WHITE PAPER

Identity and Access Management: The Foundation for Secure, Efficient, and Compliant Enterprise Application Environments

Sponsored by: NetIQ

Sally Hudson
September 2011

IDC OPINION

Enterprise organizations are embracing holistic approaches as the next logical step in leveraging identity and access management (IAM) to achieve and maintain continuous security and governance, risk, and compliance (GRC) health. Critical elements include:

- Role-based lifecycle management
- Real-time audit and reporting capabilities with alerts
- Continuous policy enforcement and reporting
- Standards-based access control and automated password reset
- Automated user provisioning/deprovisioning

All of these capabilities must integrate easily with existing systems and data sources to secure businesses, support GRC initiatives, and create better business practices through IT efficiencies.

EXECUTIVE SUMMARY

IDC research shows that large organizations are looking to increase security, protect privacy, and achieve compliance as they move to embrace new technologies and continue to refine business processes. A key component of this strategy rests on IAM and GRC technologies. Global companies and international industries are looking for best practices that allow them to maximize investments in their current applications infrastructure — for instance, investments in SAP applications — and integrate them with industry-proven IAM and GRC solutions. This paper focuses on the SAP/NetIQ partnership and how it can benefit customers facing these challenges.

METHODOLOGY

Competitive intelligence data is collected by analysts in IDC's Security Products group on an ongoing basis. The information consists of public information gleaned from reports, SEC filings, non-NDA briefings, and conversations with industry contacts. It also includes both demand-side and supply-side research conducted by IDC on a regular basis.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

IN THIS WHITE PAPER

In this white paper, IDC outlines the particular advantages of an identity-driven, holistic approach to achieve security, efficiency, and compliance within the enterprise, with a specific focus on NetIQ (formerly Novell) SAP environments.

SITUATION OVERVIEW

Enterprise IT departments face escalating security and operational challenges. The majority of these challenges are posed by continual fluctuations in information, identities, and access points. This threat vector is created by distributed and mobile computing, increased consumerization of IT, and increased threats from internal and external sources. To combat these threats, organizations must coalign security and identity with GRC initiatives and update and review these areas on a continuous basis.

Enterprise organizations must also focus on meeting the demands of government and industry regulations. Today, these demands include the Health Insurance Portability and Accountability Act [HIPAA], the Gramm-Leach-Bliley Act [GLBA], the Sarbanes-Oxley Act [SOX], CobiT, ITIL, the European Union's DPD (EU DPD), Solvency II, EU Directives 136 and 140, Japan's JPIPA, and PCI DSS, among many others on an ever-expanding, international list. IDC research shows that European regulations on privacy and PCI DSS will continue to be implemented, will be more enforced by financial institutions or regulators, and will be more visible to the public. In addition to audit and certification, compliance is also monitored by regulatory bodies such as ICO (United Kingdom), CNIL (France), and AEPD (Spain) for privacy regulations. While all of these regulations have different specifications, they do have central themes in common: The regulations are designed to guarantee that only the people who *should* have access *do* have access to data and information.

Although cumbersome and complex, these regulations are necessary to help guard against loss and/or leakage of intellectual property, customer information, and highly sensitive content. It is critically important that governments and commercial corporations be able to certify that access control and access to information are continually monitored, enforced, and tracked for all entities accessing the system, from both inside and outside the company. This is essential to guarantee security, meet compliance, and assure customers and regulators that sensitive information is safe from misuse and corruption.

Identity and access management is the foundation technology used by organizations to build secure and compliant business processes and access control policies.

MARKET AND TECHNOLOGY TRENDS

Identity and access management is the who, what, where, when, and why of information technology. It encompasses many technologies and security practices, including secure single sign-on (SSO), user provisioning/deprovisioning, authentication, and authorization. Over the past several years, the Fortune 2000 and governments worldwide have come to rely on a sound IAM platform as the foundation for their GRC strategies. This is borne out by the numbers: *IDC research shows that the IAM market accounted for almost $4 billion in license and maintenance revenue in 2010, and we estimate that 80% of these sales were directly driven by the need to meet regulatory compliance mandates.*

This lays the foundation for the larger GRC infrastructure for the enterprise, an area where companies such as SAP and NetIQ (and Novell before it) have combined years of experience and expertise. IDC defines GRC infrastructure as focusing on solutions that provide policy and workflow definition; documentation; policy enforcement and operationalization; and monitoring, testing, and verification of controls at the IT infrastructure layer. It is an ongoing, dynamic process. As more organizations decentralize with branch and home offices, remote employees, and the consumerization of IT, the need for strong security and GRC practices is greater than ever.

As the number of highly publicized IT security breaches grows, the demand for more detailed audits and reporting requirements within organizations increases as well. This creates painstaking and time-consuming challenges for IT and business professionals required to perform the logging, reporting, and audit point processes necessary to meet SOX, GLBA, PCI DSS, EU DPD, Basel II, ITIL, CobiT, and the myriad of other regulations. The challenges extend to include access control, systems integration, transparency, automation, and remediation. Without the proper tools, the task soon becomes overwhelming and prone to mistakes, oversights, and deliberate shortcuts within companies.

IDC's position is that there is no single technology capable of solving all the security and compliance needs of an organization. To this end, IAM is increasingly used in conjunction with secure information and event management (SIEM) and GRC software to provide a comprehensive and holistic approach to enterprise security and compliance. SIEM solutions include software designed to aggregate data from multiple sources to identify patterns of events that might signify attacks, intrusions, misuse, or failure. Event correlation simplifies and speeds the monitoring of network events by consolidating alerts and error logs into a short, easy-to-understand package.

Implementing an IAM/SIEM/GRC infrastructure is not a do-it-and-forget-about-it process for IT because it involves an ongoing relationship with Human Resources and business managers. After discovery has taken place, roles have been defined, and access privileges have been granted or revoked based upon job function and division, ultimately these transactions must be validated and certified as being in compliance with policy and regulations. The ability to automatically pull access, control, and data usage information from various system sources and generate timely exception reports to be matched against policy is highly appealing to most corporations.

NetIQ and SAP: Synergies for Identity Infusion in the Enterprise

Following the Novell acquisition in April 2011, the legacy Novell identity, security, and compliance products are now sold under the NetIQ brand. NetIQ currently boasts a customer base of over 6,000 identity and security customers worldwide. It is focused on providing customers with solutions to securely deliver and manage computing services across physical, virtual, and cloud computing environments. NetIQ has built strong momentum through its industry-proven identity-based security solutions and its expanded partner ecosystem — two key components for future growth. Every year standards are amended and refined, and organizations must continually scramble to keep pace with the evolving nature of regulations. NetIQ has architected its identity and security management products to respond to situations in real time. The goal is to allow customers to act/react in a matter of seconds versus a matter of days and to correct problems in real time rather than on a reconciliation basis. This is a key differentiator in NetIQ's approach. IDC research has shown NetIQ to be a consistent worldwide market leader in IAM software solutions.

SAP, the international software giant based in Walldorf, Germany, has 53,000 employees worldwide and a customer base that exceeds 109,000, spanning all industries in over 120 countries. It is the largest ERP vendor in the world. As of early 2011, SAP reported a community of 2,400 partners worldwide. Part of the company's growth strategy includes co-innovation with partners, driven by ongoing investments in the partner ecosystem. IDC expects that most of this co-innovation will leverage existing partners and strategic acquisitions rather than a significant expansion of the partner community.

The legacy Novell/SAP relationship flourished for more than a decade. It began in 1999 when the companies initiated a Linux partnership and then expanded to include eDirectory in 2002. In 2009, Novell's IAM software achieved integration certification with SAP BusinessObjects business analytics software and SAP NetWeaver adaptive middleware for information and business process management across the enterprise. The legacy Novell, and now NetIQ, identity and security technologies are SAP certified on both platforms. There are currently 2,500+ mutual clients. This partnership allows NetIQ to address a number of challenges that SAP application owners and IT departments are facing today, including:

A constantly changing user population that needs access to SAP applications hosted internally, on the Web, and in the cloud

- Giving users appropriate access; provisioning them quickly to provide productivity (This is time consuming and labor intensive — especially if there are multiple instances of SAP applications to manage.)
- Providing appropriate access without compromising security
- SIEM for monitoring and remediating security and compliance events

As part of this effort, NetIQ's software solutions portfolio currently provides SAP customers with the following:

The NetIQ Identity Framework: A Single, Integrated Backbone

The NetIQ Identity Framework comprises the following components:

- **Identity Manager 4 Advanced Edition.** This software is capable of automating and managing literally thousands of user identities both inside and outside the enterprise. It enables complete control over the management, provisioning, and deprovisioning of identities in physical, virtual, and cloud environments. It can extend enterprise-compliant processes to SaaS applications securely and with sustainability and ensure that enterprise security policies are consistent across business domains. Identity Manager provides comprehensive, activity-level reporting on who has access to what and offers business-friendly user interfaces that map seamlessly into existing user interfaces. Importantly, it adapts to the customer environment (e.g., SAP NetWeaver) so that customers can retain their existing policies while adding intelligence for alerts when proposed changes conflict with current policy infrastructure.

- **Sentinel.** This product provides organizations with real-time visibility and intelligence into IT events to mitigate security threats, improve security operations, and enforce policy controls across physical, virtual, and cloud environments. Sentinel leverages the Identity management suite to deliver industry-proven user activity monitoring capabilities by tying users to specific events and quickly identifying critical threats. Sentinel can easily detect anomalous activities in a distributed or traditional IT infrastructure to speed remediation and build a strong security foundation. As an identity-aware security intelligence solution, Sentinel is well-equipped to address the advanced threat environment, improve operational efficiency, and streamline regulatory compliance processes.

- **Access Manager.** This software implements industry standards–based federation capabilities to give users a secure way to pass authentication information across domains. The software enables straightforward access to employees, customers, and partners using standards-based access management technologies that make it easy to securely share identity information across business and technical boundaries.

Access Governance Suite

This suite comprises three critically important components:

- **Access Certification.** This component includes the Compliance Certification Manager (CCM) and provides a complete, enterprisewide view of user access data so that organizations know exactly who has access to what. This is invaluable in preventing abuse and security breaches. Data is collected across manually provisioned, help desk–provisioned, and automatically provisioned systems. CCM ensures that user access to resources is appropriate and compliant with policies. CCM also streamlines review, certification, and reporting via automated processes, which reduces the risk associated with manual changes and reviews. It manages the entitlements associated with users throughout the user lifecycle, including when internal and external users join, move within, and leave the enterprise.

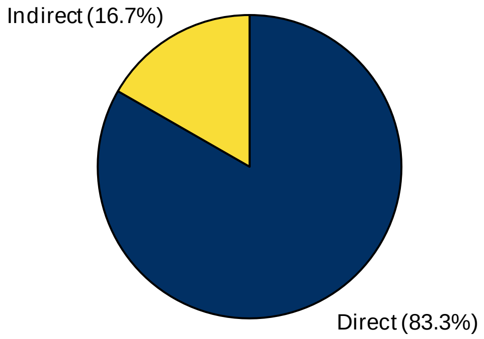
- **Role Lifecycle Management.** This software allows the review of access rights across automatically provisioned, help desk–provisioned, and manually provisioned systems. Roles Lifecycle Manager simplifies how user access is managed on a periodic/quarterly basis, giving visibility to patterns and logical groupings. This simplifies access change management and compliance. Roles Lifecycle Manager simplifies the process of making sure access rights are appropriate and provides access metrics to ensure that roles are used effectively.

- **Access Request and Change Management.** This component provides a self-service portal for the business and simplified mechanisms for granting access requests. The Access Request and Change Manager provides a single business-friendly interface with embedded governance (approvals, policy checks, escalations) through which IT professionals and/or line-of-business (LOB) managers can request and approve access rights. By enabling self-service access requests to the line of business, organizations can lower IT administration costs and streamline access delivery while maintaining compliance.

All of these products have been optimized to work within SAP enterprise environments and provide increased security, business efficiency, and the ability to meet detailed and granular compliance audits. Enterprise IT sites that rely on SAP software constitute a multibillion-dollar worldwide market today (see Figure 1).

FIGURE 1

Worldwide SAP Direct and Indirect Revenue Share for All Software



Total = €13.3B

Note: Data provided is estimated.

Source: IDC, 2011

The capabilities of the NetIQ/SAP platforms are illustrated by the following case study.

Customer Profile

CGT (Compagnia Generale Trattori)

CGT, based in Milan, is the official dealer of Caterpillar machinery and engines in Italy. CGT sells the entire CAT range of earthmoving and mining machinery, diesel engines, and industrial gas turbines. The company also provides value-add services to its clients, including technical assistance and parts, rental of machines, and resale of used equipment.

Challenge

With approximately 1,300 employees across 41 branches, CGT was finding it challenging to manage user identities and access rights across dozens of different corporate applications and databases. CGT had merged with another company to extend coverage to all of Italy, creating a company where 1,100 people were accessing the IT systems each day. To maintain security, create appropriate roles and access controls, and improve business processes, CGT needed to implement an automated user provisioning and deprovisioning system.

The company relies on SAP for all financial, sales, and human resource applications; on legacy iSeries for service and parts management; and on many applications deployed on Lotus Domino and legacy systems based on Oracle Database. Prior to the implementation of the NetIQ technology, updating a user's profile to reflect a change in personal information or to provide access to new applications was a manual process that required significant effort from the IT department because of the many different user directories. This created delays and left the business frustrated that its requests could take several days to execute. Equally, users were required to spend significant amounts of time logging in and out of systems, causing further frustration and inefficiency.

Solution

After evaluating several potential solutions from leading vendors in the IAM space, CGT decided to implement NetIQ Identity Manager, Access Manager, and SecureLogin. The ability of the NetIQ solutions to work across a broad variety of software environments — CGT uses the IBM i platform alongside Microsoft Windows and also has large Lotus Domino and SAP environments — was a key factor in the decision.

According to IT Manager Claudio Passoni, CGT needed a solution that would work with the company's heterogeneous environment and that would also provide prebuilt connectors to standard enterprise software such as SAP, iSeries, and Lotus Domino. To design, implement, and roll out its new identity and security management solution, CGT worked with three external partners. Unisys Italia was the lead partner and project coordinator, while Aglea handled the required modifications to CGT's SAP solutions. Net Studio was the principal implementation partner for the NetIQ technologies.

CGT was struggling to manage updates to employee profiles and access rights in a timely and efficient way. By selecting Identity Manager and Access Manager from NetIQ, the company has improved the speed and efficiency of identity management, enhanced security, and ensured that IT is more responsive to requests from the business and promptly aligned with organizational change. At CGT, the SAP installation is in four different directories across the company, creating a problem with the manual provisioning process from a time and accuracy perspective. The NetIQ software is allowing CGT to implement an automated roles-based access control system. This not only saves time and improves security but also allows the company to automate the attestation process to meet compliance rules and privacy regulations.

"The rules are being designed to reflect intercompany interactions," said Passoni, noting that CGT is working to build common base profiles, which will allow business chiefs to assign roles appropriate to each user and transaction.

CGT is also using SecureLogin to provide single sign-on capabilities to users across the network.

Results

Passoni and his team give NetIQ products high marks for ease of use and implementation. Using the Identity Manager and Access Manager solutions, CGT has:

- Created a single central repository for all user identity information
- Simplified and accelerated the setup of new users, saving time and effort
- Automated authorization updates due to organizational change
- Extended authentication over the Web, facilitating logins from remote locations

CGT and its partners are now rolling out the new NetIQ solutions across the entire company. Identity Manager acts as a central point of control over user identities that were previously managed in dozens of different directories and applications. Access Manager enables the company to extend authentication seamlessly over the Web, simplifying and securing remote work through enterprise portals. The deployment of Identity Manager has accelerated and largely automated the provisioning of new user accounts at CGT, reducing delays for employees and cutting the workload for the IT department. "With Identity Manager, we can create automated workflows to provision new users when they are created in the SAP Human Resources solution," said Passoni. "Setting up new users takes a matter of minutes, and when we make changes to user information, they are automatically synchronized across all connected directories and systems — so the NetIQ solution saves us significant amounts of time and effort."

FUTURE OUTLOOK

As companies embrace newer (e.g., mobile, cloud) technology to improve economies of scale and reduce operational expense, security and compliance issues will continue to be top of mind for C-level executives. All areas of IAM contribute to access control and compliance, including advanced authentication, Web SSO/federated SSO (WSSO/FSSO), enterprise SSO (ESSO), user provisioning, personal portable security devices, SIEM, and access governance. Secure access control is critically important because corporations and other entities must be able to track and report on "who had access to what when" and what they did with the data once they were there. Even if a company contracts with a cloud service provider, it is not exempt from compliance regulation responsibility.

Vendor success in this market will rest largely on partnerships and ecosystem building, as identity-driven infrastructure must be used in conjunction with GRC concerns and systems management capabilities. Again, no single entity has all the necessary pieces to the compliance and security puzzle. Further, as consumerization of IT blurs line between professional life and personal life, risk factors multiply yet again, making the need for holistic and proactive solutions that much more important from a security and GRC perspective.

CHALLENGES AND OPPORTUNITIES

NetIQ faces strong competition in the enterprise identity space. In the SAP market, this competition primarily comes from industry heavyweights Oracle, IBM, and CA Technologies. Further, newcomers with point solutions in certification and attestation could take focus away from a holistic solution approach.

NetIQ must continue to leverage its longstanding relationship and acquired expertise with SAP customers to demonstrate value. This can be seen through the customer deployments of easily integrated NetIQ Identity solutions and the realized ROI from these projects. Customers are looking for less, not more, complexity when solving compliance and security issues, and NetIQ has a proven track record with SAP in this area.

CONCLUSION

Enterprise organizations are leveraging identity solutions to increase security and achieve compliance while enhancing business productivity. SAP customers in particular can leverage the NetIQ Identity solutions to achieve these goals. Using the SAP-certified NetIQ Identity and Access Management and Access Governance software, SAP customers can realize benefits by:

- Easily integrating and protecting existing SAP investments
- Saving time and money by automating manual processes
- Realizing greater ROI in a shorter period of time
- Redirecting resources to other projects

Most importantly, SAP customers can use identity as a foundation to enhance security and simplify compliance in today's increasingly complex and vulnerable IT environment. This identity foundation allows enterprise IT to more easily build out additional capabilities to keep pace with the changing business and computing landscape. Importantly, the NetIQ software can be extended to protect enterprise systems beyond SAP to create a holistic corporate identity foundation.

Copyright Notice