness of policy enforcement.

- ☑ VigilEnt Policy Center, for example, provides management reports to monitor and report on users, policies, quizzes, and policy violations. Security officers can easily run reports to identify employees or groups that have or have not read policies and how well they understand them. Security officers can then send follow up e-mails through VigilEnt Policy Center to remind employees that have failed to read policies or pass quizzes.
- ☑ Security check-up (compliance) reports through VigilEnt Security Manager provide analysis of how policies have been adopted across the technology infrastructure of the organization. VigilEnt Security Manager provides a mechanism to score systems, as well as consolidate scores at hierarchical levels to evaluate departments, business units or the entire enterprise.
- ☑ NetIQ Marshal products provide reports that reveal patterns of how employees may be abusing email, web and/or instant messaging services. Reports can be used to identify trends and take appropriate action to revise or enhance policies and procedures.

² For Exchange or SMTP-based e-mail servers.

Together, VigilEnt Policy Center, VigilEnt Security Manager and the Marshal products improve efficiency and reduce risk by enabling security professionals to quickly measure the effectiveness of existing policies and enforcement and identify trends and issues that may need attention or further action.

Key Policy Enforcement Advantages

NetIQ provides a comprehensive policy enforcement solution matched to the policy lifecycle while also addressing the challenges of the larger enterprise in terms of size, complexity, heterogeneous environment, lack of in-house expertise, and constant change.

Designed for the Large Enterprise – NetIQ’s Policy Enforcement Solution supports large enterprises with enterprise scalability.

- ☑ **Role-based access controls:** Support for extensive role-based access controls and policy filtering in both VigilEnt Policy Center and VigilEnt Security Manager.
- ☑ **Robust architecture:** VigilEnt Policy Center and VigilEnt Security Manager’s three-tiered architecture and robust infrastructure scales to meet the needs of the large environment, supporting an enterprise-class DBMS, light-weight, latency-tolerant communications and built-in messaging, and fault-tolerant deployments. VigilEnt Security Manager has been tested and certified for performance and scalability by an independent third-party.
- ☑ **High performance:** All three products are designed to perform at a large scale by being high performance. Both VigilEnt Policy Center and VigilEnt Security Manager have undergone extensive scalability and performance testing at all levels. Moreover, the Marshal products are among the most scalable in the industry, with support for over 100,000 e-mail or web users.

Ease of Deployment and Configuration – NetIQ’s Policy Enforcement Solution can be implemented quickly in a large enterprise.

- ☑ **Directory integration:** VigilEnt Policy Center integrates with a corporate directory such as Active Directory, eDirectory or Sun ONE to immediately incorporate an enterprise’s user base. There is no need to import or create user accounts – use the ones you already have.
- ☑ **Flexible policy importing:** VigilEnt Policy Center can easily import existing policies from numerous formats, including Word, Adobe Acrobat, HTML files, and more.
- ☑ **Lightweight deployments:** VigilEnt Security Manager provides for agentless deployments on Windows, Unix, NetWare and databases and also supports the centralized installation of Windows and Unix agents where needed.
- ☑ **Asset discovery:** Asset discovery in VigilEnt Security Manager uses scheduled port scans, DNS lookups, domain discovery and/or NIS lookups to populate the list of potential assets.
- ☑ **Configuration wizards:** Wizards help you configure and deploy the Marshal products quickly, along with seamless integration of mails servers, proxies, and antivirus software.

Support for a Wide Range of Technologies – NetIQ’s Policy Enforcement Solution includes broad support for the wide variety of technologies typical in a large enterprise.

- ☑ **Technology assessment:** VigilEnt Security Manager provides vulnerability and configuration management for major operating systems and applications including Windows, Unix, Linux, iSeries, NetWare, IIS, Sun ONE, Apache, Oracle, Sybase and SQL Server.
- ☑ **Content security:** Marshal products support a wide range of technologies including mails servers, proxies, and antivirus software applications

Extensive Built-in Knowledge – NetIQ’s Policy Enforcement Solution includes extensive knowledge among all products involved in the policy enforcement lifecycle.

- ☑ **Policy content libraries:** VigilEnt Policy Center’s library includes policies and standards developed by recognized expert Charles Cresson Wood, CISSP, with additional quizzes and technical standards from NetIQ. The policy library is organized according to ISO 17799 standards for optimum organization. Optional VigilEnt Policy Center content modules are available for HIPAA, Gramm-Leach-Bliley Act (GLBA), and FDA 21 CFR Part 11.
- ☑ **Built-in technical checkup templates:** VigilEnt Security Manager includes thousands of security checks for mission critical operating systems such as Windows, Unix, Linux and OS/400, enterprise-class databases such as Oracle, SQL Server, Sybase, web servers such as IIS, Apache, Sun ONE, Netscape, iPlanet, and Check Point firewalls
- ☑ **Content security rules:** The Marshal products’ configuration wizards include extensive rules for enforcing acceptable use policies, information classification and handling rules, and other security provisions.

Frequent Updates – NetIQ’s Policy Enforcement Solution helps manage change with frequent updates to its extensive knowledge base.

- ☑ **Policy content modules:** VigilEnt Policy Center’s enables customers to quickly develop and rollout new policies to address efficiency and risk.
- ☑ **Technical checkup templates:** VigilEnt Security Manager is periodically updated to account for new vulnerabilities aimed at mission critical operating systems, enterprise-class databases, web servers, and firewalls.
- ☑ **Content security rules:** MailMarshal includes an automatic update service to address new techniques used by spammers and attackers.

Conclusion

NetIQ’s Policy Enforcement solution offers one of the most comprehensive solutions from a single vendor available today.

Only Complete Policy Enforcement Lifecycle solution – NetIQ offers the only solution to address the complete policy enforcement lifecycle including policy establishment, education, enforcement and evaluation.

Enterprise Class Solution – All NetIQ products are designed to support a large enterprise by (1) scaling to large user-bases, number of machines, variety of platforms, and bandwidth of e-mail, web and instant messaging traffic; (2) providing role-based access and filtering of content and (3) integrating with key corporate technologies (e.g., LDAP directories, Exchange and SMTP servers, enterprise DBMSs, etc.).

Solution Integration – VigilEnt Policy Center exports policies (or standards) to VigilEnt Security Manager as checkup templates. This enables a policy owner to create a policy in VigilEnt Policy Center, export it to VigilEnt Security Manager, and perform assessments of key technologies against those policies (standards). Policies in VigilEnt Policy Center are also mapped to rules in the Marshal products, enabling clear enforcement of Acceptable Use Policies. When an employee violates Acceptable Use Policy, Marshal can automatically direct them back to VigilEnt Policy Center to review the policy that was violated.

To learn more about a proactive approach to Enterprise Policy Enforcement, visit NetIQ's Security Management Solutions web page at <http://www.netiq.com/solutions/security/default.asp> – feel free to download VigilEnt Policy Center, the Marshal products or VigilEnt Security Manager for a free, 30-day trial. To contact the sales office nearest you, please fill out our sales contact form on our [website](#).