NetIQ

Solution Flyer
Identity-Powered Security

Identity-Powered Security

Balance user convenience with reduced organizational risk.

Identity-Powered Security at a Glance:

- **Identity Governance and Administration:**
  NetIQ's identity management capabilities help you efficiently provide appropriate access permissions so users can do their job.
- **Access Management and Authentication:**
  Matching authentication requirements with the risk associated with the access request ultimately serves to minimize the risk that insider credentials are being abused by outsiders.
- **User Activity Monitoring:**
  The activities of privileged users must be scrutinized, because gaining access to privileged accounts can potentially expose an organization to great risk.

The Tight Link between Identity, Access and Security

Identity and access management is disconnected from security management in many IT organizations. Traditionally, identity and access management has focused on getting business users the right access to do their jobs, regardless of complexity from cloud and mobile apps, while security teams have focused on defending the organization from external and internal threats.

But both want the same thing—to protect sensitive information from misuse or theft using a method that is transparent and convenient for users. And both teams have capabilities that would be useful for the other.

Users Are the Weakest Security Link

Business users demand access to anything from anywhere on any device, exposing organizations to greater risk. Malicious or careless employees have always provided some risk, but now external attackers are using social engineering, spear phishing and custom malware to obtain insider credentials, particularly from privileged users with elevated credentials. The 2015 Black Hat Hacker Survey reveals that 45% of hackers report that privileged account credentials are their most coveted target asset, giving them the most direct access to sensitive data. Once insider credentials are acquired, attackers can access and exfiltrate information undetected for weeks or months, because activity associated with legitimate credentials is often undetected by security monitoring systems that aren't focused on the everyday work habits of insiders doing their jobs. With no way to tell if an insider is truly who they say they are, users have become our greatest security risk.

Businesses Demand a Return on Access Governance

Besides the need to provide secure, convenient access for users, regulations mandate companies demonstrate they are appropriately governing user access to critical systems and data, or face fines. Because of this, access governance programs have evolved into a tedious, misunderstood compliance project to appease auditors. The result of this is rampant rubber-stamp approval of every users' privileges whille vulnerabilities remain. According to the most recent Ponemon Cost of Cyber Crime Study, half of all organizations surveyed have invested in access governance, the top security enabling technology deployed. But it falls to fourth on the list in terms of ROI, coming in at a meager 13%.

CFOs want to know that they're getting a return on their access governance spend. One metric that will indicate this is the number of access revocations that take place following an access review by line of business managers, resulting in actual risk reduction. To increase revocations, better information and risk-based prioritization needs to be provided to busy business managers, so they understand the implication of certifying high-risk access.

Address Risk While Satisfying User Demands

NetIQ® is helping organizations address risk and complexity, from both privileged and regular users, with an integrated set of solutions for managing the identity and access lifecycle, authentication, access governance, privileged users and accounts and security monitoring. We call our approach Identity-Powered Security, and it consists of three complementary disciplines:

Identity Governance and Administration—NetIQ's identity management capabilities help you efficiently provide appropriate access permissions so users can do their job. Smart, yet simple access governance enforces the least privilege principle which helps to reduce separation of duty violations from users with "access creep," a common problem when employees

accrue access for special projects or when changing roles. Minimizing user permissions to only what is appropriate is a proven method to help reduce compliance violation fines and thwart potential insider attacks.

Access Management and Authentication—As local, remote and mobile users interact with business applications, the way they authenticate must be contextually controlled to minimize the hassle. Simple credentials (such as username and password) may be appropriate for low-risk authentications, but as the risk context increases, there may be a need to request additional credentials or step-up authentication. Matching authentication requirements with the risk associated with the access request ultimately serves to minimize the risk that insider credentials are being abused by outsiders.

User Activity Monitoring—Finally, we must monitor activity because we know some insiders will abuse their privileges, and we have to assume that well-funded, creative attackers will eventually gain insider credentials. In particular, the activities of privileged users must be scrutinized, because gaining access to privileged accounts can potentially expose the organization to great risk. By monitoring what users or machine accounts are doing with their access, using identity as a key source of context, we can identify abnormal activity patterns with analytics to reduce event noise, find the real threats, and take decisive action to disrupt attacks.

NetIQ, Identity and You

NetIQ is the world's leading provider of integrated Identity, Access and Security Management solutions. Every day, we use our broad experience and expertise to help customers respond effectively and rapidly to their most demanding users, auditors and complex threats by giving them visibility and control of access to sensitive assets and services—wherever it is, and whoever the user is.

NetIQ can help you to achieve Identity-Powered Security by providing the tools you need to aggregate identity information from across your IT infrastructure, and integrate this information into your security monitoring tools, delivering the essential "identity context" teams need to recognize—and address—potential attacks faster than ever before thought possible.

Visit **www.netiq.com** to learn more about NetIQ's identity, access and security solutions.

NetIQ provides identity, access and security solutions in the following categories to deliver Identity-Powered Security, with a special emphasis on privileged users.

Identity Governance and Administration	Access Management and Authentication	User Activity Monitoring	Privileged Identity Management
Manage rights so users have access to what they need and nothing more.	Authenticate that users are who they say they are, providing convenient and secure access across cloud, mobile and enterprise apps.	Enrich security monitoring with identity and access information to provide insight needed to detect and disrupt attacks and minimize damage.	Manage privileged identities to enforce appropriate use of their access rights.
■ **Self-service access request and approval**	■ **Step-up authentication based on risk**	■ **Enrich security monitoring with identity**	■ **Delegated administrative rights for privileged users**
■ **Identity and access provisioning**	■ **Multi-Factor authentication**	■ **Detect and disrupt suspicious user activity**	■ **Enforce access controls for privileged users**
■ **Access governance and certifications**	■ **Single-sign on across cloud, mobile and enterprise apps**	■ **Evidence user activity for compliance**	■ **Monitor and record privileged user activity**
			■ **Detect and disrupt misuse of privileged rights**
			■ **Comply with data access regulations**

www.netiq.com

Worldwide Headquarters
515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
+1 713 548 1700
888 323 6768
info@netiq.com
www.netiq.com
www.netiq.com/communities/

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