



Web Access Management: The Business Imperatives

CA SiteMinder® Web
Access Manager

Table of Contents

Securely Leveraging the Internet: The Business Imperatives	3
Time-to-Market.....	3
Cost Savings.....	3
User Satisfaction.....	4
What is Web Access Management?	4
Authentication Management — Confirming Who You Are	4
Authorization Management — Determining What You Are Entitled To Do	4
Auditing & Reporting — Understanding What Was Done and Proving It	5
CA SiteMinder® Web Access Manager (CA SiteMinder)	5
How CA SiteMinder Responds to the Business Imperatives	6
CA SiteMinder Accelerates Time-to-Market	6
CA SiteMinder Drives Reduced Costs	6
CA SiteMinder Improves User Satisfaction.....	6
Summary.....	6

Securely Leveraging the Internet: The Business Imperatives

The Internet continues to drive a steady transformation of how organizations operate and grow. It does this by providing ubiquitous, inexpensive and standards-based connectivity that all people and organizations can take advantage of to communicate and collaborate. Organizations leverage the Internet and internet technology in an uncountable number of ways, from servicing their customers to collaborating with their supply chains.

While the Internet has been an important phenomenon for more than 10 years now, it remains a critical transformative force in the world, driving change in business, government, entertainment and social interaction. Given this it remains a critical business imperative for organizations to continue to prepare for the day when the Internet is the foundation of all internal communications and operations as well as external interactions with customers, business partners and others around the globe.

For all the benefits, fully embracing the Internet also can expose high level business challenges. An organization must determine how to simultaneously let business in while keeping risk out. Virtually every organization these days needs to achieve several goals that are often largely dependent on their IT strategies. These business goals are improved time-to-market for products and services while preserving reasonable security and control, cost savings and efficiency and improved user satisfaction.

Time-to-Market

As markets and business environments change, speed and agility are essential to refocusing business resources and priorities in order to quickly and efficiently bring new and enhanced products and services to market. Successfully responding to the opportunities enabled by the Internet can change an entire business, enabling faster product development, new markets and channels, closer customer relationships, stronger brands and greater competitive barriers.

However, while the use of the Internet can enhance organizational speed and agility, it can also create numerous security exposures and vulnerabilities. By definition with the move to the Internet you are placing your organizational lifeblood — your proprietary and private data and applications — in an easily accessible medium. How do you secure these critical resources — both easing access and controlling access? How do you provide access to these assets while also meeting your IT control objectives that are so critical for regulatory compliance and data privacy?

Today, organizations continue to deploy ever growing portfolios of applications in support of rapidly increasing and diverse user populations. This places unprecedented demands on an organization's IT and security management strategies.

Cost Savings

Every sensible Internet strategy revolves, at least for profit seeking organizations, around the ultimate business truth — it only matters if it leads to your organization making or saving money. As companies continue to assemble ever larger portfolios of applications that are accessed by rapidly expanding user populations, significant security management scaling problems generally arise. Historically, organizations could deploy a limited number of applications to a relatively small number of users in a reliable, low cost manner, even if security management was conducted in a highly manual fashion. As the number of these applications and users grew with the growth of the Internet, the costs to support and secure them has often grown exponentially. This approach simply is not viable.

In the IT organizations of large enterprises, this growing portfolio of applications has stretched development resources to the limit. IT must continue to find ways to provide new generations of business-supporting applications while controlling costs. Traditionally, these applications have all had their own similar but separate security implementations — using access control lists (ACLs) and custom security logic to provide authentication, authorization and auditing/reporting services, treating each user separately and independently of the same user in other applications. In the IT security arena these applications are typically referred to as being “siloesd” from a security perspective.

The siloesd security model works fine when you have just a few applications and a relatively small user community. However, few businesses can afford to build, embed and maintain dozens or hundreds of separate security implementations as they scale up to full Internet usage with all their user constituencies. Just as IT departments strive to standardize on and share resources in such areas as application servers, Web servers, operating systems and hardware, they also need to provide centralized, shared security resources to achieve consistency, usability and simplicity — and considerable cost savings.

User Satisfaction

The definition of a “user” has undergone significant changes since the advent of the Internet. Previously, IT organizations only needed to serve the application and data needs of a subset of internal employees and thus a user was defined as some set of internal users. Today, Internet-enabled IT systems touch virtually every employee in every area of an organization. In addition, the arrival of the Internet-enabled enterprise and the flood of Web applications have raised the bar yet again for IT.

Today, forward-thinking IT organizations are reaching beyond enterprise boundaries to tightly integrate customers, employees, partners and vendors into a corporate ecosystem. Initiatives such as customer self-service and supply-chain integration are predicated on supporting a broader class of users accessing growing numbers of applications and interacting with more data. A “user” can now often be best described as encompassing every constituency of the organization.

These diverse users work at different companies (or are retail consumers), with different roles in their organizations and with varying application needs. Employees want applications that support their job functions. Customers and prospects need applications to help them purchase and use company products. Partners need applications to support their unique, upstream or downstream, complementary roles. In response, IT organizations need to provide enabling applications, infrastructure and security management solutions.

To drive improved time-to-market, cost savings and user satisfaction, IT organizations should implement security management shared services — particularly in the area of identity and access management.

What is Web Access Management?

Web access management systems provide a centralized security infrastructure that enables authorized use and prevents unauthorized use of Web resources and data. In short, it lets business in and keeps risk out.

Web access management solutions automatically verify a user’s credentials, enable that user to access specific resources and control the entitlements that the user has to those resources. To be effective, the Web access management solution must be built on a strong enterprise-class technology providing several key capabilities: authentication management, policy-based authorization and auditing/reporting services, while layering seamlessly into the existing heterogeneous infrastructure found at most large organizations.

Authentication Management — Confirming Who You Are

User authentication involves much more than simply creating and managing user passwords. Effective authentication management centrally coordinates the use of the multitude of methods or technologies that can be used for authentication, such as passwords, certificates, smart cards, forms, one-time password tokens and various types of biometrics (fingerprints, voice ID and more). This enables security professionals to select and apply the appropriate authentication technology for a given application or data resource without hardwiring the authentication system directly into each application.

Centralized authentication management enables IT to change, upgrade or add to the organization’s portfolio of authentication technologies without changing the underlying business applications that are being protected. This centralized approach provides the necessary scalability in large corporate environments, where it is not uncommon to have hundreds if not thousands of separate applications requiring security. If a new authentication method is needed to be directly integrated into each underlying application, its rollout would be significantly impacted.

Centralized authentication management also makes it far easier to manage a user’s session across many applications. This centralized session management enables both single sign-on (SSO) and single sign-off functionality. With SSO users present their log-in credentials once and receive access to all the applications and resources to which they are entitled without having to re-present their credentials. From an end-user’s perspective this is the type of security that makes sense.

Single sign-off provides the critical security-enhancing complement to SSO by providing immediate exit from open application sessions after a single log-off. Open application sessions are a typical security hole that dishonest people can easily slip through.

Authorization Management — Determining What You Are Entitled To Do

Authorizing users to individual applications — defining entitlements, assigning entitlements to people and enforcing the access policies in real time that apply to them — is another component of centralized access management that is expensive to deliver with “siloeed” application security architectures. Creating and maintaining user authorization logic within each application is an expensive proposition, particularly when user populations and application portfolios are expanding and specializing rapidly.

Authorization management requires an understanding of users, roles (or groupings), the resources they can access and the rules (determined from governance policies) that govern which users can access what and when. The more granular the centralized authorization management the easier subsequent management becomes. Using centralized authorization management services of a Web access management system, enterprise applications become consumers of these authorization services.

For example, when a user has been authenticated and seeks access to a particular application, the authorization management service will first consider the user's identity, authentication system used, group, title, location and other profile parameters in making its access decision and then pass along some of this information to the requested application. The application subsequently applies its own granular logic regarding what screens, functions and data that the user can use and view.

Auditing & Reporting — Understanding What Was Done and Proving It

Security related system auditing and reporting — a critical portion of most IT operations — becomes increasingly difficult as the number and type of users and applications increase. Assuming that each separate application has its own auditing and reporting features (often they don't) built into the application, it quickly becomes infeasible to get a consolidated view of resource usage across the enterprise. Absent this comprehensive view, it is difficult to assess what system or security improvements must be made. It also is difficult to prove to internal and external auditors that sufficient IT controls are in place.

In industries such as financial services, health care and many others, increased concerns about data privacy and security as well as specific federal and state regulations are driving a mandate for consistent and auditable enterprise wide resource security and access policies. The ability to provide information and reports to internal and external auditors is a critical step to meeting many of these requirements.

CA SiteMinder® Web Access Manager

CA SiteMinder® Web Access Manager (CA SiteMinder), a key portion of CA's comprehensive Identity and Access Management Solution, is a market-leading Web access management software solution. CA SiteMinder provides a centralized security management foundation that enables user authentication and controlled access to Web applications and portals.

CA SiteMinder delivers the market's most advanced security management capabilities and enterprise-class site administration, allowing organizations to reduce IT operational costs and enabling greater IT control and security. CA SiteMinder enables the secure delivery of essential information and applications to your employees, partners, suppliers and customers — and scales with your growing business needs.

In addition CA SiteMinder delivers single sign-on and single sign-off to applications by centrally managing the user's application sessions.

Key features of CA SiteMinder include:

- **Authentication Management.** CA SiteMinder supports a broad range of authentication methods, including passwords, one-time password tokens, X.509 certificates, custom forms and biometrics, as well as combinations of authentication methods. The authentication management capabilities of CA SiteMinder enable the use of any number of authentication methods to be used with the wide range of user communities and applications that a given organization might have.
- **Authorization Management and Single Sign-On.** CA SiteMinder centralizes the management and application of authorization policies for customers, partners and employees across all Web applications by providing a shared security service. Users sign-on to an organization's Web site managed by CA SiteMinder to gain access to all relevant, applications and data available at that site for which they are entitled. Single sign-on provides a richer user experience, increases security and reduces customer support costs related to forgotten passwords. In addition because of its central Web access management role, CA SiteMinder also provides SSO to the Web applications that the user is authorized to access.
- **Auditing and Reporting.** CA SiteMinder enables organizations to define auditable activities to be logged, where that information should be stored and provides pre-defined web based reports covering user and administrative activity involving protected resources. Auditing and reporting lets managers track user and administrative activity and analyze and correct security events and anomalies.
- **Secure Identity Federation With Partners and Customers.** Identity federation enables organizations to securely manage users and user data as they move among partner, customer and other affiliated Web sites, receiving an SSO experience between external organizations and internal business units. CA SiteMinder provides support for widely adopted industry standards such as the Security Assertion Markup Language (SAML) and WS-Federation (implemented by Microsoft as ADFS) to make identity federation straightforward to accomplish as an integral component of a Web access management system deployment.

Finally, CA SiteMinder itself is a highly secure application, applying strong security technology to enable secure communication with its own distributed components. Organizations can deploy CA SiteMinder with confidence.

How CA SiteMinder Responds to the Business Imperatives

CA SiteMinder Accelerates Time-to-Market

CA SiteMinder enables companies to more quickly respond to changing market dynamics and opportunities by deploying new Web applications to broader groups of users, consistent with continually changing business strategies. In many situations these applications are critical to achieving a rapid time-to-market for new products and services. However, without the appropriate security infrastructure the deployment or enhancement of those applications is likely to be delayed or postponed, creating a significant drag on corporate agility and speed.

For example, if a financial services company wanted to deploy a new trading application on the Web, it won't do so until it is reasonably certain that the application is backed by a proven security system and process, as security can't be compromised even if other business benefits might be foregone as a result.

The centralized Web access management capability of CA SiteMinder creates a more secure environment for enterprise applications. It delivers a consistent security experience for large numbers of users and applications through a centralized, shared resource. This eliminates the need for proprietary, redundant security code inside each application. By leveraging this reusable system, organizations are able to deploy sensitive applications with confidence.

CA SiteMinder Drives Reduced Costs

CA SiteMinder also provides numerous cost saving advantages from both an IT development and administration point of view, not even mentioning the productivity advantages to the user. CA SiteMinder provides highly flexible capabilities for security administrators to create and enforce security policies and to quickly tailor access management functionality to the unique needs of their environment.

CA SiteMinder enables dynamic rules and policies, centralized authentication and authorization management, role-based access control, centralized Web agent management and much more. This solves an apparent paradox by significantly accelerating development cycles (driving costs down) while simultaneously increasing the level of security achieved for those applications.

Some industry experts believe that externalizing and separating access-management logic from application development can result in a savings of approximately 50 percent of the resources normally dedicated to security development for each application project. For many Fortune 1000 firms, these development savings alone can justify the deployment of CA SiteMinder. In addition organizations can also benefit operationally by having their Web access management externalized from the underlying applications as maintenance and ongoing management costs are also reduced. Just think of the cost to the IT Helpdesk alone in helping users who have forgotten their passwords. In fact some organizations can financially justify the deployment of CA SiteMinder with just this area of savings.

CA SiteMinder Improves User Satisfaction

For end users CA SiteMinder enables increased productivity and an enhanced overall application experience. Single sign-on features enable users to seamlessly navigate between and among applications quickly and easily and with fewer interruptions, significantly improving the likelihood of application adoption. This can be critically important for external users such as customers and partners, who have other choices a mouse-click away. A well structured, seamless user experience will build partner confidence, customer loyalty and employee satisfaction, strengthening brand value, market influence and ultimately, revenue and profits.

Summary

The Internet's sweep through the world of business, government and non-profits/academia has been dramatic but it's far from over. As the number of unique users who need access and applications that need to be developed and maintained increase, IT organizations are racing to meet the demand. However, information security is non-negotiable as organizational survival largely depends on the trust of its users. The sooner organizations take concrete actions to ease this transition, the smoother the transition will be.

