



Sustainable Compliance: How to Align Compliance, Security and Business Goals

Regulatory compliance has become an important corporate initiative as the complexity and scope of the regulatory environment continues to increase. Coupled with the rise in cyber attacks and insider threats, organizations are now searching for a more effective, sustainable, and scalable approach that will achieve their compliance objectives while improving the overall security posture of the organization.

In this white paper, we will examine some of the challenges that modern organizations face in their efforts to develop and adapt a compliance program to solve today's needs and support new requirements in the future.



Table of Contents

Today's Challenge	1
Security Budgets Continue to be Driven by Compliance.....	1
Rising Pressure to Meet Increasing Regulatory Mandates	1
The Nature of Security Threats Is Rapidly Evolving	1
IT Security Has Not Kept Pace with Evolving Technology and Business Models	2
Achieving Sustainable Compliance	2
Business Alignment	2
Harmonized Controls.....	3
Good Security Leads to Compliance	3
Automation, Integration, and Optimization	4
Adapting to a Rapidly Evolving Threat Landscape.....	4
Evolving Technology.....	4
The New Attacker	5
Evolving Business Models.....	5
Align Compliance, Security, and Business Goals with NetIQ Identity and Security Management Solutions..	6
Conclusion.....	7
About NetIQ.....	8



Today's Challenge

In today's complex regulatory environment, many organizations struggle to integrate regulatory compliance programs with day-to-day security operations. This can lead to audit findings and data breaches that result in costly mitigation, or even fines and penalties. According to Ponemon's 2010 *Annual Study: U.S. Cost of a Data Breach*, the average organizational cost of a data breach is approximately \$7.2 million dollars, up 7% from 2009.¹

As compliance programs place ever-greater demands on IT resources, businesses are left urgently searching for a more effective, sustainable, and scalable approach that will achieve compliance objectives while improving the overall security posture of the organization. In this white paper, we will examine some of the challenges that modern organizations face in their efforts to develop and adapt a compliance program for current and evolving needs.

Security Budgets Continue to be Driven by Compliance

The mandatory nature of regulatory compliance, combined with specific and quantifiable penalties for non-compliance, has directed a large portion of overall security spending toward compliance efforts. It is hard to argue with this objective, because the goal of compliance spending is to protect corporate profitability and avoid increased costs from non-compliance and possible brand damage. However, when security projects are focused solely on meeting a minimal set of audit criteria rather than minimizing risk, much of the potential benefit of this funding is wasted.

The challenge for security teams is to ensure that security expenditures are directed toward a comprehensive risk mitigation program aligned to the risk tolerance and business objectives of the organization. Allowing the "accredit and forget it" approach to drive security priorities is like cramming for an exam. You may pass the exam (or the audit), but you are unlikely to retain the benefits you would have gained from careful study and planning. Passing an audit for PCI DSS, for example, is a good achievement. But even PCI DSS, considered one of the most prescriptive mandates, is only a minimum security standard and does not guarantee protection against data breaches. Case in point: Both Heartland Payment Systems and T.J. Maxx had achieved or were achieving PCI compliance when their systems were breached by a global identity theft ring, resulting in two of the largest breaches of credit card data in history. Ask yourself: Does compliance drive your security program without always improving security?

Rising Pressure to Meet Increasing Regulatory Mandates

The increased number of compliance mandates is driven in no small part by a growing public awareness of corporate malpractice and the risks of data theft. Regulatory and industry bodies have responded to public concern by mandating breach notification and imposing increasingly broad controls with more stringent penalties for non-compliance. Furthermore, as organizations seek to enforce compliance standards across their businesses, they may impose additional or even contradictory goals on administrators and compliance officers in the process.

Many of today's organizations are struggling to implement a sustainable compliance program that can address the full set of compliance mandates and adapt quickly as mandates evolve or new mandates are created. How rapidly can your organization adapt to new and evolving compliance mandates?

The Nature of Security Threats Is Rapidly Evolving

External threats have evolved from individual hackers to sophisticated, organized groups motivated by financial and political gain. These attacks are often backed by the funding of international corporations, organized crime, and even governments. With this level of support, it is not surprising that security breaches are enabled by increasingly sophisticated technology and often assisted by someone on the inside. The insiders are bribed, coerced or even recruited specifically to join the organization to steal sensitive information. With this in mind, do you know if your team is prepared to defend against these sophisticated attacks, and do you know who in the organization you can trust?

¹ 2010 *Annual Study: U.S. Cost of a Data Breach*, The Ponemon Institute, March 2011.



IT Security Has Not Kept Pace with Evolving Technology and Business Models

Staffing is one of the largest, fastest-growing categories of IT budgets. In an effort to slow this growth and control costs, there has been constant pressure to outsource where possible, especially where specialized skill sets are required. In fact, it has been several years since the average organization was staffed exclusively by true employees.

As a result, most organizations have policies and controls in place to support temporary staff, onsite partners, and even visitors.

In the effort to control costs, what many organizations have failed to consider is that outsourcing tasks does not transfer responsibility. If the outsourcing partner fails to adhere to control objectives, the liability is still held by the organization. Outsourcing is delegating, not abdicating. Because many organizations have been slow to realize this, their policies and controls have not kept up with outsourcing whether it is from a service or cloud provider. Do you know who in your organization is responsible for ensuring that service and cloud providers adhere to your control objectives? Are you taking necessary steps to protect sensitive information?

Achieving Sustainable Compliance

The foundation of a sustainable security and compliance program is a common, business-aligned framework that addresses the complete set of industry and regulatory mandates while alleviating the underlying security exposures. This is easier to state than to achieve, but the alternative is a costly and sometimes ineffective program that does nothing to improve the overall security posture of the organization. Business alignment is critical to ensure security expenditures are focused on the relevant exposure, based on the nature and risk tolerance of the business.

Without alignment, it is difficult to demonstrate the efficacy of current expenditures or justify additional investments. A common, harmonized framework of control objectives is required to reduce the cost and complexity of addressing multiple mandates. Harmonizing on a common set of control objectives, however, is not sufficient in and of itself. A truly sustainable program requires automation to reduce the labor costs associated with the monitoring, enforcement, and evidencing of effectiveness of these control objectives.

Business Alignment

Increased recognition of the importance of IT security and compliance and the significant costs involved has begun to change the role of the security executive. Increasingly, CISOs are reporting to the CEO or CFO rather than operating as a department within IT. A recent Forrester report² notes that 54 percent of organizations have a chief information security officer reporting directly to a C-level executive, while 42 percent have a CISO reporting to someone outside of the IT department. The role of the CISO will continue to evolve over time, but the fact that CISOs are reporting outside of the IT department, with access and input to how business decisions are made, is a milestone and trend that needs to continue.

In a recent CSO Online article³, Eric Cowperthwaite, CSO of Seattle-based Providence Health & Services also acknowledged this trend, stating:

"[T]he CSO/CISO has become a permanent part of the group sitting at the table deciding how the company does business. The CSO leads the security function within the business and that function is now viewed as a necessary function within the business, rather than something to be given lip service to keep the regulators away but otherwise ignored. This is a significant and powerful change, in my opinion."

Closer business alignment enables security to be involved earlier in new initiatives. This allows the security teams to interject risk mitigation into the planning phase rather than having to layer on costly security remedies after the fact, slowing or becoming an outright barrier to new business initiatives.

² "Forsights: The Evolution Of IT Security," 2010 to 2011

³ Bill Brenner, Senior Editor, *The New CISO: How the role has changed in 5 years*, CSO Online, November 2, 2010, <http://www.csoonline.com/article/632223/the-new-ciso-how-the-role-has-changed-in-5-years> (accessed March 15, 2011).



A recent example of security obstructing business goal attainment was demonstrated at a large corporation in the United States where multiple business units had independently adopted software as a service (SaaS) solutions. During a routine internal audit of their provisioning controls, the audit team pulled the controls documentation and began reviewing evidence that the process was being followed. The review was going well until someone asked how users are provisioned to the SaaS applications.

After a protracted effort, the audit team finally managed to collect documentation for each process and the associated owners. The materials were laid out and completely covered a large conference room table. After careful review of the materials, they found numerous process inconsistencies, identified owners who had moved to other positions, and

cases where the processes violated existing controls. These internal audit findings resulted in the security team taking the stance that no SaaS applications could be adopted until further notice.

Situations like this can be avoided when the security team is closely aligned to the business and involved early in business initiatives. Additionally, early involvement by the security team may allow the risk mitigations needed for new initiatives to be included in the cost of the initiative, rather than further burdening an already oversubscribed security budget.

Harmonized Controls

A sustainable compliance program must efficiently handle the myriad collection of regulatory and industry mandates faced by an organization, and be readily adaptable to address new and ever-evolving mandates. It must also avoid the all too familiar annual or quarterly “audit panic.” Early inefficient compliance programs – as well as many programs today – fail to address these criteria. The programs are reactionary and include distinct projects for each regulation or mandate. Most organizations have evolved their approach and now maintain a central team to coordinate security and compliance controls.

The next step in achieving a sustainable program utilizes a harmonized set of IT controls. The set is created based on a best-practice framework, and control objectives are defined to collectively address the complete set of regulatory, industry, and internal corporate mandates. This approach allows the security and compliance teams to focus on a single target set of controls, avoiding confusion, conflicting controls, and unnecessary expense.

Leveraging a common set of controls simplifies audits and provides a framework for audit reporting based on how the controls map to a given mandate. As the regulatory environment evolves, controls can be added to this common set, allowing the organization to quickly adapt their compliance program.

Good Security Leads to Compliance

Streamlining compliance activities into a common framework is not simple. Security and compliance teams may involve multiple groups within an organization, crossing organizational and geographic boundaries.

Approaching security and compliance with a set of harmonized controls is effective only if the selected controls are appropriate to address the security risks of the organization. It is important to remember that regulatory and industry mandates are minimum guidelines and do not ensure the security risks of the organization are addressed. The Heartland Payment Systems, Inc. breach from January 2009 is a good example. Heartland had just passed a PCI DSS audit when a breach occurred.

A more effective approach is to focus on how to address the security risk of organization and allow compliance to be achieved as a by-product. It is clear that Heartland now understands this approach as Kris Herrin, CTO of Heartland recently commented that, “One of the most important things for us is to make sure [that] our security controls are sustainable and that they’re done in a way that we have sustainability to the control... We can’t just throw something in one quarter because it sounds like a good idea, and then a year down the road, find that it is not mitigating the risk we expected it to mitigate.”⁴ In order to improve their security postures both in the short- and long-term, organizations must

⁴ Beth Schultz, [What's Next for SIEM? SIEM platforms can deliver, if implemented correctly](#), SC Magazine ebook (2011).



ensure that the appropriate controls and tools to address the security risk are defined and fit within a comprehensive risk mitigation program that stipulates deployment, staffing, and security process planning, and is aligned to the risk tolerance and business objectives of the organization. For instance, an astounding 86 percent of data breach victims had evidence in their log files prior to being breached, according to the *2010 Data Breach Investigations Report*. By not reviewing the logs, these organizations left themselves open to a breach. This behavior exemplifies the danger of a “check-the-box” approach to compliance.

Organizations that pursue compliance for the sake of compliance are like people who go on crash diets. They may look good for a while, but will probably not have improved their health or made a genuine commitment to a healthier lifestyle overall. And the weight loss is likely not sustainable long term. Likewise, sustainable compliance is best achieved by focusing on improvements to the overall security posture of the organization.

Automation, Integration, and Optimization

Crucial to reducing the cost of compliance and avoiding annual or quarterly “audit panic” is the automation of routine, labor-intensive tasks. Automation helps to ensure a reliable, repeatable process and strict adherence to policy. Some examples of tasks that are appropriate for automation include data collection and evaluation and monitoring and enforcement of technical and manual controls. Automation can also be leveraged in the capture and utilization of embedded corporate and best-practice knowledge, freeing up skilled staff for more important tasks. By freeing overburdened resources, automation can help reduce human error and decrease training costs for new employees. This type of automation for security and compliance is what Identity and Access Management, SIEM, security assessment, and other enterprise software packages are intended to deliver. Make sure that the solutions you select provide the level of automation your organization needs.

Adapting to a Rapidly Evolving Threat Landscape

A sustainable security and compliance program must be structured to adapt to changing compliance mandates and an evolving threat environment. This includes changes in the nature of and motivation behind attacks and new risks associated with changing technologies and evolving business models.

Evolving Technology

The nature of attacks has been consistently evolving in the “arms race” between security practitioners and attackers. If anything, this trend is accelerating as the primary motivations of attacks are now financial and political. The good news is that security practitioners have earned the right to be called security professionals. Some of the most talented staff within IT are in security groups, and security programs are maturing.

The bad news is that attackers have also become more professional and organized. They are recruiting talent, investing in research and development, and producing new, more advanced tools. The “Stuxnet” worm is a notable example of what such well-funded groups can produce. According to the Verizon Business RISK Team’s *2010 Data Breach Investigations Report*, 32 percent of attacks were by organized groups, including 24 percent by organized criminal groups.⁵ In terms of compromised records, the report found that 85 percent were attributed to well-funded criminal organizations, including organized crime and governments.

One reason why most IT professionals enter the field is to work with the latest technologies. The industry, which hasn’t disappointed them, is characterized by consistent waves of new technologies – with each wave comes security risk and, with some, new business models. The latest of these has been *virtualization*, the use of consumer devices and services within the enterprise and cloud infrastructure and software services. The operational savings associated with both

⁵ Verizon Business RISK Team in cooperation with the United States Secret Service, “2010 Data Breach Investigations Report,” Verizon Business, July 2010, http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf?&src=/worldwide/resources/index.xml&id (accessed March 15, 2011).



virtualization- and cloud-based services are such that in some organizations, adoption has overtaken the understanding of the associated risks, and security teams are playing catch-up. Make sure that your organization is continually reviewing these trends and obtaining outside help where needed. The majority of even the most sophisticated attacks can still be slowed or stopped by relatively simple controls, provided they are consistently enforced.

The New Attacker

Today, many data breaches are being perpetrated not by outside hackers but by financially and/or politically motivated insiders. According to the *2010 Data Breach Investigations Report*, 27 percent of data breaches were perpetrated exclusively by internal agents, with an additional 1 percent by partner agents and 27 percent by multiple agents.⁶ With this large percentage of breaches attributed to insiders, the question is who are these insiders?

Enterprise environments today have a diverse and dynamic workforce in which a greater number of people have access – directly or indirectly – to sensitive information and systems. In this dynamic environment, the risk of user activity contributing to a data breach is growing. In the same Verizon report, 90 percent of internal activity attributed to a breach was found to be from deliberate actions, 6 percent from inappropriate activity, and 4 percent through unintentional activity.⁷

Often, non-malicious activity may also lead to downtime, lost revenue, and audit failures. For instance, a large retailer in the U.S. recently experienced an outage when a new administrator made changes to Active Directory Group Policies outside the change control process. The administrator then attempted to cover his tracks when he realized he had caused downtime. His actions directly led to a halt to product shipments for several days as they struggled to restore operations. The activity was not malicious, but it was inappropriate and had significant negative ramifications.

Whether the activity is that of a typical end user, manager, or privileged administrator, the risks associated with deliberate, inappropriate, or inadvertent activity can be significantly reduced through relatively simple controls. An example of such controls would be a policy to ensure exiting employee accounts are quickly disabled, shared administrative accounts are avoided, and the activity of privileged users, whether administrators or end users, are monitored. The leak of U.S. State Department documents to Wikileaks is an example of unauthorized activity by an authorized user. The breach allegedly perpetrated by Pfc. Bradley Manning illustrates a conflict between free access to information to improve communication and narrowly restricted access for security. There were reportedly many signals that Pfc. Bradley Manning should not be trusted with sensitive information, but he was still given access. For example, while stationed at Fort Huachuca, Arizona, Pfc. Manning was reprimanded for putting mundane video messages to friends on YouTube that carelessly revealed sensitive information. Yet he soon graduated from training as an intelligence analyst with a security clearance.⁸ The first step is providing the minimum access required. The second and critical step is to monitor how privileges are leveraged.

Evolving Business Models

In addition to the evolving nature of attacks, security organizations are also faced with the challenges of an increasingly dynamic and loosely defined perimeter. Those considered insiders in most organizations today include much more than just employees and contractors. Insiders today can include the staff of partners, managed service providers, hosting providers, and cloud providers. Anyone who directly or indirectly manages sensitive information, or the systems and applications that host it, is an insider. This has been overlooked by many until recently.

Organizations are learning that in outsourcing, they have delegated tasks but not responsibility. As a result, there is increased focus on negotiating specific controls and requiring independent security audits. SAS 70 certification is simply not sufficient. Service providers who once viewed security as something beyond the scope of their services have been forced to introduce base security processes and routine auditing in their core service offerings to remain competitive.

⁶ Verizon Business RISK Team in cooperation with the United States Secret Service, "2010 Data Breach Investigations Report."

⁷ Verizon Business RISK Team in cooperation with the United States Secret Service, "2010 Data Breach Investigations Report."

⁸ Denver Nicks, [Private Manning and the Making of Wikileaks](http://thislandpress.com/09/23/2010/private-manning-and-the-making-of-wikileaks-2/), This Land, September 23, 2010, <http://thislandpress.com/09/23/2010/private-manning-and-the-making-of-wikileaks-2/> (accessed March 15, 2010).



In this data-centric world with evolving threats and loosely defined perimeters, there is increasing discussion and effort to move to what Forrester is describing as “The Zero Trust Network Architecture.”⁹ In this model, the focus is data-centric from the inside out and relies on building security into the network and systems directly, rather than as an overlay after the fact. In order to improve security, the perimeter collapses around the data itself. While it will take time to shift our enterprise environments to a model like this, the core concept can be applied today by moving from a focus on where your critical systems and information are, to the recognition that the insiders who have access are likely not all employees and that all activity must be monitored. Trust no one.

Virtualization and readily available bandwidth are taking outsourcing to the next level as cloud computing enables both large and small organizations to reduce cost and increase flexibility within IT. As with outsourcing, these technology changes are not always deployed with security in mind. As organizations become more aware of the risks associated with data center consolidation and cloud computing, those businesses and agencies with a low risk tolerance are increasingly reluctant to leverage these technologies. Fortunately, industry experts have come together through groups such as the Cloud Security Alliance (CSA) to work on this problem. In the publication “Security Guidance for Critical Areas of Focus in Cloud Computing,” the CSA recommends that organizations take several key steps to protect assets deployed in the cloud.¹⁰ First, organizations considering cloud computing should identify the assets that would be most appropriate for this type of deployment and identify their risk tolerance for these assets before deciding whether the cost savings outweigh the risk. If a decision is made to leverage the cloud, the organization should invest a portion of the cost savings associated with cloud computing to fund the development, implementation and monitoring of security controls specific to the assets in the cloud. And perhaps most importantly, prior to signing any contractual agreement with a cloud vendor, it is critical to agree on service level agreements, required controls, and audit rights, and incorporate the agreement in the final contract.

Align Compliance, Security, and Business Goals with NetIQ Identity and Security Management Solutions

NetIQ offers multiple product families in its identity and security management portfolio to address the needs of organizations seeking to meet their compliance objectives while maintaining a secure environment and aligning with stated business objectives:

NetIQ® Directory and Resource Administrator™ mediates access to Microsoft Active Directory, limiting the user to particular actions for specific views of the overall directory. As part of NetIQ’s identity and access management offering, it supports user provisioning and other automated tasks and processes. It also eases directory consolidation efforts and helps enforce security policies and segregation of duties.

NetIQ® Change Guardian™ products provide real-time monitoring and notification of changes across your distributed environment, providing detailed insight into files, directories, file shares, registry keys (on Windows), system processes, database activity (on Oracle, Microsoft, Sybase, and other databases), and more. They also deliver enhanced audit information to provide greater fidelity and clarity of information than native log events can provide, and recording pre- and post-change information for improved incident analysis.

NetIQ® Security Manager™ provides real-time monitoring of system changes and user activity, centralized log management and correlation, and incident response automation – all within a single, integrated, and scalable infrastructure. When tightly integrated with NetIQ Change Guardian products, NetIQ Security Manager delivers correlated, rich, and relevant information in real time to security and compliance teams, helping them to respond quickly and decisively should an issue arise.

NetIQ® Secure Configuration Manager™ enables periodic assessment and reporting of system configuration changes

⁹ John Kindervag with Stephanie Balaouras and Lindsey Coit, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture,” Forrester Research, Inc., November 5, 2010, <http://www.forrester.com/rb/research>.

¹⁰ Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing,” <http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf> (accessed March 15, 2011).



and matches that configuration against regulatory requirements and best practice policies to help ensure compliance with SOX, PCI DSS, HIPAA/HITECH, FISMA, NERC CIP, and more. Furthermore, NetIQ Secure Configuration Manager's user entitlement reporting assesses user permissions for access to critical information, providing the business with answers to *who* has access and *what* is their level of access to critical information, helping to reduce insider threat.

NetIQ provides other products to address data protection and regulatory compliance needs. To learn more, visit www.netiq.com.

Conclusion

The challenge of building an effective compliance program – one that helps you to meet your compliance, security, and business objectives simultaneously – is more daunting than ever before. The task of complying with scores of overlapping regulatory and industry mandates, often with the same set of IT resources, is time-consuming and complex. Too often, overwhelmed security teams revert to an “accredit and forget it” mindset, allowing a minimal set of audit criteria to drive their security priorities, rather than focusing on managing risk in alignment with the risk tolerance and business objectives of the organization.

In addition to the pressures of meeting multiple mandates and ensuring that the security budget is effectively utilized, organizations today are faced with a rapidly evolving threat landscape. As new business models such as outsourcing and cloud computing make the network perimeter more fluid and financially or politically motivated attacks are perpetrated by sophisticated, organized groups or malicious insiders, organizations must rapidly develop security program maturity to avoid a breach. Today's organizations must be able to effectively develop, implement, and monitor appropriate security controls for their critical information and infrastructure wherever it may be. They must recognize that the “insiders” who have access to this critical information may not be who they seem, and as a result, all activity must be monitored and no one can be completely trusted.

In this complex and challenging environment, the single best way to achieve compliance is to get the security basics right. First, implement and manage to a harmonized set of controls that meet your evolving regulatory and corporate mandates. As you implement these security controls, make certain that the solutions you select provide the level of automation required by your organization. The automation of routine, labor-intensive tasks is critical to reducing the cost of compliance and avoiding “audit panic” because it ensures a repeatable process and strict adherence to policy. Only an integrated, automated approach to compliance rooted in sound security principles is effective, sustainable, and scalable – enabling you to achieve your compliance objectives and improve the overall security posture of your organization.



About NetIQ

NetIQ is a global, IT enterprise software company with relentless focus on customer success. Customers and partners choose NetIQ to cost-effectively tackle information protection challenges and manage the complexity of dynamic, highly-distributed business applications.

Our portfolio includes scalable, automated solutions for Identity, Security and Governance, and IT Operations Management that help organizations securely deliver, measure, and manage computing services across physical, virtual, and cloud computing environments. These solutions and our practical, customer-focused approach to solving persistent IT challenges ensure organizations are able to reduce cost, complexity and risk.

To learn more about our industry-acclaimed software solutions, visit www.netiq.com.

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.

Copyright © 2012 NetIQ Corporation and its affiliates. All Rights Reserved.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Worldwide Headquarters

1233 West Loop South, Suite 810
Houston, Texas 77027 USA
Worldwide: +713.548.1700

U.S. / Canada Toll Free: 888.323.6768

info@netiq.com

www.netiq.com

<http://community.netiq.com>

For a complete list of our offices

In North America, Europe, the Middle East
Africa, Asia-Pacific and Latin America,
please visit www.netiq.com/contacts.