WHITE PAPER

Staying Secure in a Cloudy World

The unprecedented rate at which organizations have adopted cloud computing has fundamentally transformed business and government computing infrastructure. IT market researcher IDC predicts that IT cloud services revenue will reach $43.2 billion in the United States by 2016—up from an estimated $18.5 billion in 2011. Although cloud computing undoubtedly affords organizations with remarkable cost savings and operational efficiencies, it also brings new risks and uncertainties. Those organizations that deploy public, private or hybrid cloud infrastructures—which today is virtually all of them—must mitigate inherent security risks while also maintaining compliance with industry and government regulations.

Fortunately, advances in information security and compliance management technologies have empowered cloud-computing users to reduce risk, improve threat response, and drastically reduce the effort needed for compliance management. And NetIQ is leading the charge. This paper contains three simple steps for maintaining visibility and control when moving to the cloud and explains how NetIQ can help with each.

NetIQ

NetIQ | WHITE PAPER

Table of Contents

Cloud Computing Benefits

Cloud computing has revolutionized the way IT delivers applications and services to its users. Its adoption is growing at a rate five to eleven times faster[1] than traditional software, and a considerable portion of IT budgets are increasingly moving to the cloud.

There are dozens of tangible benefits cloud computing brings to organizations—most notably, reduced operating costs, increased scalability and improved business agility.

Security Challenges in the Cloud

Despite the tangible benefits associated with cloud computing, moving to a public, private or hybrid cloud architecture certainly has its challenges—especially as it pertains to security and compliance. IT still has the liability and responsibility to be secure and compliant, and to govern the business while continuing to deliver business services at the right time, to the right user, in the right place.

Reducing Security Risks

A common misconception about migrating applications and services to a cloud infrastructure is that the migration diminishes cyber security risks due to the (perceived) sophisticated network security protections offered by the cloud provider. This is a dangerous assumption, because the need to protect the confidentiality, integrity and availability of your sensitive data, and demonstrate compliance with industry and government regulations, never diminishes and ultimately remains your responsibility. Relying on the protections afforded by a cloud provider can prove to be a devastating decision, as evidenced by Expedia's cloud-computing breach in 2011 and Apple's iCloud breach in 2012.

Although cloud providers consistently deploy best-in-class firewalls and intrusion prevention systems (IPSs) to defend against known cyber threats, these devices do not mitigate risks associated with system misconfigurations and misaligned (and mismanaged) administrative privileges. These security risks apply just as much to systems hosted in the cloud as they do to those present on a physical network. Systems out of sight should never be out of mind.

Detecting Security Breaches

IPS devices, next-generation firewalls (NGFWs), and other signature-based defenses are highly effective at detecting known threats. Some offerings can even detect unknown threats targeting known operating system and application vulnerabilities. However, today's most sophisticated and dangerous cyber threats incorporate never-before-seen malware that is custom-designed to exploit unknown, zero-day vulnerabilities within operating systems and applications as part of an advanced persistent threat, or APT.

Monitoring for security breaches of systems hosted in the cloud can be far more challenging than monitoring on a physical computer network. Most cloud providers do not provide customers with access to the management consoles or logs of their network security devices because the providers use them to monitor intrusions affecting many customers in a multi-tenant virtualized environment. Because of this lack of visibility, it is much harder, if not impossible, for customers to proactively detect and respond to threats to their sensitive data.

Organizations such as the Cloud Security Alliance (CSA) are defining standards that would support federation of cloud security and audit data and give customers better visibility of their sensitive data. However, it is too early for vendors to have begun adopting these standards. Until there is better visibility of sensitive data hosted in the cloud, IT teams must categorize the types of information being

[1] "The Top Three Cloud Stocks from Gartner's Magic Quadrant," *The Motley Fool*, March 7, 2013.

created within their organization and, based on its sensitivity and value, assign levels of associated risk. Once known, IT can better determine which types of information, if any, are suitable for external hosting, and the policies and procedures for governing access.

IT may decide to keep highly sensitive information in house, either in applications or private clouds, where it can prevent breach or theft by centrally controlling and monitoring who has access.

Sustaining Regulatory Compliance

Migrating applications and other IT services to the cloud never diminishes the need to demonstrate compliance with industry (such as PCI and NERC) and government (such as HIPAA, FISMA, SOX, GLBA) regulations. However, demonstrating compliance to external auditors can prove more challenging in a cloud environment as many of the security systems in place to secure the cloud infrastructure are provided and monitored by the cloud provider—not your organization.

Organizations must ensure that sensitive data hosted in cloud services, including private clouds or infrastructure provided as a service (IaaS), is protected and managed in a way that is consistent with corporate information management policies and industry regulations. They will also need to monitor and validate service levels and ensure service providers can consistently deliver the service levels and customer experiences they promise.

Three Simple Steps to Gaining Visibility and Control

Organizations cannot rely on the security defenses of their external cloud providers alone. Prior to implementing cloud technology, organizations must proactively and continuously implement best-of-breed security controls within their on-premises systems to become “cloud-ready.”

A cloud-ready security program helps teams manage the complexity and risk introduced by the cloud. By tightening security controls, systems and policies within the enterprise prior to using cloud technologies, teams can better manage the unavoidable growth in users, devices, applications and information exchanges that occur. A cloud-ready security program will effectively scale throughout hybrid environments composed of both traditional and cloud components, such as components from IaaS providers. Cloud-ready security programs are data-centric, focused on risk mitigation, and help teams maintain a state of continuous security and compliance. Components of a cloud-ready security program include:

- **Change monitoring** – Change monitoring solutions continually monitor, identify and report on unexpected changes to critical files, platforms, applications and systems. These unexpected, often unauthorized, changes could be either unintentional or malicious, yet still compromise the security and compliance posture of the entire organization. For example, file integrity monitoring (FIM) is a specific type of change monitoring technology that monitors the integrity of key files by comparing their current states against known-good baselines. FIM alerts IT to the potential presence of malicious code embedded within operating systems and applications helping to detect advanced threats that may have bypassed traditional security defenses.

- **Secure configuration management** – Secure configuration management solutions assess the security configuration settings (such as password compliance, enabled services, patched vulnerabilities and open ports) of critical IT systems against regulatory requirements, security best practices and corporate IT policies to demonstrate compliance and manage information security risks. If one of these solutions finds a security setting in violation of a secure configuration management policy, the solution alerts IT so it can assess and, if necessary, remediate that setting. Today’s configuration management solutions make it easy for

organizations to “harden” their critical IT systems and maintain a strong security posture while meeting compliance needs.

- **Privileged account management** – Privileged account management solutions enable IT to control and audit use of privileged user credentials (typically Active Directory) through granular permissions delegation and administrative activity monitoring. These offerings protect organizations from unauthorized privilege escalation and help to identify privileged account misuse.

- **Security information and event management (SIEM)** – SIEM solutions provide a holistic view of an organization’s IT security systems and their related security events. SIEM platforms aggregate logs and other security-related data from firewalls, anti-virus (AV) platforms, IPS devices, application software and more, and then correlate this disparate data in an effort to uncover hidden threats.

These four security and risk management solutions work in concert to help organizations improve infrastructure security and reduce risk. Unless an organization leverages these technologies to secure their on-premises systems first—in a coordinated effort to become cloud ready—it faces increased risk migrating any services to the cloud.

The following three-step process—which incorporates aspects of change monitoring, secure configuration management, privileged account management, and SIEM technologies—provides a sensible framework for securing on-premises systems.

Step 1: Reduce Risk

The first step in gaining visibility and control of systems in the cloud is to reduce risk. You can accomplish this by reducing your infrastructure’s attack surface, monitoring the integrity of system configurations and optimizing privileged user access.

Reduce your attack surface. Simply put, an infrastructure’s attack surface is the aggregate of all means by which an attacker could gain unauthorized access to a system, make unauthorized changes and obtain sensitive data. To reduce your attack surface, IT must harden systems by configuring user access to only those applications, services, ports and protocols that are deemed necessary to the business. After doing so, IT must continuously monitor and assess these systems to ensure they remain configured to best practices.

A wide variety of enterprise IT security software is available to manage, monitor and enforce configuration best practices for systems directly connected to your network. When planning for a move to the cloud, you must review each of these pieces of software to determine whether they will still be effective in the cloud, where the cloud service provider may not support direct low-level access in the same way you do in your environment.

Leverage IT security frameworks. To help organizations achieve IT security best practices—and ultimately reduce network security risk—several organizations have constructed IT security frameworks (many of which are referenced in industry and government IT security regulations, such as PCI and FISMA) that incorporate guidelines for hardening the security configurations of firewalls, routers, switches, servers, desktops, laptops and mobile devices. Some of the more common IT security frameworks are:

- SANS 20 Critical Security Controls
- NIST SP 800-53
- ISO 27001
- COBIT

Leading secure configuration management solutions incorporate policy templates for all four of these frameworks. Users can leverage dashboards and reports that identify out-of-compliance hosts and review instructions for remediating hosts back into a compliant state.

Optimize privileged access. When it comes to granting administrative privileges to IT personnel, most experts agree that organizations should follow the "principle of least privilege." Least privilege dictates that users should be granted the lowest level of user permissions they can have and still do their jobs. Unfortunately, not all platforms support the granular privileges required to grant least privilege, and many platforms make it very difficult to configure and manage those privileges. Also, least privilege alone doesn't reduce risks from overburdened or ill-intentioned IT personnel. By leveraging leading privileged account management technology—installed both on-premises and to cloud-based platforms and services—IT organizations can grant permissions to IT personnel through granularly defined roles, with each role assigned one or more entitlements (permissions). And to prevent unauthorized user privilege escalation, better privileged account management solutions incorporate dual-key security, requiring two IT administrators to confirm privileged account escalation.

Step 2: Improve Threat Response

With the security configurations of on-premises and third-party providers (such as IaaS providers) hardened and your privileged user accounts optimized, the second step to sustaining security and compliance in the cloud is to improve your threat response. You can accomplish this by detecting threats from within your hybrid infrastructure, correlating those threats against intelligence generated by your other security defenses, and monitoring privileged users for potential access violations.

Detect threats from within. When it comes to detecting cyber threats that target your cloud-based hosts, your cloud provider's firewall and IPS are your first line of defense. But as today's most damaging threats target zero-day vulnerabilities, you can't rely alone on your cloud vendor's traditional perimeter defenses.

Rather than focus protection on a perimeter that now extends well beyond traditional borders, security teams need to target security controls at the data itself—wherever it may reside. Data-centric approaches to threat defense, the classic examples being encryption and tokenization, are among the most effective ways to protect critical data and meet compliance objectives. Security teams should extend the data-centric approach to the sensitive systems and users that regularly access and interact with critical data. Examples of data-centric security solutions that focus on sensitive systems and users are those that monitor privileged user activity for unusual behavior or unauthorized access to sensitive files, or that monitor security events and changes in real time to detect accidental or malicious changes to sensitive files and systems.

By adopting a data-centric approach, security teams can more effectively and proactively detect potential threats and mitigate risk to sensitive data and systems. This approach enables teams to reliably achieve security, compliance and business objectives—even when the IT environment is becoming increasingly complex due to the adoption of disruptive technologies such as cloud.

Integrate your security defenses. Enterprise adoption of SIEM technology has exploded in the past decade. Unlike basic log monitoring solutions that merely aggregate logs, SIEM solutions integrate and correlate intelligence from all your security defenses—both on-premises and in the cloud—to provide IT with a single control panel for responding to everyday security events and uncovering advanced attacks that may otherwise go undetected. Leading SIEM platforms also offer tight integration with change monitoring solutions to deliver richer security intelligence and to enable faster response.

Monitor privileged access violations. Leading privileged user management offerings not only enable IT to group privileged users into roles, but they also log privileged user activity into a secure, read-only archive. This provides a detailed audit trail of all privileged user actions, including attempts

to access unauthorized systems—whether on site or in the cloud at a third-party provider, such as an IaaS provider—which can be telltale signs of privileged accounts being compromised during an APT or other targeted attack.

Step 3: Reduce the Compliance Effort

The third and final step to gaining visibility and control over your cloud infrastructure is to reduce the effort of achieving and sustaining compliance with industry and government regulations, such as PCI, HIPAA, FISMA, SOX, NERC, and others. You can accomplish this by adhering to relevant IT security frameworks, leveraging the policy library within your secure configuration management solution and automating compliance reports and alerts.

Adhere to IT security frameworks. As mentioned in Step 1, many industry- and government-mandated IT security regulations reference best practices found in common IT security frameworks. By leveraging best-of-breed FIM and secure configuration management solutions—both on your physical networks and in the cloud—your organization can adhere to relevant IT security frameworks, which in turn reduces the effort of achieving and sustaining regulatory compliance. Here are examples of IT security frameworks and the IT security regulations that reference them:

- SANS 20 Critical Security Controls referenced by PCI
- NIST SP 800-53 referenced by FISMA
- COBIT referenced by SOX

Leverage secure configuration management policy templates. A secure configuration management policy consists of individual “tests” (and groups of tests) that describe the intended state of a specific host’s configuration settings. Better product offerings incorporate policy libraries—collections of preconfigured tests—that correspond to all major industry and government regulations, including those already referenced in this document.

By mapping secure configuration management regulatory policy templates to both internal and cloud-based hosts affected by IT security regulations (such as hosts that process credit card transactions), IT can dramatically reduce the effort of achieving and sustaining regulatory compliance.

Automate compliance reporting. Most leading information security products—especially those with specific roles in achieving regulatory compliance—offer canned reports to help demonstrate compliance with industry and government regulations. Better security solutions automate the compliance reporting function, resulting in compliance reports automatically delivered to internal auditors and IT management personnel.

How NetIQ Can Help

Today’s cyber threat landscape is constantly evolving, and so are the industry- and government-imposed regulations faced by enterprises and federal agencies. Without the right tools in place, achieving and sustaining security and compliance in the cloud (or, for that matter, on physical networks) can be a daunting task. Thankfully, NetIQ can help.

We understand that traditional approaches to mitigating data security and compliance risks are no longer effective by themselves and that you require a comprehensive solution. Our suite of identity, access and security management solutions integrate seamlessly to help you control access to cloud services and data, reduce your risk of data breaches in hybrid environments, and achieve compliance with industry regulations and security policies in the cloud.

Let's review five key NetIQ products and discover how each contributes to the three aforementioned steps to achieving and sustaining security and compliance in your enterprise so you are prepared for the advent of cloud.

NetIQ® Change Guardian™

NetIQ Change Guardian provides privileged-user activity and change monitoring to help IT professionals detect and respond to potential threats in real time. The solution alerts you of changes throughout your distributed environment, offering detailed insight into Active Directory, files, directories, file shares, registry keys (on Windows hosts), system processes and more. The alerts also indicate whether an action was authorized, and include before-and-after details of the change. NetIQ Change Guardian delivers enriched security information with the detail necessary to identify threats and record change, providing greater fidelity and clarity than native log events alone.

NetIQ Change Guardian helps organizations secure their hybrid infrastructures and maintain regulatory compliance through the following capabilities:

- **Privileged-user monitoring**. Logs the activities of privileged users, such as network architects and administrators, to reduce the risk of insider attacks.
- **Real-time change monitoring**. Monitors changes to critical files, platforms, applications and systems in real-time to prevent breaches and ensure policy compliance (includes file integrity monitoring).
- **Unauthorized change alerts**. Provides intelligent alerts upon detecting unauthorized changes potentially related to an APT or other targeted attack. The alerts deliver the detail necessary to identify threats and record change—specifics such as *who* performed the action, *what* action was performed, *when* the action was taken, and *where* the action was taken.
- **Compliance reporting**. Delivers reports automatically to demonstrate your ability to monitor access to critical files and data and satisfy industry and government compliance mandates.

NetIQ Secure Configuration Manager™

NetIQ Secure Configuration Manager enables periodic assessment and reporting of system configuration changes and matches that configuration against regulatory requirements and best practice policies to help ensure compliance with SOX, PCI, HIPAA, FISMA, NERC and other regulations. Its user entitlement reporting assesses user permissions, providing you with information on who has access and what level of access they have to critical information, helping to reduce insider threats.

NetIQ Secure Configuration Manager plays a pivotal role in securing hybrid infrastructures and demonstrating compliance with IT security mandates through the following capabilities:

- **Configuration assessment**. Provides customizable policy templates that align with dozens of IT frameworks and regulatory standards and continually compares current system configurations against known-good baselines. Helps to reduce your network's attack surface and demonstrate compliance.
- **User entitlement reporting**. Assesses user permissions for access to critical systems, helping auditors understand who has access to what level of critical information.
- **Business exception management**. Helps suppress configuration alerts in instances where certain systems must legitimately deviate from approved configuration standards and documents the rationale for such exclusions.
- **Security and compliance dashboards**. Conveys, through customizable dashboards, the security and compliance posture of systems quickly and intuitively, meeting the needs of multiple stakeholders.

NetIQ Privileged User Manager

NetIQ Privileged User Manager limits unauthorized transactions and access to sensitive data by delivering privileged-user management and tracking across all Windows, UNIX and Linux environments. It works by allowing administrators to centrally define the commands that privileged users are able to execute on platforms, ensuring only authorized users can perform specific administration tasks.

NetIQ Privileged User Manager works to secure sensitive assets and demonstrate compliance with industry mandates through the following key capabilities:

- **Simplified policy management.** Allows you to centrally create security rules via a web-based console, then enforces them across all managed UNIX, Linux and Windows systems.
- **Proactive risk management.** Records and plays back user activity—down to the keystroke level—with powerful risk-analysis tools.
- **Continuous compliance.** Provides permanent audit records and automated data filtering to prove compliance. Automatically adds changes to the permanent audit record, and filters data to ensure high-risk events are immediately visible.

NetIQ Directory and Resource Administrator™

A full-featured privileged account management solution, NetIQ Directory and Resource Administrator mediates access to Microsoft Active Directory, limiting users to particular actions for specific views of the overall directory. It also supports user provisioning and other automated tasks while helping to enforce security policies and segregation of duties.

NetIQ Directory and Resource Administrator helps to secure assets and demonstrate regulatory compliance through the following capabilities:

- **Granular access controls**. Helps you granularly assign Active Directory permissions to IT users through more than 60 roles and 300 powers.
- **Privilege escalation control**. Prevents unauthorized privilege escalation through dual-key security, requiring two Active Directory administrators to confirm changes to users' permissions.
- **Controlled self-service tasks**. Reduces costs by enabling end users to update their personal directory information and reset their own passwords.
- **Centralized activity logs and reports**. Demonstrates regulatory compliance through centralized logging of all administrative actions and flexible, comprehensive reporting.

NetIQ Sentinel™

NetIQ Sentinel is a full-featured SIEM solution that simplifies the deployment, management and day-to-day use of SIEM technology. NetIQ Sentinel readily adapts to dynamic enterprise environments and delivers the true actionable intelligence security professionals need to quickly understand their threat posture and prioritize response—both on-premises and in the cloud.

NetIQ Sentinel enables security analysts to monitor system integrity while affording auditors with the comprehensive reporting needed to consistently demonstrate regulatory compliance. Key capabilities include:

- **Security intelligence aggregation**. Aggregates log data and other security and network intelligence from across your entire IT environment, including firewalls, AV, IPS devices, secure email and web gateways, data-loss prevention (DLP) systems, applications, databases and much more.
- **Anomaly detection**. Automatically identifies inconsistencies in your organization's physical, virtual and cloud environments through powerful vendor-supplied and customer-created

correlation rules. Let's you baseline "normal" network traffic and detect anomalies potentially pointing to threats.

- **Identity enrichment**. Ties specific activities and security events to users across the enterprise through integration with NetIQ Identity Manager.
- **Simplified compliance reporting**. Automates tedious compliance reporting functions to satisfy the needs of both internal and external compliance auditors.

Conclusion

Cloud computing is changing the way businesses and government agencies deliver IT services to the users they serve. However, despite providing cost reductions, increased scalability and improved business agility, cloud computing can exacerbate the challenges of securing critical systems and demonstrating compliance with industry and government regulations. The increasing use of cloud and other business-enabling technologies can push your already complicated IT environment to its limits, adding unprecedented interdependencies and integrations with third-party providers.

Organizations can safely reap the benefits of a cloud-computing infrastructure by first implementing the aforementioned three-step process within their own on-site environment. Once you've achieved this, it becomes more straightforward to extend the right controls and processes into the cloud as needed. By following this process, organizations can gain back the visibility and control they need to effectively secure their sensitive data within hybrid environments that consist of on-site and third-party provider systems. They can also maintain the regulatory compliance they've worked so hard to achieve.

NetIQ's award-winning security and compliance solutions work in concert with each other—and your existing IT security infrastructure—to help your organization achieve and sustain security and compliance, even in a cloudy world.

About NetIQ

NetIQ is a global enterprise software company that meets the demands of hybrid IT with solutions for identity and access management, security and data center management. Using our solutions, customers and partners can capitalize on the opportunities in today's complex and ever-changing IT landscape. By aligning technologies and service delivery methods, our customers are better able to provide strategic value at the speed of business.

Learn more about our award-winning software solutions at www.netiq.com.

 562-A41014-001

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.**