WHITE PAPER
Security Solutions

verizon

The Identity and Access Management Imperative: Securing the Extended Enterprise

Introduction

For nearly three years, a junior trader allegedly used stolen passwords and insider knowledge to conduct fraudulent trades at a large French bank. His activities started in 2005 on a small scale, but by 2007 the level of illegal trades had soared. Apparently, with the aid of an assistant, the trader was able to circumvent the bank's weak oversight and controls. When the bank discovered his fraud in January 2008 the fallout was catastrophic. The losses—$7 billion worth—were more than double the bank's 2008 net income.

Not surprisingly, in the aftermath of this security breach the bank implemented stronger security measures. Efforts included security training, redefining read/write access permissions, and gaining better visibility into user activities. The banking giant has closed many of the gaps in its user identity and access controls, but at great cost to its organization, reputation, and shareholders.

While the magnitude of this event is unparalleled, the risk posed by unauthorized users at any organization is still great. A study presented by McAfee CEO Dave DeWalt at the 2009 World Economic Forum found that companies lost an average of $4.6 million in intellectual property the previous year.[1] Despite the constant threat to data, applications, and networks, solving identity and access management (IAM) challenges continues to elude most organizations. This paper discusses how organizations can use emerging technologies and new service options to implement an IAM solution that aligns with their unique needs and business demands.

The IAM challenge for executives

The digital world is creating shifts in the way business gets done, resulting in both exciting but often troubling times for executives. What was once an intimate corporate network is now a globally connected web of people and devices. More employees work remotely, carrying sensitive data on notebooks and PDAs. Partners and suppliers are invited inside the corporate walls to interconnect their own systems and share information. Vendors and contractors are trusted with access to sensitive data.

Many C-level executives may not know for certain that their information is secure—that only the right people are gaining access to the appropriate applications, networks, and data. And now with the introduction of cloud-based services, mobile devices, and remote users, there are even more connections to critical data and applications both inside and outside of the enterprise.

Identity and access management (IAM) is the security discipline that authorizes users to access corporate systems and information. It helps prevent fraudulent access and use of data that could potentially impact the business, its partners, or even worse, its customers.

The majority of organizations haven't been able to realize the full promise of IAM—to secure the enterprise information in a cost effective and compliant manner. Many have implemented components of IAM, some even accomplishing the elusive "single sign-on," but often fall short in other areas. This failure is evident as research from Verizon Business investigations shows 75% of breaches went undetected for weeks or even months.

The majority of organizations haven't been able to realize the full promise of IAM—to secure the enterprise information in a cost effective and compliant manner.

The extended enterprise tests the limits of IAM

Identity management is a top security project for many IT organizations. It's not difficult to see why. Manufacturers and suppliers are opening their systems to retailers to jointly manage inventory. High-tech product companies are allowing partners and distributors to access sensitive information, ranging from product development plans and pricing to sales leads and product training.

This "networked" business model means managing access for users the company knows little about. A 2009 Data Breach Investigations Report by the Verizon Business RISK team shows that almost one third of data breaches were linked to trusted business partners, such as suppliers and contractors.

Cloud-based applications are on the rise, bringing more complexity to managing user security. A 2009 study by IDG found that about 30% of the respondents had applications running in the cloud, and an additional 16% had plans to bring applications to the cloud in the next 12 months.[2] More than 80% of these same respondents reported they did not have a security strategy in place for cloud computing.

Layered on top of these new business considerations is the requirement to meet industry-specific regulations and standards. Enterprises must address the information security compliance requirements in HIPAA, Basel II, PCI DSS, and others. Many companies may be at risk in this area. For example, the RISK team's data breach study found that of the victims that were subject to PCI compliance, only 19% had met the PCI requirement to assign a unique ID to each person with computer access.

Managing so many different types of users and applications can be difficult. Maintaining compliance across this rich array of contributors and connection points can make the task nearly impossible. As companies struggle to implement IAM internally, it's clear that new solutions should be considered.

Where internally managed IAM becomes difficult

The value of IAM extends beyond securing desktops and applications. It extends to securing all network access points—whether business and partner interfaces, wired, wireless, or remote. As organizations start to uncover all of the variables in the IAM equation, the complexity becomes evident. Integrating network environments, legacy and web-based systems, thousands of users, and disparate applications into a comprehensive IAM strategy requires best practices overlaid with a custom approach. There is no simple, out-of-the-box solution that IT administrators can deploy to handle every contingency.

Organizations that choose to run in-house IAM can often see their efforts fall flat, stalled by the sheer size of such an undertaking. Classifying and connecting thousands of users, applications, and locations is a job that far exceeds the resources found in most organizations. The impact of the extended enterprise, operational complexity, and resource constraints must be carefully considered when creating an IAM strategy.

Keeping up with the extended enterprise

How fast IT can securely integrate new users—whether new hires or the result of partnerships, reorganization, or acquisition—determines how quickly these users can make a contribution to the enterprise. The business expects IT to respond to their new projects but doesn't expect integrated end-user access to be a showstopper. It wants immediate access to new systems, whether they are recently launched applications, new systems acquired in a merger, or new applications accessed from the cloud. Business users can be intolerant of delays due to lack of access.

The difficulty doesn't end with deployment. Because each system requires its own authentication, users are required to remember a number of access credentials. Naturally, passwords are forgotten, and productivity is lost while both the locked-out user and the help desk work to restore access.

A fascinating scenario demonstrates where a weakness in a petroleum company's IAM strategy created a data breach that financially impacted customers. Within days of writing checks or using credit cards, the company's customers experienced some type of fraud. At first investigators thought it was a simple case of hackers getting access to several POS systems. After ruling that out, the investigation team dug deeper and found the breach was actually connected to one default user account that was assigned to all of the vendor's technicians. A trap was set, and fortunately the perpetrator was found. But this scenario illustrates the vulnerabilities of extending the enterprise and emphasizes the meticulous care that must be taken to protect data.[3]

Who is behind data breaches?

74%	resulted from external sources.
20%	were caused by insiders.
32%	implicated business partners.
39%	involved multiple parties.

Verizon Business 2009 Data Breach Investigations Report

IAM solutions play a critical role in helping organizations respond to changing business conditions, without compromising security.

Dealing with operational complexity

The heterogeneous IT environment found in most organizations is a result of adding IT investments over the years. IT departments face an assortment of standards, platforms, and legacy systems that must be rigorously managed to address compliance with security policies and regulatory requirements.

As more systems come online and new partnerships are formed, IAM must scale to match the need. This often means additional efforts for every IT project to incorporate end-user security and access. It also means keeping IAM applications current and available. With systems in numerous locations, the task becomes more and more resource intensive.

The rush to integrate new users can feel like a choice between rapid integration and maintaining security. However, rolling out new software and making it immediately available to partners before taking the time to secure it can have grave consequences. It puts the business at risk for data breaches and security threats. Businesses can hardly afford the risks, losses and damaged reputation associated with these types of failures.

Managing IAM with constrained resources

A business that deploys and runs an internal IAM solution must have its own staff, including security analysts, IT developers and administrators, and incident-response teams who all have knowledge of a variety of IAM methodologies and software applications. If internal teams don't possess the required expertise in identity management, incomplete policies and procedures for securing users may result—instead of a robust IAM strategy.

The rapidly growing IAM market currently has a shortage of technical consultants possessing the specialized skills needed to implement an identity solution, operate identity controls, and security countermeasures. Consultants who are available are in high demand and are, consequently, expensive.

Although the ability to control all aspects of an internal IAM solution may sound appealing, the trade-off in the costs to plan, deploy, and manage the diversion of critical resources from other projects and the lengthy time to deploy can be significant. Often budgets are insufficient to support a scalable IAM strategy because many IT organizations don't fully articulate the ROI for IAM until a breach has occurred.

For the enterprise that finds IAM too expensive and resource intensive, it's time to rethink whether an internal IAM strategy is the right plan. Moving to an externally provided solution can be a cost-effective way to address the problems inherent with an internal IAM approach and simultaneously provide additional benefits, such as leveraging best practices and managing deployment times.

Solving IAM challenges with hosted services

Like many mission-critical applications, IAM is now available as a hosted and managed service, and can resolve many of the user management, authentication, and authorization challenges that organizations face. By embracing cloud-based services, CIOs are discovering that they can quickly respond to changing business needs and at the same time, control the costs associated with deploying and managing their applications.

A hosted IAM solution can help organizations control the expense and complexity of managing user access and authentication. Most important though, hosted IAM solves the federated identity challenge that allows an authentication credential to be trusted among multiple applications.

> By embracing cloud-based services, CIOs are discovering that they can quickly respond to changing business needs and at the same time, control the costs associated with deploying and managing their applications.

Increase business agility with federated identity

Federated identity helps reduce authentication management by establishing user authorization across systems, even across companies. It allows disparate systems within and outside the company to be seamlessly joined from a security perspective. Implementing federated identity management can help maintain security and lower risk by authenticating a user just once and passing the authentication across multiple systems, including external partner websites.

For example, if trust has been established between a supplier's system and the company's inventory management system, the supplier can log in to the internal inventory system as a trusted user. This mutual trust agreement with the supplier system is extended to those who have access to that system.

When setting up a federated identity process, each system or entity must establish trusted links with every other entity, creating a web of connections. However, this complexity can increase management overhead and limit the flexibility to leverage different specifications as new relationships are formed and SaaS applications are added.

Hosted IAM providers can play a critical role in helping organizations untangle this web by acting as a broker, enabling authentication between entities without having to actually store user identities. In this scenario, a hosted IAM solution reduces the need for every system to establish trusted links with every other system, thus controlling the overhead needed to manage all of the links. The broker creates a single trusted link that all systems can leverage, much like a hub with spokes. Once a user is authenticated, the user can log into any other federation-enabled service, including SaaS applications. A hosted IAM solution takes the burden of developing this service out of IT hands. It allows IT to leverage a best-practices broker service that is maintained by the service provider.

Manage risk and address information security compliance requirements

Meeting standards and regulations can be tricky, especially as organizations expand access beyond their firewalls to customers, partners, suppliers, and applications in the cloud. It's difficult enough to manage systems within the corporate domain but even more difficult when accounting for access across a firewall. Therefore, it's vital to centrally manage user access and easily provide reports for compliance assessments.

IAM takes time to implement and working with the service provider's team of experts helps organizations quickly deploy solutions and meet security compliance requirements. Hosted IAM can be set up in a fraction of the time it takes to deploy IAM internally. It can also provide a centralized solution that's easy to manage and delivers policy enforcement rules that afford the same rights to users as if they had signed on to the individual systems directly.

When considering the effort needed to manage the security compliance requirements within regulations and standards such as PCI DSS, Basel II, and HIPAA, it's important to use a hosted IAM provider that thoroughly understands regulation requirements and provides reporting functionality. The service provider can also analyze the enterprise IT environment and provide expert advice on security gaps and remediation steps, helping both the business and the IT department address its security compliance requirements.

The potential for risk can be seen in many business arrangements—particularly one as common as offshore partnerships. Consider a pharmaceutical company that adds an offshore partner to gain cost savings and speed time to market for a new product. To realize the advantages, significant data sharing between the two companies must happen. For example, the partner may need access to a critical data center that contains sensitive patient research covered by HIPAA regulations. The right IAM solution makes it possible to quickly add partners in a secure manner and helps demonstrate compliance through auditing and reporting.

Speed implementation and control costs

When employees leave, partner and supplier relationships change, or companies merge or divest, all of those user connections must be managed. This is an area of concern for many organizations as they expend significant resources to try and adapt to their changing user base.

Just developing an IAM solution can take many months. It takes time to create a work plan, locate hardware, purchase software, install and configure the system or systems, train administrators, create connections to other systems, and test the application. And these are just a few of the tasks required.

Hosted IAM eliminates the need for businesses to purchase expensive IT infrastructure hardware and software. It also allows organizations to get up and running quickly on systems that have the most up-to-date, leading IAM applications. Increased scalability also provides an extremely short time to productivity, which means that contractors and partners are able to begin work and access resources quickly and efficiently.

Expanding operations to the cloud environment can not only control costs and create efficiencies; it's an opportunity to improve overall security posture.

Companies that utilize hosted IAM are able to rely on the knowledge of experts who have deployed multiple IAM solutions and can make recommendations based on the particular needs of the company. This experience also enables service provider professionals to identify potential vulnerabilities in the organization's IAM strategy and helps the enterprise maintain the security of its mission critical data and applications.

Hosted solutions provide high availability and disaster recovery options, and can be scaled up or down as needs change. In addition, licensing, maintenance, and support costs are generally included in hosted IAM pricing, providing a positive total cost of ownership (TCO) analysis.

When the complexities of the IT environment include applications already in the cloud, hosted IAM makes even more sense. Expanding operations to the cloud environment can not only control costs and create efficiencies; it's an opportunity to improve overall security posture. It doesn't necessitate creating new security policies for the cloud, but rather viewing cloud protection as an extension of existing security policies to encompass an additional platform.

Summary

Changes in the marketplace are creating more urgency for CIOs and CSOs to implement a better IAM strategy—one that aligns with specific business needs without significantly increasing costs or risk. It's a difficult challenge and one that won't be solved overnight. However, it cannot be put on the bottom of the IT project list just because the company has limited resources and budget. Nothing is a higher priority than protecting sensitive company and customer data.

As IT organizations look to fully implement IAM while being pressured to manage expenses and head count, a hosted IAM solution makes sense. By combining the expertise of IAM professionals with an architecture that is prepared for IAM based on industry best practices, organizations can reach their security goals in less time and better manage the cost of their solution, rather than trying to build and maintain the same level of security on an in-house basis.

There are a number of benefits with a hosted IAM solution. As with any hosted application, it is managed in a secure data center environment that has high availability, can scale with the growth of the company, and has 24x7 global support. A hosted solution should rely on proven technology and offer ready-to-apply security policies. Benefits can also include controlled costs via less up-front spending and a shift from CAPEX to OPEX, as well as reduced staffing and time to implementation.

Hosted IAM enables organizations to keep up with their extended enterprise and simplifies the complications it creates for identity and access management. No longer will it take days or weeks to integrate new users—their contributions to the business can be quickly realized.

Verizon Business can help you securely extend your business

If you're struggling to quickly integrate systems and bring new users online, or have questions about how to get started with IAM, Verizon Business has the professional expertise and network to help your business be more agile and secure.

Whether you're looking for an identity management solution that is hosted or need help managing your in-house solution, your enterprise can enable comprehensive IAM through one trusted provider. Verizon Business Identity Management Services can be delivered as a service to you directly from our global IP network—one of the most resilient and reliable networks in the world.

For more information, contact your Verizon Business account manager or visit verizonbusiness.com.

About Verizon Business

Verizon Business, a unit of Verizon Communications (NYSE: VZ), is a global leader in communications and IT solutions. We combine professional expertise with one of the world's most connected IP networks to deliver award-winning communications, IT, information security and network solutions. We securely connect today's extended enterprises of widespread and mobile customers, partners, suppliers and employees—enabling them to increase productivity and efficiency and help preserve the environment. Many of the world's largest businesses and governments—including 96 percent of the Fortune 1000 and thousands of government agencies and educational institutions—rely on our professional and managed services and network technologies to accelerate their business. Find out more at www.verizonbusiness.com.

[1] McAfee. January 2009. Unsecured Economies: Protecting Vital Information

[2] IDG Research. April 2009. As hyper-extended enterprises grow, so do security risks.

[3] Verizon Business. August 2009. International petroleum company turns to Verizon Business to solve a perplexing security attack.

verizonbusiness.com