A *Podcast Briefing* produced by SearchSecurity.com

Key Trends in Web Access Management and How CA SiteMinder® R12 Addresses Them

TechTarget
The IT Media ROI Experts

Sponsored By: ca™

SearchSecurity.com

Key Trends in Web Access Management and How CA SiteMinder® R12 Addresses Them

a Podcast Briefing presented by David Kirkdorffer and Matthew Gardiner

■ This *Podcast Briefing* is based on a CA/TechTarget Podcast: "Key Trends in Web Access Management and How CA SiteMinder R12 Addresses Them."

Introduction

Web access management (WAM) controls access to Web-delivered resources across an enterprise in a precise and flexible manner. A major goal of WAM implementations is to simplify the user experience while ensuring privacy, security, and access to key information to the user. WAM solutions also support enterprise policies and infrastructure and maintain the security of the enterprise systems.

WAM solutions must be sufficiently flexible to work with the browsers and web servers currently in use at the enterprise, as well as outside the enterprise if it has externally-facing services. They must also limit access to services in as granular a fashion as the enterprise requires, and centralize the enforcement and management of application security.

Single sign-on, in which a user only needs a single user identifier and a single password for access to all Web-based applications and services, has emerged as a means of centralizing user authentication and authorization in WAM solutions. It improves security behaviorally as well as electronically, since users only need to remember one user identity, and therefore are less likely to need a written list of user identifiers and passwords.

WAM solutions have evolved over time to include a number of elements, including:

- Enrolling new users, so that user authentication data is transmitted and stored securely
- Managing user privileges, in order to ensure that a given user has access to only the services and data that particular user requires
- Auditing access to critical data, which provides for improved regulatory compliance
- Identity federation and provisioning, so that an enterprise can share user identities and authentication with other enterprises

This document details some of the current trends related to WAM. It also provides information about how CA SiteMinder R12 can help organizations leverage their WAM systems to meet evolving challenges related to centralized security and management, compliance, and evolving application infrastructures.

The Evolution of Web Access Management

WAM systems were developed to organize the security management chaos created by the rapidly multiplying numbers of Web-based applications and millions of users across large enterprises. WAM systems have been critical in meeting challenges posed by redundant security processes and major compliance initiatives.

Inside...

The Centralization Challenge

Prior to WAM, security was provided on an as-needed basis as each application came online. This situation caused a proliferation of what are known as "security silos." Each silo had its own infrastructure, security model, and user experience. Web access management solutions and, specifically, CA SiteMinder came about in response to this situation. With WAM systems, companies were able to eliminate security silos across the enterprise by centralizing sign-in and providing authentication management, authorization, and security auditing processes.

The centralization made possible by WAM systems meant that IT groups needed fewer people to manage the security for applications and their users. However, the trend toward more and more applications, often numbering into the thousands, made it difficult for IT organizations to provide comprehensive security management for all aspects of the applications. Customers are now finding that their WAM systems must provide a middle ground that allows them to delegate some security management to groups with a deeper knowledge of the business or application while maintaining overall centralized control.

The Compliance Challenge

WAM systems have been critical in helping companies meet major compliance initiatives such as Sarbanes-Oxley (SOX), Data Protection Act (DPA) in the UK, the European Union Data Protection Directive (EUDPD), the Health Insurance Portability and Accountability Act (HIPAA), and many other IT-impacting privacy and control regulations. Organizations are now returning to their WAM systems with requirements to meet new compliance challenges, such as the ability to generate more precise reporting for both internal and external auditors. Furthermore, companies want all of their system investments, including WAM, to be flexible enough to solve these challenges more quickly and less expensively than in the past.

The Functionality Challenge

Organizations want more and more from their WAM systems every day. A lot of this push comes from challenges imposed by the realities of the Web, both good and bad. Malicious activity from external intruders requires stronger security and authentication. Architectural advances such as Web services and service-oriented architecture also demand effective security management. Yet another function that is high on the list is federation. Each of these areas is addressed in one way or another by CA SiteMinder R12. One forward-looking step is the introduction of CA SOA Security Manager, which provides security for new XML-based Web services applications and is closely integrated with CA SiteMinder.

Issues

- What are the current trends in Web Access Management?
- How is CA SiteMinder R12 addressing these WAM trends?

Web Access Management Trends

David Kirkdorffer: What have been some of the key trends in Web Access Management over the past few years?

Matthew Gardiner: The three most important trends, from my perspective, are:

- WAM systems have transitioned from being tactical Web security systems to being a centralized security infrastructure for an enterprise. These systems now provide single sign-on, together with authentication, authorization, and auditing (AAA) for the whole enterprise. In many cases, deployed WAM systems support thousands of applications and millions of users. However, while many organizations are fairly far along in this transition, the transition itself has created a new set of management challenges.
- WAM, IAM, and security systems in general are now important parts of the regulatory compliance and governance infrastructure. But as they have matured, many organizations are now coming back to their WAM systems with more compliance requirements.
- The definition of a WAM system has changed and broadened. While it is still quite clearly about AAA and single sign-on for the Web, WAM now encompasses strengthening enterprise authentication and enabling federation. Federation, in turn, enables Web services security.

Centralization

Kirkdorffer: How are WAM systems being used as a centralized security infrastructure and what challenges arise as a result?

Gardiner: The centralized security provided by WAM systems was developed to eliminate security silos, which were produced by the practice of building security into each Web application provided by the enterprise. Many organizations have totally embraced this model and now provide centralized security for hundreds or even thousands of applications, and in some cases for millions of users.

But centralized security management has created its own challenges. Centralization has allowed organizations to rely on relatively small staffs to manage their security systems. But it is not realistic for a centralized staff to know enough about the thousands of applications and millions of users to really manage all the security aspects centrally. Organizations that have moved their security this far realize that, although they cannot return to the chaotic world of security silos, they must find a middle ground where they have centralized control, but can delegate administration. This middle path allows the centralized security organization to manage and control the security environment, while allowing different people—business people or IT people out in the organizations—to manage the security for individual applications or individual user communities.

Compliance

Kirkdorffer: The second trend dealt with compliance. In general, IAM is a set of technologies that organizations use to ensure various types of regulatory compliance. How are Web Access Management systems being used increasingly to drive compliance within organizations?

Gardiner: Organizations are in the next stage of security and compliance. The goal now is to use security systems to provide better compliance. While they have gotten past their first audit or their initial SOX, HIPAA, and PCI compliance initiatives, these were generally very expensive and time-consuming projects. Now these organizations are coming back and asking how they can accomplish proving and improving compliance cheaper, better, and faster. They want to know how they can get more out of the security systems they have in order to reach their compliance goals more easily.

Organizations are reexamining their WAM systems in particular and saying, “This is the kind of reporting I need and I need it at a moment’s notice.” Or “These are the types of users that did not traditionally need access to the security system, or the WAM system, but they do now.” For example, auditors might need real-time access to the WAM system or they might need certain reports, and so organizations are looking to their WAM and IAM systems to provide solutions for these challenges.

Broadening the WAM Definition

Kirkdorffer: The third key trend is how WAM systems today are being tasked to do more than they did in the past and thus how their definition is broadening. What are some of the key trends in this broadening of the WAM definition?

Gardiner: This really goes right back to the Web, that is, the Web as it has existed for the last 10-plus years. It is really the inventiveness around the Web—both good and bad—that has not really slowed. Because of these opportunities and challenges, organizations must deal with a lot of security issues. For example, the need for stronger forms of authentication is constantly being driven by the malicious activities of people who try to steal credentials. If not for their actions, ever-stronger forms of authentication would not be needed. But some people try to steal credentials in very inventive ways, like phishing and asking people in other sly ways to reveal their credentials.

So WAM systems are responding by enabling stronger forms of authentication. Newer technologies are also available to help with these challenges. For example, federation is an area that has been getting a lot of attention, and investment, because it eases the user’s access to applications, no matter whether those applications are in other domains internally or even within a partner’s domain.

Another area that is expanding the definition of WAM has to do with the big architectural changes represented by service-oriented architectures and Web services. More and more organizations are redesigning how they deploy applications, both for internal and external use. This means that WAM systems, since they are right in the middle of Web security today, are being asked to do more and thus the definition of WAM systems is expanding significantly. So, where WAM used to be about AAA and single sign-on, that is now only part of their definitions. Now these systems enable better authentication and federation, security for service-oriented architectures, and Web services security.

The Role of CA SiteMinder R12

Kirkdorffer: How does the new CA SiteMinder R12 address the previously detailed trends of centralized-yet-distributed enterprise security infrastructure, compliance, and the expanding definition of WAM?

Gardiner: CA SiteMinder R12 was developed with these trends in mind. These trends were validated when leading customers brought them up during discussions about what they wanted to see for CA SiteMinder in the future.

- **Centralized security infrastructure and delegated management.** CA SiteMinder R12 introduces what is called application and policy lifecycle management, which essentially combines a set of new functions and is a more business-friendly abstraction of the application. It represents a more granularly defined segregation of administrative tasks within CA SiteMinder combined with the ability to delegate security administration widely in a clear and controlled way.

  CA SiteMinder R12 also has a whole new Web-based UI, which places this new functionality into the hands of the delegated administrators. So, the combination of these things within CA SiteMinder R12 makes up the new application and policy lifecycle management model and is the key to addressing the need to both centralize and delegate.

- **Compliance.** CA SiteMinder R12 provides an entirely new reporting infrastructure that includes the ability to evaluate policies. This helps organizations determine which applications a user or class of users can access. While determining access is a reporting function, it is important that the policies that control that function are evaluated at the same time. This policy evaluation function is a whole new capability that is going to prove very valuable, not only from the control standpoint but also by generating precise reports for internal auditors and perhaps even external auditors.

- **Expanded breadth of WAM.** As it has evolved, CA SiteMinder has been expanding the concept and capabilities of Web access management. In earlier versions, CA SiteMinder included functions centered on federation and even Web services security through a complementary product. However, with this latest release, CA has introduced a new product called CA SOA Security Manager, which is highly complementary to CA SiteMinder. This product provides end-to-end security for XML-based Web services, and it is a great way to provide AAA and single sign-on for XML Web services. CA SOA Security Manager also provides XML threat prevention by stopping malware in addition to doing the traditional AAA and single sign-on.

In practice, organizations can deploy CA SOA Security Manager independently of CA SiteMinder, if they are not a CA SiteMinder customer, and use it to control access to Web services. However, a more typical situation will find CA SiteMinder customers combining CA SOA Security Manager with their CA SiteMinder deployment to provide Web security systems that can cover their websites as well as their emerging services.

So this third trend, the expanding nature of WAM, really places organizations in a good position to stay ahead of the curve in their efforts to provide security management ahead of need, provide federation capabilities to enable business, or provide centralized security services for Web services even before the organization moves significantly into the deployment of Web services. This is a great break from the past, when security was almost always implemented after the fact.

Conclusions

Kirkdorffer: What are the most important take-aways from this discussion?

Gardiner: Primarily that the WAM revolution is alive and well, an area that has proven to be a good investment in the past as well as going forward. Organizations that have invested in WAM systems and CA SiteMinder in the past have realized a good return and will continue to do so in the future. And CA SiteMinder continues to be the Gold standard in Web access management. CA customers continue to place their trust in CA SiteMinder to manage and protect their Web assets.

Kirkdorffer: Where can people get more detailed information about WAM, IAM, and CA SiteMinder?

Gardiner: The best place to go for information about IAM is www.ca.com/iam. For information specifically related to CA SiteMinder R12, such as white papers, go to www.ca.com/security.

■ **Mathew Gardiner** is the Senior Product Marketing Manager 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

TechTarget
The IT Media
ROI Experts

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.