Closing the security intelligence gap

Integrated Identity, Access and Security Management

Emerging technology drives IT complexity

Despite steady investments in security, ever larger data breaches continue to dominate the news. Increasing IT complexity, driven in part by cloud, mobility, and social identity, impairs the ability of security teams to protect sensitive data because traditional approaches to identifying threats and responding to breaches are no longer effective against the latest generation of cyber-attacks. In the most lucrative data breaches, attackers will often acquire the credentials of a trusted internal user and then exploit vulnerabilities in the way we manage and monitor internal users with broad privileges.

A security intelligence gap that must be addressed

A strong defense against the evolving "inside threat" must start with the best practice of implementing more granular and business-appropriate access controls. Simply put, provide only the minimum rights required for all users and minimize the number of privileged users. Once these controls are in place, privileged users must be monitored to make sure their activities are normal and business-appropriate.

The problem with traditional approaches to security monitoring is that, as the IT infrastructure expands and more tools are added, even more security event "noise" is generated. Stretched-thin security teams are left with mountains of data to analyze and make sense of. In the "noise", the activities of privileged users are often lost and it's easy to lose track of what is normal user behavior. Security teams begin to miss critical indicators that may signify an attack. When security teams are unable to gain insight into activities and events that may signal a threat because of weak or missing security analysis, a security intelligence gap is said to exist.

The solution to this problem is an integrated approach to security that incorporates additional context about users and events into security monitoring solutions. Through analysis of contextual information, event "noise" can be reduced and abnormal activity can be detected. "Identity" is a key source of context for understanding what is normal behavior for users within an organization. When the user "identity" is integrated into security practices, users with inappropriate access rights can be identified, monitored and managed to avoid unnecessary risk from internal and external attackers.

Source: Cyberthreat 2015 Defense Report North America & Europe.

Build a strong defense with Identity-Powered Security

Identity-Powered Security is the integration of identity information into security monitoring and breach response. Using this approach, identity management, access management, and security event management work hand-in-hand to provide the full range of organizational knowledge around who someone is, what activity is normal for them, and what they need access to. Identity-Powered security helps teams cut through the noise of activity and quickly identify if the actions of a user are normal and acceptable, or unusual and

NetIQ

damaging. When enriched with this "identity context", security data is transformed into truly actionable security intelligence that teams can use to disrupt an attack and speed incident response before damage is done.

NetIQ, Identity and You

NetIQ is the world's leading provider of 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 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.

NetIQ is your partner in the delivery of Intelligent and Integrated Identity, Access and Security Management. Below are just a few of the ways we help our customers keep their information safe and their organization compliant.

Getting the Right Access, Fast	Limit the Risk from Privileged Users	Detect Breaches Faster	Report and Stay Compliant
• Automate identity, provisioning and approval processes so your people have appropriate access their first day on the job. • Immediately revoke access when an employee leaves or changes roles, to reduce the risk of data loss. • Ensure that least privileges are granted and enforced to comply with regulations, maintaining a consistent identity across all your systems. ***NetIQ Solutions*** • NetIQ® Identity Manager • NetIQ® Access Manager™ • NetIQ® CloudAccess	• Limit privileged access to Active Directory, Windows, Linux or UNIX systems and report on what administrators are doing. • Monitor changes to critical assets in real-time and include identity intelligence to make better security decisions. • Monitor and report on administrator activity for critical servers. ***NetIQ Solutions*** • NetIQ® Directory and Resource Administrator™ • NetIQ® Privileged User Manager™ • NetIQ® Sentinel™ • NetIQ® Change Guardian™	• Speed identification and disruption of threats before they cause damage by providing real-time event analytics. • Develop security intelligence for defense against future attacks. • Monitor privileged user access to files that contain sensitive data. ***NetIQ Solutions*** • NetIQ® Sentinel • NetIQ® Change Guardian • NetIQ® Privileged User Manager	• Monitor user activity and enforce IT regulatory compliance. • Detect, and automatically overwrite, changes to access policies and comply with IT regulations. • Demonstrate access governance and IT regulatory compliance, and automate review of access rights. ***NetIQ Solutions*** • NetIQ® Change Guardian • NetIQ® Secure Configuration Manager • NetIQ® Access Governance Suite • NetIQ® Identity Manager

Visit **www.netiq.com** to learn more about NetIQ's complete portfolio, including solutions for systems and application management, workload management and service management.

NetIQ, the NetIQ logo, Sentinel, Secure Configuration Manager, Change Guardian, Directory and Resource Administrator, and Access Manager are trademarks or registered trademarks of NetIQ Corporation in the USA. All other company and product names may be trademarks of their respective companies.

© 2015 NetIQ Corporation and its affiliates. All Rights Reserved. 1070SMC 2015 po