A *Podcast Briefing* produced by SearchSecurity.com

Key Trends in the Identity and Access Management Market and How CA IAM R12 Suite Addresses These Trends

TechTarget
The IT Media ROI Experts

Sponsored By: CA

SearchSecurity.com

Key Trends in the Identity and Access Management Market and How CA IAM R12 Suite Addresses These Trends

a Podcast Briefing presented by David Kirkdorffer and Michelle Waugh

■ This *Podcast Briefing* is based on a CA/TechTarget Podcast: "Key Trends in the Identity and Access Management Market and How CA IAM R12 Suite Addresses These Trends."

Introduction

A digital identity generally consists of an identifier and a means of authenticating that identifier. In the early days of computing, identity and access management (IAM) was largely limited to maintaining a repository of user identifiers and associated passwords. These digital identities allowed a user to access a given system with all its associated applications and data. As systems and networks became more complicated, those identities were sorted into roles, and access and privileges were granted or limited based on those roles.

Systems and networks are now much larger, with more users and applications, and IAM security has therefore become much more complex. The exponential growth of IT resources has created a major challenge for IAM implementation: many enterprises have experienced a proliferation of independent systems, with individual identity management stores and protocols for different groups within the enterprise. This diversity of identity stores makes it difficult for IT to offer coherent and secure identity and access management. As a result, many enterprises are embarking on IAM initiatives to centralize and unify identity storage and management.

The IAM paradigm has shifted in recent years from the identity-based and role-based security paradigm to one of user-targeted access, increasing the scope of IAM to encompass all networked applications, services, portals, and content. IAM deployments need to specify how each user interacts with the system, providing access to only the applications and information that user needs.

The new IAM paradigm and the drive to centralization are due in large part to developments in the regulatory environment and in technology. Regulatory compliance has become a driving issue for many enterprises, especially for those that use and store identity-based data. Many companies began to examine their IAM technologies and to institute IAM initiatives due to new and updated regulatory laws, such as Sarbanes-Oxley (SOX), Data Protection Act (DPA) in the UK, the European Union Data Protection Directive (EUDPD), and the Health Insurance Portability and Accountability Act (HIPAA).

In terms of technology, service-oriented architectures (SOA), for example, bring together business processes and functionalities as services. Protocols designed around those services interlink them by describing how they communicate. Those protocols frequently require identity authentication for both the users and applications accessing them.

This document discusses the following questions:

- What is driving interest in IAM solutions today?
- What is the impact of service-oriented architecture on IAM, and how do these trends map to CA's IAM R12, the most recent release of CA's IAM security suite?

Inside...

Trends

David Kirkdorffer: IAM has been a major force in the enterprise IT marketplace for years now. What are the trends that are driving customer needs today?

Michelle Waugh: I see three major trends:

- IAM is being used more as a security infrastructure and is reaching into the lines of business to get them more directly involved in management.
- IAM makes compliance more proactive and cost-effective.
- IAM addresses new and emerging technologies such as service-oriented architecture (SOA).

Organizations are constantly seeking ways to enable better service at a reduced cost. The Web has been and continues to be a key area of investment for organizations. However, rather than viewing security as a reactive requirement, organizations are beginning to accept security as a core fundamental element of Web applications, a view that may be regulation-driven or simply forward-thinking risk mitigation.

Our customers are relying on their IAM systems to be highly scalable, meaning to millions of users and thousands of applications, while providing strong centralized control. In addition, customers want the flexibility of delegating across large numbers of non-IT administrators, allowing those lines of business to self-manage with appropriate oversight.

Security

Kirkdorffer: That sounds a bit complicated. With this growth, when hundreds or even thousands of Web applications are in use, how is IT dealing with this expanding security responsibility?

Waugh: For a long time now, IT has been finding ways to do more with less. In this case, IT is looking to the business to share in managing security policy. This makes a lot of sense in that those close to the business have a much better understanding of who should have access to what data or applications within their own organization. The key is to help non-IT people understand the structure and the effect of security policies in their own terms. That is one of the key aspects within CA's latest IAM R12 release. We have added a business layer that allows administrators to manage access in more business-friendly terms. This allows IT to delegate policy management, which is critical when there are many applications.

Compliance

Kirkdorffer: Another important trend you mentioned is making compliance more proactive and cost-effective. Can you talk more about this?

Waugh: One cannot discuss IAM security without talking about compliance. Compliance remains an enormous challenge. Today, most companies are worried about simply meeting their auditor's requirements, with less thought given to efficiencies. Passing audits has come at a very high cost, with a lot of manual processes. New regulations continue to appear. Most important, priorities continue to change as companies revalue with their governance and address regulatory compliance in a more comprehensive way.

Kirkdorffer: What has changed in terms of addressing this compliance challenge?

Waugh: Previously, most companies focused on auditing actions taken regarding their IT systems. This helps prove compliance controls are in place but after the fact or they are tracking down the sources of violation. While this is still important, companies are also taking a more proactive approach to identifying vulnerabilities before a breach actually occurs.

We have addressed this more thoroughly in our latest IAM R12 release by providing improved preventive and detective controls, and combining this with centralized auditing and logging. For example, an administrator using IAM R12 can identify what a particular user has access to. The administrator also can see some context so it is easier to understand what that access provides insight into or what role is assigned to the user, and therefore what access they are provided. The administrator can also look at information from a resource perspective, rather than a user perspective: the administrator can see what users have access to a given application and what are they allowed to do. IAM R12 provides the functionality for reporting on this information, scheduling those reports, and delivering them in various formats. This makes the job of complying and proving compliance easier, faster, and cheaper.

Service-Oriented Architectures

Kirkdorffer: How is IAM addressing the security of service-oriented architectures?

Waugh: IAM must expand its reach across the entire business infrastructure, including all the applications, forwarding platforms, and technologies as they are entering the mainstream. Supporting a service-oriented architecture for the use of Web services powerfully enables business agility. Like all other components in the infrastructure, these services must be secured. CA has just released a new product in our portfolio called CA SOA Security Manager. As SOA and Web services continue to emerge and be more vital elements in applications and enterprise infrastructure, companies have a critical need to centrally manage security and identities. It is just as important to cover security from end-to-end and enable easier and more complete compliance reporting, for SOA applications and Web services used within those applications, as it is for the more traditional aspects of IT.

Kirkdorffer: How does CA SOA Security Manager fit into CA's overall IAM solution?

Waugh: CA SOA Security Manager can be deployed and used separately. However, we also have clients that use it with CA SiteMinder®, which enables a very broad Web security solution, including Web access management, federation, and Web services security, all in the same infrastructure and the same policy system. This is a great example of how CA has built a comprehensive IAM solution: it can be used one module at a time, and as more pieces are put into play, the whole is greater than the sum of the parts.

Traditional Infrastructure

Kirkdorffer: What about traditional IT infrastructure? Is the need to secure and manage legacy systems being replaced by the Web?

Waugh: No. In fact many of our customers continue to have a strong dependence on traditional, or even legacy IT infrastructure, such as mainframes. Even with the emergence of the Web and new application architectures like SOA, historical systems continue to play a key underlying role, because deployed IT systems rarely go away. That is a key focus for CA. We are an independent software company without any of the underlying motivation toward one platform or one particular application infrastructure. Just as we have responded to trends in Web or distributed system security, we are continuing to invest in the mainframe, as is evidenced by our recent release of R12 Mainframe IAM solutions. We work closely with each of our customers to help them build an enterprise-scale, flexible, centralized security infrastructure that covers them from the Web back to the mainframe, and allows them to manage all their users, whether they are employees, partners, or customers. We help them to comply more easily and cost-effectively and to be more competitive in their own marketplace.

Conclusion

Kirkdorffer: Where would you suggest people turn to get more information?

Waugh: A good place to start would be www.ca.com/security, which has more IAM Podcasts and Webcasts, white papers, and solution briefs. Also on our site are some customer stories that describe how they have met their own big risk security or compliance challenges using CA's IAM solution.

■ **Michelle Waugh**—Senior Director of Product Marketing for Identity and Access Management Solutions at CA.

About TechTarget *Podcast Briefings*

TechTarget *Podcast Briefings* provide the pertinent information that senior-level IT executives and managers need to make educated purchasing decisions. Originating from our industry-leading Vendor and Expert Podcasts, TechTarget-produced *Podcast Briefings* turn Podcasts into easy-to-follow technical briefs, similar to white papers.

For inquiries and additional information, contact:
Dennis Shiao, Director of Product Management, Webcasts
dshiao@techtarget.com

About TechTarget

We deliver the information IT pros need to be successful.

TechTarget publishes targeted media that address your need for information and resources. Our network of technology-specific Web sites gives enterprise IT professionals access to experts and peers, original content, and links to relevant information from across the Internet. Our events give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Our magazines give you in-depth analysis and guidance on the critical IT decisions you face. Practical technical advice and expert insights are distributed via specialized e-Newsletters, video TechTalks, podcasts, blogs, and wikis. Our Webcasts allow IT pros to ask questions of technical experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events, the expert interaction of Webcasts, the laser-targeting of e-Newsletters, and the richness and depth of our print media to create compelling and actionable information for enterprise IT professionals.

CA_01_2008_0001