
Centrify Adds Value to Active Directory - And the Business

Date: June 2007

Author: Jon Oltsik, Senior Analyst

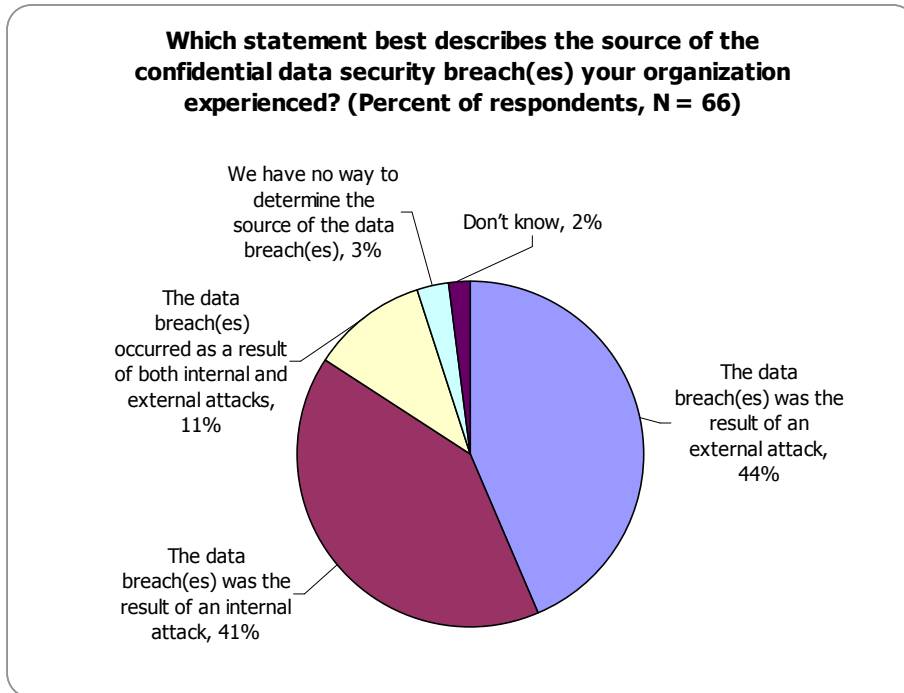
Abstract: Business initiatives, regulatory compliance requirements and security concerns are prompting businesses to invest in Identity and Access Management (IAM), but they often face a difficult choice between limited point tools and adding a complex IAM infrastructure. Centrify may have a better mousetrap. The company builds middleware that makes Microsoft Active Directory the IAM boss of UNIX, Linux, Macintosh and web application systems, providing a simple but powerful solution.

Overview

The application of Identity and Access Management (IAM) is in a state of transition. In the past, IAM tools were used primarily to streamline IT operations and lower cost. Great benefits, but not seen as core to the business. In today's business climate, however, IAM has become a mission critical requirement. Why? Because large organizations must be able to deal with:

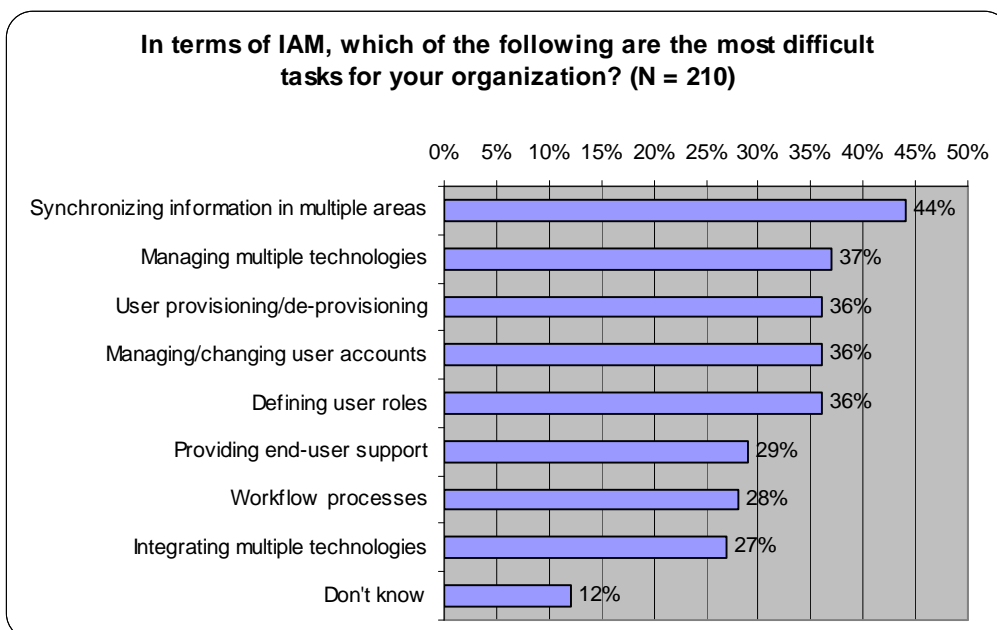
- **External users.** Enterprise networks are now "open for business" to external parties like customers, business partners and suppliers. To enable these outside constituencies, IT managers must have the ability to provision new user accounts to multiple systems quickly or set up federated identity relationships with peripheral organizations.
- **Regulatory compliance mandates.** Government and industry regulations such as Sarbanes-Oxley, HIPAA and PCI place new demands on enterprises to audit, log and report on user activities. The CIO may find himself in hot water when the SEC asks for specific information about user access and activity patterns and he responds with reports detailing IP address leases and network traffic patterns.
- **Increasing security threats.** ESG has found that of those organizations that have experienced a data breach in the past 12 months, 41% say that the breach was the result of an internal attack while another 11% claim that the data breaches resulted from both internal and external attacks (see Figure One). To counter these types of threats, CIOs need a combination of tight access controls and detailed auditing tools that can be used to track user activities and streamline forensic investigations.

Figure One: Origins of Data Breaches



Unfortunately, accomplishing these tasks can be extremely difficult as IAM activities are done in IT silos all over the enterprise. This creates an IT operations challenge as administrators are forced into a pattern of redundant operations and administration. According to an ESG Research survey, when asked to identify the most difficult IAM tasks, security professionals pointed to managing identity information spread throughout the enterprise, synchronizing individual technologies and provisioning/de-provisioning users (see Figure Two).

Figure Two: IAM Difficulties



Existing Solutions Are Limited

In spite of these escalating requirements, IAM tools have been around for years, so it would be safe to assume that there is an abundance of technologies available to solve these vexing problems. Not exactly. To meet business requirements, IT executives need solutions that can be deployed quickly, integrate with existing identity repositories and scale across the enterprise. Unfortunately, many IAM solutions don't meet this profile because:

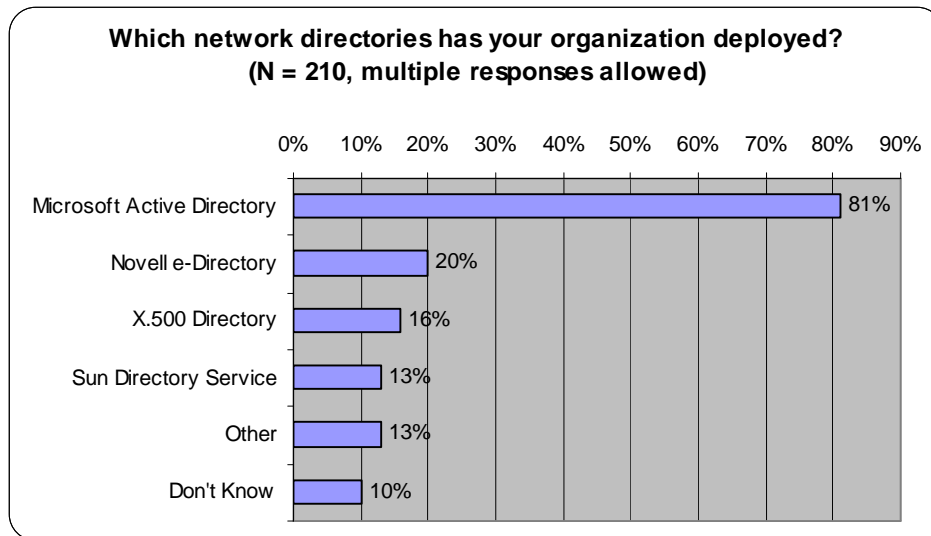
- **Point tools can't scale.** There are certainly plenty of IAM utilities and point tools available to address tactical issues. Some can add detail to Microsoft Active Directory reports, while others can translate schemas between multiple identity repositories. Sadly, a true enterprise solution would require a multitude of independent point tools creating more IAM islands and a management nightmare. In this scenario, IT operations, security managers and auditors would be left with the tedious task of piecing together multiple tools and reports in order to get a complete picture of enterprise activities.
- **Networking solutions can't see beyond the OSI stack.** Like point tools, network management systems offer only a partial solution. In the network world, users are equated with IP addresses, ports, protocols and connections. For example, I may be able to see that IP address 192.168.1.1 connected to another system while speaking HTTP over Port TCP port 80, but this information is just technobabble to concerned business managers. The burden of translating this networking minutia into business context remains a cumbersome, manual process.
- **IAM suites are expensive enterprise projects.** With no place else to turn, many IT managers opt for IAM suite solutions that layer a completely new IAM infrastructure across enterprise IT. While these solutions may ultimately work, they can take years to implement and carry millions of dollars in product and services costs. The CEO won't be pleased when she commits \$5,000,000 to an IAM project only to find out that new business initiatives can't be supported for another 3 years.

The Centrify Alternative: An IAM Middleware Bridge to Microsoft Active Directory

With business, compliance and security requirements growing daily, CIOs pine for an alternative to today's inadequate IAM offerings. Fortunately, attractive alternatives are emerging. One such option comes from Centrify, a venture-backed startup located in Mountain View, California. The Centrify management team is no stranger to IAM. In fact, the group has roots in early IAM pioneers such as Computer Associates, Microsoft, Netscape, NetIQ, Novell and others.

Centrify employs a simple but elegant approach, building middleware tools that bridge AAA (authentication, authorization and auditing) to Microsoft Active Directory—a foundational service in most enterprise networks. What's so special about AD? After years of experience, large enterprises have refined Active Directory implementation and strong AD administration skills. Centrify products can act as software glue between this existing stronghold and burgeoning IAM requirements. ESG Research indicates that this is a particularly shrewd move since AD is a staple at most large organizations—a whopping 81% use Active Directory, which is four times the size of the next closest response (see Figure Three). As a result, building on top of a ubiquitous platform like Microsoft Active Directory should certainly appeal to the majority of enterprise organizations.

Figure Three: Network Directories Deployed



Centrify approached the IAM market in two phases. The company's initial product is called DirectControl, an IAM middleware bridge between Active Directory on one side and UNIX/Linux, J2EE, web platforms and Apple Macintosh systems on the other. In effect, what DirectControl does is turn these heterogeneous systems and applications into Active Directory clients, thus extending standard AD administration and functionality. With DirectControl in place, AD becomes the nexus for cross-platform authentication, access control and group policy. IT managers can centrally provision/de-provision users in AD rather than in multiple systems independently. This leads to IAM efficiencies and improved security. Users also benefit as they can authenticate solely to AD, rather than multiple times to various systems and applications.

With DirectControl as a base, Centrify added deep auditing capabilities with its recent introduction of DirectAudit. DirectAudit takes advantage of the Centrify agent located on UNIX/Linux systems to capture user activities on those systems. In this way, Centrify can provide a useful audit trail and replay capabilities for compliance audits and forensic investigations.

Together, DirectControl and DirectAudit can help address some of the most troublesome IAM issues related to accommodating external users, meeting regulatory compliance mandates and improving internal security. CFOs and CIOs will also be pleased that Centrify middleware is easily deployed and far less costly than an enterprise IAM suite. In this way, Centrify can begin to deliver business value in the immediate term.

The Bottom Line

Business pressures demand IAM improvements, but this isn't easy. Today's IAM infrastructure is a jigsaw puzzle of identity repositories and silos, so piecing together a cohesive view can be a time consuming, manual process. Management tools can help, but most are either too narrow, exceedingly expensive to purchase or overwhelmingly difficult to deploy.

The Centrify recipe is simple: make the tools you already count on more productive by extending their reach and capabilities. Centrify layers its authentication, access control and auditing sauce on top of ubiquitous Active Directory to make this happen. This makes Centrify one of those rare companies that figured out how to add a whole lot of additional value without a lot of ripping, replacing, re-architecting or training.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc and is intended only for use by Subscribers or by persons who have purchased it directly from ESG. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.