

I D C V E N D O R S P O T L I G H T

Smart Identity Security: The Next Generation of Identity and Access Management

February 2006

Adapted from *Worldwide Identity and Access Management 2005-2009 Forecast and Analysis*, by Sally Hudson, Brian E. Burke, Charles J. Kolodgy, Christian A. Christiansen; IDC #33851 and "Knock Knock!" *Should You Let Them In? Identity Management/User Provisioning Deployment Considerations*, by David Senf; IDC #32545

Sponsored by A10 Networks

Widespread IT heterogeneity is preventing organizations from effectively securing and managing identities across data, applications, and other resources. The ability to manage access into these resources is cumbersome at the best of times. This makes it harder to ensure that only the right people get the right information at the right time. Reduced security, lower productivity, and higher administration costs result when resource accessibility is not (or cannot be) properly managed. This report examines the applicability of identity and access management (IAM) to support top business challenges, highlights the trends impacting both IAM solutions and identity data itself, and looks at the role of A10 Networks in simplifying and streamlining IAM and network security.

IAM and the Path to Interorganizational Federation

Regulatory compliance, security, and IT cost/complexity are among the most important business issues facing managers today. Identity and access management (IAM) solutions enable other solutions, such as Web services, to address these issues by driving more precise control over resource access across a disparate environment.

Moreover, as standards, technologies, and adoption change over time, the impact of IAM is expected to increase. In particular, a shift is starting to emerge in IAM as organizations federate customer, supplier, and partner identities from across the value chain. Both a standardized means of dealing with identity data and architectural/technology shifts are prerequisites to enabling interorganizational federation.

The identity and access management market is defined as a comprehensive set of solutions used to identify users in a system (employees, customers, contractors, et al.) and control their access to resources within that system by associating user rights and restrictions with the established identity. This is accomplished via implementation of some or a combination of the following technologies within an organization:

- User provisioning
- Advanced authentication
- Legacy authorization
- Directory services

These are all critical components of an IAM solution.

The major market drivers for IAM include the increasing realization among IT and business professionals as to the benefits of centralized, IT-driven provisioning systems, and, of course, the move to comply with federal regulations. Government and industry regulations are putting unprecedented pressure on corporations to secure access to information and applications, not just with employees but also with customers, partners, and contractors. Moreover, budgetary and staffing constraints will continue to drive organizations to look for better ways to cost-effectively manage their security infrastructure.

IDC believes that identity and access management has emerged as a key component of a compliance platform. As such, compliance and corporate governance initiatives will significantly drive IAM software spending over the next 12 months.

IAM and Compliance

Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, and ISO 17799, among other legislation and standards, mandate a higher level of internal controls over data resources. For example, Sarbanes-Oxley outlines that CEOs and CFOs signing off on financial statements are in effect standing behind the effectiveness of instituted controls. Compliance with this particular regulation will, among other actions, lead to limiting access into financial and accounting records and supporting documentation, including email, word-processed documents, and spreadsheets.

In addition, privacy regulations, such as sections of Gramm-Leach-Bliley and California's Bill 1386, also impact the management of identities. Privacy compliance, like other regulations, requires an organization to safeguard its data. And like other security initiatives, privacy compliance can be considered within the context of both cost avoidance and cost savings. For example, exposing consumer personal information can cost both an industry as a whole and damage the reputation of an individual organization. Therefore managing privacy protection can and should be built into security projects to help diminish compliance costs.

Security and privacy are often considered to be two sides of the same coin, but this is mistaken. Compliance with privacy legislation has implications that extend beyond the realm of security, such as complaints resolution or individual access to personal information stored by an organization.

Privacy compliance intersects with records management, data retention, and business intelligence, among other technologies and processes. Also, it cuts horizontally across all business lines and vertically from frontline workers straight up to the board of directors.

Given regulatory constraints limiting who has access to what resources, adding a layer to manage access rights is essential. Simplifying the processes of provisioning (activating and deactivating) user accounts is an important part of preventing unauthorized access, as it restricts the availability of certain resources to controlled groups of individuals. In general, IAM tightens the level of controls over applications and data resources within an organization. By building out user provisioning, which simplifies the granting and removal of data availability based on user access rights, organizations can begin to close the loop on security and privacy protection.

In short, IAM enables a higher level of compliance with regulations through tighter controls for defining who has access to which resources.

IAM and Streamlining IT Management

In addition to compliance, IAM is vital to reducing complexity, allowing business to be conducted with less friction. The mix of software, directories, operating systems, and databases built up over time has created interoperability challenges in many organizations, leading to a rise of complexity and cost in the delivery of IT. By consolidating user access, IAM relieves organizations from issues such as limited access to incompatible software. Furthermore, streamlined and automated account provisioning — of central importance to IAM — helps align resource access with user needs.

IDC sees IAM deployment delivering the following key benefits:

- Improved security through reducing systems exposure due to credentials remaining active longer than they should be
- Reduced complexity by consolidating and/or connecting identity information, including attributes, preferences, and access rights policies
- Reduced cost of employee/contractor churn through integrated workflow and provisioning of user access
- Reduced costs of waiting time for the provisioning of access to resources
- Reduced help-desk costs and lost productivity through delegation and self service

This last cost benefit can be particularly significant. In companies with strong password management policies, IDC estimates that about 20% of all help-desk calls are password-reset requests. In a large organization that receives hundreds of help-desk requests per day, password-reset requests become especially burdensome to support personnel. Moreover, each help-desk call can range from \$30 to \$70, depending on the help desk's geographical location (wages vary widely between U.S. and international locations). The volume and the resulting cost of password resets frequently make password resets a senior management issue.

User Provisioning: The Core of IAM

In basic terms, within the enterprise, IAM solutions automate and simplify the processes of activating and deactivating (known as provisioning) of accounts, access rights policies, cards, and other privileges from across the enterprise. Whether accounts reside with HR, IS/IT, or another department, managing the churn of employees and contractors is less costly from a systems and personnel perspective when delegated, automated, and mapped into the natural workflow of an organization.

Fundamentally, user-account provisioning relies on the ability to create replicable rules for repeatable and, in some cases, automated workflow. "Provisioning" is a term frequently used in IT for bringing a server or storage device online, but in the context of IAM, provisioning encompasses a complete life cycle of user access to resources. Because of this broad scope, reusable rules for defining the workflow throughout the IAM life cycle should garner a good deal of buyer attention. For instance, a new worker is hired, another changes position within the company, and yet another is terminated. As employees transition through this life cycle, a number of events must be triggered. In the case of a new hire or a termination, accounts and access rights to resources need to be either activated or deactivated across multiple systems.

Easing the burden of provisioning many users from across multiple systems is not only significant from a cost-savings perspective, but from a security perspective as well. IDC estimates that expired user accounts may be upward of 60% of all accounts currently active across corporate systems, which exposes the enterprise to serious security vulnerabilities. The provisioning of user accounts can help ensure a higher and more consistent level of security uniformly across enterprise resources, while keeping administrative costs in check.

By taking time- and cost-sensitive manual procedures and automating them, user provisioning can sharply reduce the costs of granting new employees, customers, partners, and suppliers necessary access. This is a key reason why, from 2004 through 2009, IDC predicts that the market for IAM will reach \$3.98 billion.

Considering A10 Networks

A10 Networks, a company founded in 2004 and headquartered in San Jose, California, has the stated mission of reducing IT complexity and enabling consolidation of IAM, wide-area network security, and application security functions. A10's IDSentrie product line is designed to address the business and technology issues previously described in this report, such as the need to accurately:

- Identify and authenticate users
- Simplify account, access, and network management
- Consolidate user identity and network/security functions
- Correlate user identity with user activity
- Enable user self-service and password synchronization

There are four major components to the IDSentrie technology platform:

- **Standard-based RADIUS authentication** has broad third-party data store support and flexible access policies for either realms, groups, or individual users. Central access control, logging, and reporting improve security and accountability, and increase security for legacy data stores
- **Unified identity manager** consolidates third-party data stores and unifies access provisioning and management. Complexity and overhead are reduced via user self-help functions, password synchronization, custom forms, and a dictionary map, improving operational efficiency and eliminating security holes and mistakes. Central password policy enforcement strengthens internal controls and accountability.
- **Identity event manager** correlates security device activity with authentication and identity information, providing comprehensive reports on user activity, resource utilization, and firewall policy violations. The analyzer supports most major firewalls and accelerates troubleshooting and forensic activity by revealing true user identity for critical traffic and events.
- **A correlated report engine for identity-based reporting** can produce more than 110 different reports across five categories — summary reports, events and alerts, bandwidth usage, protocol usage, and connections.

By integrating these four core components, the IDSentrie is able to simplify administration and user activities, consolidate and synchronize data stores, and correlate user activity with user identity. The components reportedly may be run individually or combined in any order, as well as integrated with existing IAM solutions.

The symmetric multiprocessing (SMP)-based appliance reflects A10's strategy of consolidating identity management with security and network infrastructure to produce best-of-breed performance and functionality. This consolidated and integrated approach to IAM is intended to lower total cost of ownership and produce faster return on investment. Unifying multiple technologies enables A10 to offer an economical identity management solution that represents a new price/performance benchmark in this market segment.

Challenges

IDC believes that the market demand for A10's solutions will remain strong in the near future, but the ability to quickly and easily demonstrate value in the following areas will be key to strengthening the company's position:

- Increased ability to meet compliance regulations
- Use of a consultative approach to client problems
- Business value through flexibility in deployment scenarios
- The provision of industry-specific templates and documented best practices
- Overcome the cost barrier of IAM, which has been an adoption inhibitor for many companies

Conclusion

The IAM market will continue to address some of the most burning business issues that organizations face today — that is, how to create and manage user access to a broad range of IT and physical assets, ranging from client/server and legacy software applications to telephone systems and buildings or offices. For example, IDC believes that IAM will provide the critical authentication and authorization infrastructure for Web services security.

Beyond Web services, however, organizations must take a holistic approach to safeguarding enterprise resources. When it comes to securing information, people — whether forgetful, neglectful, or malicious — are often the weakest link. Processes, such as approval of access to data and applications, need to be understood by employees and baked into the security architecture. In addition, achieving greater compliance through security technology involves making sure that only the right people have access to only the required information.

IAM significantly reduces the impact of human error by removing requirements for end-user input and by delegating to the appropriate people (those "in the know," such as managers) the assignment of access rights. Moreover, checks against user error are strengthened through an approval process for the assignment of resource access. Additionally, there are numerable vulnerabilities to be considered within an overall security strategy, such as closing ports when unused, patching systems, and using good password and key management. IAM helps shrink the attack surface through user account provisioning, account discovery, and password reset and consolidation/synchronization.

IDC believes the IAM market will increase in importance and growth, and to the extent that A10 Networks can address the challenges described in this paper, the company should enjoy continued success.

A B O U T T H I S P U B L I C A T I O N

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

C O P Y R I G H T A N D R E S T R I C T I O N S

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

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