INFORMATION SECURITY®

ESSENTIAL GUIDE TO

Identity & Access Management

Managing proper access to applications and sensitive data becomes even more important in a recession.

INSIDE

TechTarget
The Technology Media ROI Experts

INFOSECURITYMAG.COM

contents

ESSENTIAL GUIDE

IDENTITY & ACCESS MANAGEMENT

FEATURES

Arcot Makes Strong Authentication as Easy as A-B-C

Authenticate Valid Users

Block Fraud in Real Time

Comply with Regulations

Arcot solutions protect the identities of over 60 million users. You can transparently fraud-proof any username/password process without changing user sign-in behavior or requiring hardware tokens. Arcot offers a wide range of authentication methods including risk-based authentication, security Q&A, OTP via SMS/email, OATH tokens, CAP/DPA and the patented ArcotID secure software credential.

Block Online Fraud.
Protect Online Access.
Transparently.

ARCOT®

The Authentication Authority

Online Fraud Prevention | Strong Authentication | e-Document Security

Managing Identities and Access

BY KELLEY DAMORE

IN THE DIFFICULT ECONOMY we face today, a comprehensive identity and access management program moves from a nice to have to a need to have. In fact, according to a Ponemon Institute study, 59 percent of ex-employees admit to stealing confidential company information, such as customer contact lists. As workers get laid off and employees pick up new responsibilities, organizations need to adequately manage access to applications.

Easier said than done. A full-blown IAM project can take years and be very complicated as organizations integrate and cobble together their disparate systems and reconcile users and access.

But the reality is building an IAM foundation will save you dollars and headaches down the road. Automation is crucial and compliance demands are driving organizations to do just this. In fact according to our *Information Security*/SearchSecurity Priorities 2009 survey, 16% said their biggest increase in spending will be in the area of identity and access management with the biggest drivers being preventing unauthorized employees from accessing sensitive information.

Furthermore, half said migrating to a more integrated approach was important/very important. Almost 60 percent wanted to get better at strong authentication and almost 70 percent said strengthening endpoint and network access control was very important/important.

We hope to help you in your IAM journey through this Essentials Guide. In this ebook we will explain some of the newer IAM technologies such as Active Directory bridge, entitlement management, facial recognition software, USB-style smart cards and virtual directories. We'll also dive into the do's and don't around managing privileged accounts and how vendors are offering solutions for those who have root access. We'll explain the benefits and pitfalls when it comes to IAM suites. As the market has consolidated around a few large vendors, does it make sense to use their integrated suites instead of buying individual products? We'll also explain the basics when it comes to identities and managing them with a technical explainer on LDAP and biometrics. Identities and the access granted is a top concern for security professionals. We hope you find this guide useful.›

Kelley Damore is Editorial Director of the Security Media Group for TechTarget, which includes Information Security *magazine, SearchSecurity.com, SearchMidmarketSecurity.com, SearchFinancialSecurity.com, SearchSecurityChannel.com, SearchSecurity.co.uk, Information Security Decisions conference and Financial Information Security Decisions conference. Send feedback on this column to feedback@infosecuritymag.com.*

digitalPersona FINGERPRINT IDENTITY & AUTHENTICATION SOLUTIONS

Eliminate Costs and Headaches of Passwords and Strong Authentication

Make Security and Compliance Easy

- With one touch, login to Windows, Web, Citrix, Legacy Applications without changes to applications
- Know for sure who does what

Reduce IT Costs & Complexity

- Eliminate calls to your help desk
- No tokens, smart cards or passwords needed, just your finger

Centrally Manage Strong Authentication Policies

- Enforce company security policies, comply with legal mandates
- Multi-factor Authentication

Test Drive DigitalPersona for FREE!

DigitalPersona makes integrating fingerprint technology into applications simple. Our **FREE** Evaluation Kit comes complete with everything you need including documentation and access to our support team.

Go to: www.DigitalPersona.com/IAM

Trusted by 95,000,000 People Worldwide

Identity management for changing times

Identity management technology is adapting to meet enterprise needs. Learn what products can improve security and ease compliance.

BY MARK DIODATI

DOES IT FEEL LIKE THE WORLD of identity management is calcified with the same old products and a glacial pace of innovation? Strong authentication, directory services, provisioning, Web access management, and federation have been around for years but what's new?

In fact, there are a lot of developments in the identity management space and newer technologies such as privileged account management, Active Directory (AD) bridge, and entitlement management are taking off as companies look to ensure security and meet compliance demands.

While large enterprises have deployed a mix of identity management products, few have enjoyed the synergies that these products bring when they are integrated. Let's look at some of the benefits the new technologies provide and strategies that can help an enterprise fully leverage its identity management investments.

Old School Identity Management

Traditional identity management products have become an intrinsic part of the IT infrastructure and continue to be deployed today. They include:

- **Directory services** and authentication products are the oldest examples of identity management products. Directory servers use the Lightweight Directory Access Protocol (LDAP) to present data. While relatively difficult for developers to work with, LDAP has emerged as the standard repository for user and policy information.

- **Provisioning** systems add, delete, and modify user accounts across heterogeneous platforms. These systems typically include workflow (to enable the approval of changes to user accounts) and role management capabilities, which can provide security and compliance benefits.

- **Web access management (WAM)** systems provide single sign-on (SSO) and authorization services for heterogeneous Web applications. WAM systems work solely with Web applications and do not require client software besides a Web browser.

- **Strong authentication** systems leverage at least two factors to provide higher identity assurance. The most commonly deployed strong authentication system in the enterprise is the one-time password device (OTP). The device displays a unique code, which is combined with a personal identification number (PIN) to provide two-factor authentication. Other strong authentication mechanisms include smart cards (which also leverage a portable hardware device and a PIN) and biometrics.

- **Federation** technology was a response to the challenge of providing single sign-on services to users at separate organizations. Unfortunately WAM systems weren't up to the challenge as they leveraged the HTTP cookie for session management, which did not work across corporate boundaries. The default standard in federation is Security Assertion Markup Language (SAML).

New School Identity Management

Newer types of identity management technologies such as privileged account management, Active Directory (AD) bridge, security information management (SIM), entitlement management, virtual directory, and enterprise SSO products are seeing broad adoption. In most cases, these markets are growing at a greater rate as compared to traditional identity management products. They include:

- **Privileged account management** is a market segment growing fast, with most large, regulated enterprises either having already deployed or planning to deploy the technology. While provisioning systems are very good at managing user accounts belonging to real users, they are terrible at managing generic privileged accounts like the UNIX root account. These accounts are required by the target platform (try deleting the root account from a UNIX system and see what happens), so access to them needs to be controlled. The accounts are also shared by many administrators; the result is a lack of accountability.

In the hands of evil-doers, these generic privileged accounts can inflict real damage, because they can bypass security controls, destroy or breach confidential data, and cover tracks by deleting audit data. Privileged account management products provide greater accountability because the account must be checked out by the

administrator and the password associated with the account is changed frequently.

• **AD bridge** is another segment that is seeing explosive growth. These products extend authentication, authorization, and identity management from Microsoft Active Directory to non-Windows platforms like UNIX, Linux, and Mac OS. Using Active Directory, enterprises can manage identities and provide centralized authorization to these platforms. Additionally, these products enable the authentication of non-Windows users against Active Directory, and provide single sign-on between Windows, UNIX, Linux, and Mac OS platforms. AD bridge products are very popular because they enable enterprises to leverage their significant investment in Active Directory to provide security services for other platforms and close out audit findings in the process. AD bridge products can also smooth over the integration of the increased number Mac OS systems in the enterprise.

• **Security information management (SIM)** is not usually considered an identity management technology. Recently, however, enterprises have been using SIM products in ways that complement their identity management initiatives. In addition to incident management, enterprises are now leveraging SIM products to assist with authorization. With the SIM product, application owners can evaluate user access over a specified time at the beginning of an application security review. Getting authorization right means getting security right, with the added benefits of closing compliance gaps and audit findings.

• **Entitlement management** provide a much deeper level of authorization capabilities with the added benefit of eXtensible Access Control Markup Language

PURCHASING

Full Evaluation Required

ORGANIZATIONS CAN RUN INTO PROBLEMS IF THEY DON'T CHECK OUT ALL THE PIECES OF AN IDENTITY MANAGEMENT SUITE.

WHEN CONSIDERING AN identity management suite, don't make the same mistake that many of your colleagues have made by failing to thoroughly evaluate all identity management products under consideration before a purchase.

Most organizations begin their evaluations by looking for a single product to meet a pressing need. At purchase time, the vendor then offers the customer a steep discount to compel the purchase of multiple identity management products. The deployment of the primary product goes well, but then the organization finds out that the other purchased products don't meet its needs, or require significant customization to work.

Multiple products from the same vendor can be a good fit, but organizations need to vet all of the products before writing the check. The additional evaluation work takes time, but it's worth the effort. Install the identity management products in your development environment, and test them against your existing applications, particularly your enterprise resource planning (ERP) applications and Active Directory infrastructure. Finally, don't hesitate to get a pilot user group to test the products. ›

–MARK DIODATI

(XACML) interoperability. This interoperability provides investment protection by enabling enterprises to build components which should work with multiple entitlement management products. When the products were first introduced several years ago, enterprises had to develop their own custom components. The vendors are now providing plug-ins for application servers like IBM WebSphere and Microsoft Windows platforms (including SharePoint). Entitlement management products are hardly mainstream, but many large financial institutions with challenging compliance mandates have deployed them.

• **Virtual directories** products provide a valuable service. They enable maximal consumption of user and policy information by the security applications that need this information. Virtual directories can present this information via LDAP. Behind the scenes, virtual directories map the information from a variety of repositories, including relational databases, LDAP directory servers, Active Directory, and even the mainframe without implementing an expensive and time-consuming meta-directory. In the past, the default consumer of information from virtual directories has been WAM systems. Recently, enterprises are deploying virtual directories for other identity applications including entitlement management, federation, and enterprise single sign-on (SSO).

• **Enterprise SSO** products try to solve the "last mile" problem by reducing the number of sign-ons to client/server and mainframe applications. Enterprise SSO products have been available for well over a decade, but their deployment has recently picked up, especially in the healthcare and financial service markets. Enterprise SSO products have become easier to deploy because they require less customization than in the past. A new trend is transaction-level integration between enterprise SSO systems and the target application. One example of transaction-level integration is a healthcare application that prompts the enterprise SSO application to re-authenticate the doctor before allowing the writing of a prescription.

Integration

In many cases, identity management products can be blended to reap additional benefits.

For example, organizations are integrating enterprise SSO with provisioning and strong authentication products to improve application security. Provisioning products provide better security because they can change passwords more frequently in both the target application and the user's enterprise SSO wallet. Strong authentication systems (like OTPs) solve the "keys to the kingdom" problem—eliminating weak password-based authentication, which enables access to many applications.

Meanwhile, WAM and federation products are "best friends forever" because neither product provides the complete security package for Web applications, but when combined, work synergistically. WAM provides the authorization and session management, while federation provides the enterprise-to-enterprise (E2E) SSO functionality.

Another trend in the enterprise is the coupling of provisioning and strong authentication systems (e.g., OTP or smart card). When integrated, the provisioning system can manage most aspects of the authentication device. Two benefits are the elimination

of near-duplicative identity management processes and timelier identity lifecycle management, which becomes especially important when employees are terminated.

Another integration example is the use of Active Directory in conjunction with an AD bridge product to provide central authentication and authorization services for non-Windows platforms. One vendor, Likewise, provides a free, open source AD bridge product that can unite Active Directory to non-Windows platforms.

Suites Not Necessarily the Answer

Instead of going to the trouble of integrating identity management products, why not just buy a suite from a single vendor? The ostensible benefits of purchasing a suite include a lower average price per product, and vendor-specific synergies

PRODUCTS

ID Management Vendors

HERE IS A PRODUCT SAMPLING OF IDENTITY AND ACCESS MANAGEMENT SOLUTIONS. BY MARK DIODATI

Privileged account management

Cloakware, www.cloakware.com
Cyber-Ark Software, www.cyber-ark.com
eDMZ Security, www.e-dmzsecurity.com
Lieberman Software, www.liebsoft.com
Passlogix, www.passlogix.com
Symark, www.symark.com

Active Directory bridge

Centrify, www.centrify.com
Likewise Software, www.likewise.com
Quest Software, www.quest.com
Symark, www.symark.com

Security Information Management

ArcSight, www.arcsight.com
CA, www.ca.com
EMC/RSA, www.emc.com
IBM, www.ibm.com
Intellitactics, www.intellitactics.com
NetIQ, www.netiq.com
Novell, www.novell.com
SenSage, www.sensage.com

Entitlement management

Bayshore Networks, www.bayshorenetworks.com
CA, www.ca.com
Cisco Systems, www.cisco.com
IBM, www.ibm.com
Jericho Systems, www.jerichosystems.com
Oracle, www.oracle.com
Sun Microsystems, www.sun.com

Enterprise SSO

ActivIdentity, www.actividentity.com
CA, www.ca.com
Novell, www.novell.com
Passlogix, www.passlogix.com
Sentillion, www.sentillion.com

Virtual directories

Optimal IdM, www.optimalidm.com
Oracle, www.oracle.com
Radiant Logic, www.radiantlogic.com/main
SAP, www.sap.com
Symlabs, www.symlabs.com

between the products.

While it is probable that the average software cost per product will be lower, experience has shown that most organizations end up paying more due to substitute software products or customization services. *[See sidebar, p. 7]*

As for vendor-specific synergies between products, very few exist. These synergies are generally divided into two areas: a common administration console, and enhanced interoperability between products. A common administration console across the vendor's identity management products provides value if the same IT people are managing multiple identity management products. Identity management products from the same vendor provide very few interoperability features over the interoperability that exists across identity management products from different vendors. Some examples of cross-vendor interoperability include: federation products which support cookie types for different WAM systems; WAM products which work with virtually any directory server; and provisioning systems that target platforms from different vendors.

IAM in a Tough Economy

While there are numerous benefits to IAM technologies, the current fiscal environment means that identity management projects are facing increased scrutiny. Organizations must be especially careful about identity management product selection, derive more value from their existing products, look for hard cost savings, and consider building identity management functionality in-house.

While there are numerous benefits to IAM technologies, the current fiscal environment means that identity management projects are facing increased scrutiny.

First, organizations should look for buried treasure within their identity management product licenses to determine if they can get more value from their existing solutions. For example, many early WAM deployments started and ended with Web servers because the WAM technology did not provide authorization to other platforms such as application servers and ERP applications. Times have changed, and today the WAM system may be able to provide security for these platforms without additional license purchases.

Another cost-saving strategy, is the use of Active Directory in conjunction with an AD bridge product to provide central authentication and authorization services for non-Windows platforms.

As IT budget gets cut in difficult economic times, the buy versus build equation changes. In many cases, organizations can tactically solve some problems by developing small identity applications. Examples include self-service portals, provisioning connectors for internally developed applications using Service Provisioning Markup Language (SPML), and developing SIM applications using tools like Splunk.

As the economy improves, organizations will swing back to a buy mentality and identity management products will continue to evolve to meet organizational needs. Privileged account management, AD bridge, and virtual directory products will close compliance gaps and reduce costs.

Advancements will indeed take hold where identity management technology evolves to provide identity services. What's more, the service-based approach will enable the products to interoperate more deeply via standards-based protocols offering more integration than ever before.›

Mark Diodati, CPA, CISA, CISM, has more than 19 years of experience in the development and deployment of information security technologies. He is senior analyst for identity management and information security at Burton Group. Send comments on this article to feedback@infosecuritymag.com.

Focused on finance?

Introducing SearchFinancialSecurity.com!

Now there's an online resource tailored specifically to the distinct challenges faced by security pros in the financial sector. *Information Security* magazine's sister site is the Web's most targeted information resource to feature FREE access to unbiased product reviews, webcasts, white papers, breaking industry news updated daily, targeted search engine powered by Google, and so much more.

Activate your FREE membership today and benefit from security-specific financial expertise focused on:

- Regulations and compliance
- Management strategies
- Business process security
- Security-financial technologies
- And more

www.SearchFinancialSecurity.com

SearchFinancialSecurity.com

The Web's best information resource for security pros in the financial sector.

Controlling Privileged Accounts

Regulatory requirements and economic realities are pressuring enterprises to secure their privileged accounts. Applied correctly, technology can help offset the risks.

BY MARK DIODATI

IN THE WRONG HANDS , privileged accounts represent the biggest threat to enterprises because these accounts can breach personal data, complete unauthorized transactions, cause denial-of-service attacks, and hide activity by deleting audit data. Privileged accounts, such as the UNIX root, Windows Administrator accounts or accounts associated with database ownership and router access, are required for platforms to function. Moreover, they are required for "break the glass" emergency access scenarios as well as more mundane day-to-day tasks.

While important, they are notoriously difficult to secure because they don't belong to real users and are usually shared by many administrators. However a down economy increases the risk of disgruntled workers, making it more important than ever to have a system in place to control privileged access.

What's more, control of privileged accounts is at the top of the auditor's findings list, and is an essential component of compliance mandates associated with Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI DSS), the

Federal Energy Regulatory Commission (FERC), and HIPAA. If those mandates aren't enough, many business partners are asking for a review of controls associated with privileged accounts as part of their Statement on Auditing Standards (SAS) 70 reviews.

Let's take a look at the technology and strategies that are available to help organizations can get better control over their privileged accounts.

Privileged Account Management Tools

Privileged account management products can help mitigate the risks associated with elevated access. These products can help close out audit findings, assist in meeting compliance mandates, and increasingly enable an organization to pass its SAS 70 reviews.

Clearly, privileged account management products have met a need in the enterprise: the product class has experienced explosive growth in the past three years, with the number of customers doubling every year. The number of organizations that have deployed a privileged account management product now exceeds 2,000.

Privileged account management products control access to accounts via two mechanisms. The first mechanism forces the administrator or program to check out the account password and the second mechanism changes the account's password frequently on the target platform. These products also provide some workflow capabilities for approval and follow-up after giving emergency access to a privileged account.

CHECKOUT METHODS. Traditional identity management provisioning systems are not up to the task of managing privileged accounts because they lack checkout methods. But privileged account management tools provide two password-checkout methods: interactive and programmatic.

In an interactive checkout, system administrators use the privileged account to access target platforms. Typically, the system administrator authenticates to the privileged account management product via a Web browser session. Once authenticated, the system administrator retrieves the specific account password, then uses the password in an interactive session such as Windows Terminal Services, Secure Shell, telnet, or a SQL client.

Programs also need access to privileged account credentials. Examples of programmatic access include: shell and Perl scripts for the startup, shutdown, and maintenance of target platforms including databases and application servers; services controlled by Windows Control Manager; and configuration files for database and LDAP account connection information. These access methods have traditionally required the embedding of the privileged account management password. The embedding of this password is a significant security risk, because anyone with access to the script or configuration file can steal the password and use it maliciously.

FIGURE 1: **PRIVILEGED ACCESS**

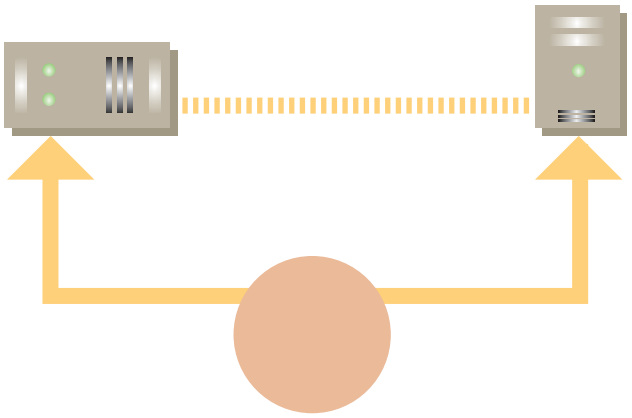
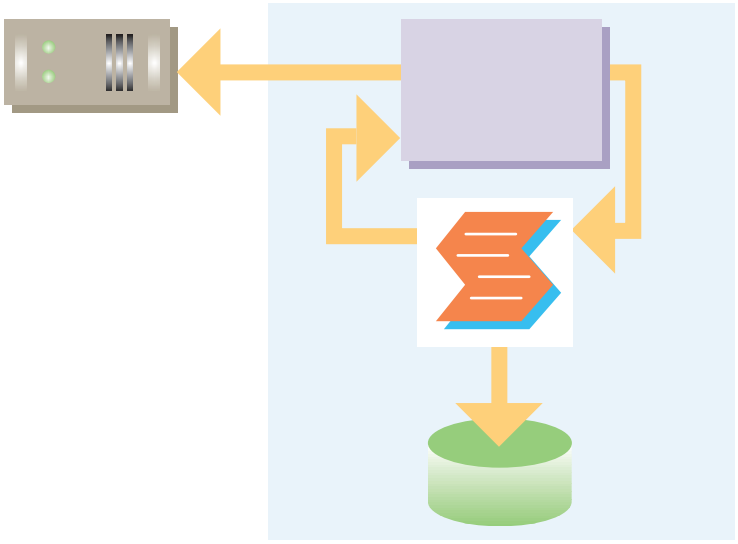


FIGURE 2: **PRIVILEGED ACCESS**



Privileged account management products have tools to help remove the embedded password, and programmatically retrieve it as needed. Programmatic retrieval requires the installation of privileged account management middleware on the target platform. This software enables the program to retrieve the account password in real-time. In some cases, a Secure Shell client residing on the target platform can be used in lieu of middleware.

The interactive access method is by far the easiest to secure, and most organizations tackle it first. The protection of accounts via the programmatic access method requires an inventory of all the places where the account password is stored, then replacing it with execution code that retrieves the password on the fly. Shell scripts and Perl files are relatively easy, but other programmatic access methods can require considerable work.

In particular, account passwords embedded in configuration files—for example those associated with application servers—are more difficult because the privilege account management product cannot control when the configuration file is read. Some of the vendors are addressing difficult programmatic access methods like application servers with modules specific to the application server. While tackling programmatic access requires elbow grease, companies that ignore the embedded privileged account passwords do so at their peril; in most cases these accounts can be used for interactive sessions by intruders.

PASSWORD CHANGE FREQUENCY. When controlling access by routinely changing an account's password on a target platform, privileged account management products provide organizations with several options, including:

- Never (not recommended but may be required for antiquated target platforms)
- Frequently (configurable, but the range is generally between one to 30 days)
- Per session (otherwise known as the exclusivity option)
- On demand

Most companies opt to frequently change most of the account passwords. Deployments in early stages typically change the password less frequently, for example every two weeks. As deployments mature and an organization gets more comfortable with the privileged account management product, passwords are changed more frequently; daily changes are common.

For very sensitive systems, some businesses implement the exclusivity option. With this option, the system administrator must "check in" the password when done with the session. The benefit of the exclusivity option is that it provides tighter accountability because the

checkout can be closely associated with subsequent actions executed by the privileged account. After the system administrator checks the account in, the product randomizes the password. The password randomization effectively means that no system administrator knows the password until it is checked out again. When the next system administrator checks out the account password, she has "exclusive" access to the account. All subsequent activity can now be correlated to this system administrator. Most organizations reserve the exclusivity option for very few high security systems because of its operational limitations: only one user can access target platform via the account at any given time.

The on-demand password change mechanism is becoming increasingly important in these economically turbulent times. When a system administrator's employment is terminated, timely revocation of access to privileged accounts is essential. The on-demand password change effectively locks the terminated administrator out of sensitive systems, because he no longer has knowledge of the account passwords.

PRIVILEGED SINGLE SIGN-ON (SSO). Single sign-on is a recent feature added to privileged account management products. The system administrator accesses the target platform via the privileged account management product's workstation client software or proxy server. Both mechanisms provide single sign-on because the system administrator is transparently logged into the target platform. Behind the scenes, the privileged account management software retrieves the password and logs the user onto the system via the session protocol (for example, telnet, Secure Shell, and Windows Terminal Services). Enhanced security is an additional benefit because the system administrator does not have knowledge of the account password.

PROGRAMMATIC PASSWORD CACHING. Highly-distributed production environments such as large retail corporations are at a disadvantage if the account management password cannot be retrieved due to network issues. Additionally, some target platforms use the account password frequently during processing, and the constant retrieval of the privileged account password would bring processing to a grinding halt. Some of the privileged account management vendors have responded by providing the ability to cache the account password on the target platform. Caching introduces additional security risks, relative to retrieving the privileged account password dynamically. However, caching is a much better alternative than leaving the password embedded in files. The account password will be more difficult to steal because it will not be resident in the file, and the password will be changed more frequently.

Important Considerations

While privileged account management tools can help organizations deal with a tricky security problem, they should be integrated with SIM and identity management systems to be truly effective. In addition, enterprises should leverage any platform privilege delegation capabilities, which reduce the need to give access to privileged accounts in the first place. Important systems also should be physically secured to help reduce the risk of intruders bypassing logical security controls.

SECURITY INFORMATION MANAGEMENT. The auditing of privileged account passwords is an essential component of successful compliance initiatives. Most organizations want the ability to determine who checked out the account and when the account was checked out. All of the privileged account management products possess this capability. Additionally, most

of the products can forward audit events to the Windows Event Log or a syslog collector.

To obtain full auditing benefits, a privileged account management product usually needs to be integrated with a Security Information Management (SIM) tool. While privileged account management products will happily log all account checkout events, that's only part of the picture. Checkout events need to be correlated with the subsequent actions taken with the privileged account. Some correlation may be possible via Windows Event Log or syslog, but organizations will benefit by spending the extra time integrating the privileged account management tool with an existing SIM tool. In some cases, the product will integrate directly with the SIM tool; in other cases the integration is achieved via syslog or the Windows event log.

IDENTITY MANAGEMENT. The integration of a privileged account management product with a provisioning system provides two benefits. The first is timeliness; the provisioning system can make real-time updates to who can access the accounts. The best example is the timely removal of access to all sensitive systems when an administrator's employment is terminated. Another example is removing access to sensitive production resources when the administrator changes job function or location. The other benefit is better security; the provisioning system's role management capabilities can restrict access to privileged accounts to authorized system administrators. For example, only system administrators in Chicago can access the accounts associated with the systems in Chicago.

Most of the privileged account management products have integration with the large identity management vendor provisioning systems. In some cases, an LDAP-based directory server can be used as a conduit between the provisioning and privileged account management systems when formal interoperability does not exist.

PRIVILEGE DELEGATION. Target platforms that can delegate privilege to real users can diminish but not eliminate the need for a privileged account management product. For example, the Microsoft Windows platform has good capabilities in assigning privilege rights to users, without giving access to the Administrator account. In general, UNIX platforms have delegation capabilities, but this varies by platform. Many organizations use UNIX security products to delegate privilege and therefore reduce the need for accessing the root account.

Some platforms, such as network routers, don't possess the necessary delegation capabilities. For these platforms, the best option is the use of a privileged account management tool coupled with a SIM product.

PHYSICAL SECURITY. Of course, in controlling privileged access, don't forget about physical security. Physical security almost always trumps all logical controls. Ensure that only authorized personnel can access the "raised floor" (that is, the data center) where the target systems physically reside. In some cases, people have general access to the data center, but should not have access to specific systems. In this case, consider a locked cabinet inside the data center.

To be sure, controlling privileged access is an issue that organizations cannot afford to ignore. Failing to secure privileged accounts could mean failed audits and worse, a data security breach with devastating consequences to the business.

Mark Diodati, CPA, CISA, CISM, has more than 19 years of experience in the development and deployment of information security technologies. He is a senior analyst for identity management and information security at Burton Group. Send comments on this article to feedback@infosecuritymag.com.

> *Identity management solutions from Sun*

GET AN OUNCE OF PREVENTION AND A POUND OF CURE

SUN COMBINES PROVISIONING AND AUDITING TO PREVENT AND DETECT COMPLIANCE VIOLATIONS

Sun Identity Manager is the first complete solution proven to reduce the cost of managing identities inside and outside your business. At the same time, it mitigates compliance risks and makes the compliance process repeatable and sustainable.

> Reduce costs for provisioning and identity auditing
> Enable repeatable, sustainable compliance
> Reduce security risks
> Scale to millions of users, including extranet users

Stay connected to identity management news and trends by joining the Sun Identity Insights Program at **www.sun.com/identity**.

Do IAM Suites Make Sense for Your Organization?

Feature-rich suites are putting a face on integration and interoperability.

BY BRIEN POSEY

COMPLIANCE AND CONSOLIDATION are at the forefront of IT security, especially when it comes to identity and access management (IAM).

Today's regulatory environment requires companies to track and control who has access to what. Meanwhile, the tools for managing that access have grown from sets of distinct products into full-blown suites. It's a result of the wave of acquisitions overtaking the IT security marketplace, with larger vendors gobbling up smaller players to broaden their security portfolios. Even companies not known as traditional players in the IAM market, like database giant Oracle, have jumped onto the playing field.

And identity and access management is hot. In a recent study, Forrester Research projects the IAM market to grow from $2.6 billion in 2006 to $12.3 billion by 2014, driven largely by compliance.

Forrester also notes that enterprises are shifting away from point products to integrated, feature-rich identity suites to ensure interoperability. Companies are looking for solid players that will be around a long time, grow with them and provide support. Suites offered by established industry players meet this requirement. But they can be time-consuming and costly to deploy, and not live up to their promise of providing an identity panacea.

Consolidation Recap

Prior to 2005, the traditional players in the IAM market were Novell, Sun, IBM and Microsoft. They offered basic identity management products linked to directory services, such as Active Directory (Microsoft) and LDAP (Sun). Other vendors at the time were SAP, BMC, CA and RSA Security, offering various pieces of the identity puzzle such as provisioning and authentication. Many smaller players offered niche products like role management and virtual directories.

Then two things happened in 2005: compliance with regulations such as Sarbanes-Oxley (SOX) started to hit full swing and the acquisition wave took hold. Oracle surprised industry observers with its purchases of two start-ups, user provisioning vendor Thor and virtual directory specialist OctetString. The additions followed Oracle's acquisition that year of Oblix, a supplier of Web access controls. Also in 2005, CA acquired software from InfoSec to clean up obsolete identities, and BMC grabbed Web access vendor OpenNetwork Technologies and Calendra, a supplier of directory management products.

The consolidation wave continued in 2006. Sun acquired Neogent, a product for automating identity management, while RSA acquired Web site authentication companies Cyota and PassMark Security and in turn was snapped up by storage giant EMC. In 2007 Oracle bought Bharosa, a supplier of strong authentication for Web sites, and Bridgestream, an enterprise role management software company, while Sun purchased Vaau, another role management vendor. Meanwhile, IBM acquired enterprise single sign-on (SSO) vendor Encentuate.

All these acquisitions have largely shifted the IAM market to a few big players offering integrated suites.

All these acquisitions have largely shifted the IAM market to a few big players offering integrated suites. There are plenty of small vendors offering standalone products, but three areas in particular could be potential takeover targets for larger vendors looking to round out their suites: enterprise SSO, virtual directories and privileged account management.

Key Functions

Identity and access management suites combine technologies that fall into four broad, interrelated categories: identity administration, identity infrastructure, access management and auditing.

Under the identity administration umbrella sits user provisioning, role management, privileged user account management and enterprise role management. The distinction between role management and enterprise role management is important. While traditional role management is static, just setting up users in roles and groups, enterprise role management is dynamic. It is role-based authentication that can cross multiple business units and functional areas in a company and be flexible to shift around roles as the structure of users change through company growth and acquisition.

Identity infrastructure includes anything holding identity information: directories, virtual directories and meta directories. Access management includes overseeing access to multiple applications as well as SSO technologies, both for the enterprise and the

Web, and federated identity management, a close relative of SSO. Auditing includes keeping track of users and their roles, which overlaps a bit with all of the above.

An obvious upside to suites is that they offer the whole IAM pie to customers—suites are a one-stop shop for the four main functional areas of IAM. All of them offer user provisioning, while enterprise SSO is a component of some large suites, including those from BMC, CA, IBM, Novell and Oracle. Evidian, a specialist in SSO and federated identity management, has those functions as the centerpiece of its suite.

Andras Cser, Forrester senior analyst, says enterprises are looking to integrated product sets for interoperability and streamlined support; it's easier to get a technical fix with a suite than with individual products. Pricing is another motivator. "If you're trying to buy a lot of functionality and even if you don't need it, the chances of getting and buying functionality are cheaper," he says. And for the most part, suites have caught up with point products in functionality, Cser adds.

Aside from helping enterprises avoid the integration headaches associated with separate products, suites can allow companies to centralize access management functions. They have a single GUI or Web interface with dashboards for providing provisioning, managing roles and groups and for managing directory services.

Aside from helping enterprises avoid the integration headaches associated with separate products, suites can allow companies to centralize access management functions.

Integrated suites also centralize directory management, making different directory services like Active Directory and LDAP play together. Many companies use a mix of systems—mainframes, Windows and Unix environments—that were cobbled together as they grew internally or through acquisitions. Rather than rip out all their perfectly operational identity plumbing like RACF, Active Directory or LDAP, most enterprises would rather work with their existing directories. They just want the ability to manage them all with a single tool. The need to work with different directory services, which can't be easily consolidated or replaced with a single directory service, is a fundamental issue for many large enterprises.

Another advantage with IAM suites is the ability to produce reports. Reporting is at the heart of compliance with regulations like SOX, HIPAA and industry standards like the Payment Card Industry Data Security Standard (PCI DSS). Rather than relying on another product like Cognos or Actuate to crank out a report, a suite may be able to generate reports and store the data in a database for retrieval. An example is Oracle Access Manager, which leverages the company's database capabilities to store access information from different components of the suite. It has pre-built reports that can be used for compliance purposes to identify who has access to what systems. The report templates can also be used for incident management to record user access attempts or failed logins—a tell-tale sign of hacker mischief.

Reports may be Web-based or in hard copy for auditors and regulators, and they may also be integrated with security information management systems, as CA does with its suite.

Buyer Beware

But suites don't always deliver on their promise to be the panacea for all of an enterprise's IAM issues. First off, rolling out an entire IAM suite can be a time-consuming and costly venture for any company. Depending on the size of the organization, the costs could start in the hundreds of thousands of dollars and go up from there. For an enterprise with hundreds of offices and operations around the globe, deployment of a full suite is usually done in stages and can take a couple of years, and then only if everything goes smoothly. An enormous amount of planning goes into integrating an IAM suite with a company's architecture and existing directory services, including set up or migration of users, roles and groups to the new system.

Second, not every product set excels in everything. A product that is outstanding in provisioning may not be as good at reporting, for example, or its GUI or Web interface may be difficult to navigate.

The growing set of features in suites also makes buying decisions more difficult. The business requirements of most companies don't always match one-to-one with every feature. According to Forrester, this is further complicated by more stakeholders such as auditors and non-technical business people involved in the selection process and purchase of an identity solution.

While suites generally offer broad functionality, they tend to lack two newer technologies: virtual directories and privileged account management.

While suites generally offer broad functionality, they tend to lack two newer technologies: virtual directories and privileged account management. Virtual directories are servers that can access identity information in real time from multiple sources in a single view without storing identity data themselves. This allows multiple directories to be queried by accessing only the virtual directory, which, in turn, accesses the physical directories to answer the identity query. Virtual directories are used for SSO and federated identity management. Only Oracle, Sun and SAP have their own full virtual directory capabilities.

And privileged account management, which protects system administrator accounts, is in demand because of compliance concerns, but isn't fully represented by any of the major IAM suites.

What's Ahead

As the mix of systems, portals and applications— whether Web-based, client-server or mainframe—becomes increasingly complex, the need for tighter access control will grow as companies work to meet compliance demands. This will require the type of fine-grained entitlement management not currently found in IAM suites. Entitlement management further restricts access to systems and applications beyond just the types of roles and groups in traditional access management systems. It can involve restricting access based on time of day, geographical location or even type of transaction.

Compliance requirements are also affecting the growth of the IAM suite in the area of multifactor authentication. An example is the directive in 2005 from the

Federal Financial Institutions Examination Council (FFIEC) recommending two-factor authentication for Web-based banking. So not only do IAM suites have to handle standard user IDs and passwords, they're now expected to handle smart cards, one-time password (OTP) tokens and even biometrics.

This trend will grow as IAM suites will also have to bear the burden of the integration of logical and physical security, much of it underpinned by smart cards and other two-factor authentication devices.

The evolution of IAM suites is driven both by the natural trend of consolidation in all industries and market demand for compliance tools. Compliance doesn't equal security but, for better or worse, compliance is king, and IAM suites are just following the lead.

Brien Posey is a five time Microsoft MVP who has written thousands of articles and whitepapers over the last thirteen years, and written or contributed to dozens of books. Prior to becoming a freelance technical author, Brien has served as a CIO for a national chain of hospitals and healthcare facilities, and was once a network administrator for the Department of Defense at Fort Knox. He has also served as a network administrator for some of the nation's largest insurance companies. Send comments on this article to feedback@infosecuritymag.com.

Of course your employees wouldn't abuse their access to sensitive data.

Unless you left the door open. Find out with Symark's free 30 day trial.

80% of computer crime is an inside job. With Symark's Access Control and Identity Management products, you'll be able to identify and strengthen your security's weak points, manage access, and allocate privileges. You can track who's doing what, where and when. And Symark's security products are easy to deploy and provide rapid ROI. Our commitment to quality products and superior technical support has made us the leading vendor of security administration solutions in heterogeneous UNIX and Linux environments worldwide. For more information, visit our web site at www.Symark.com/30daytrial. And outfox those who would put your company at risk.

symark
Control Access. Control Risk.™

Symark's free 30 day trial:

POWERBROKER®
UNIX/Linux Access Control & Accountability

www.symark.com

US & Canada: (800) 234-9072
Europe: +44 (0)8704 586 224
International: +1-818-575-4000

IAM Priorities
IN DIFFICULT ECONOMIC TIMES

BY DAVID GRIFFETH

The challenge for identity and access management professionals will be securing data from former employees who know the system from the inside out.

WHAT CHALLENGES will 2009 bring for identity and access management professionals? With the world economy in a state of turmoil, markets correcting themselves and employers reducing staff, the pull of illicit insider activity is stronger than ever.

Companies across all sectors have already begun to lay off staff. It may begin with the "dead wood," but inevitably some companies are going to have to lay off talented IT and information security professionals. Illegal activities that once seemed unpalatable to out-of-work technologists may seem better than starving: Just as liquor store break-ins and gas n' go crimes will increase, so will more sophisticated crimes, such as data theft and social engineering. While it may seem hard to imagine, criminal actions are often committed by former employees who rationalize the activity because they're upset about losing their jobs.

Defense Strategies: Proactive IAM Processes

Locks keep honest people honest, or, in the case of identity and access management, account terminations keep honest people honest. Identity management and information security professionals will need to scrutinize their account-termination processes like never before, because leaving an unauthorized or former employee's account active and enabling access to sensitive or valuable data could be catastrophic. Make sure to have an updated roster of every account owned by every individual in the company so that all those accounts can be deleted or disabled if anyone is terminated.

Now is the time to be proactive. Assess and refine existing processes. How long has it been since the company's entire account life cycle process was last evaluated? Are you confident in the integrity of that process, including the external data it depends on, such as HR feeds? Is the governance data for contractors sufficient and timely? Are there appropriate separations of duties, and are they adhered to? If the answers to these questions are unclear or unknown, alert management and start evaluations for process improvement.

Budget Cuts: Using Frameworks and Documentation

Another challenge in 2009 will be funding. Budget promises made in 2008 are sure to be forgotten as many companies adjust to the new economic reality. So how will enterprises properly secure data when the funding to do so may seem insufficient? Innovation. Set up a framework that is effective, even if manually intensive. An example of this may be an Excel- or Outlook-based quarterly report for system owners that details accounts with privileged access, identifies owners and partners, establishes roles, and archives emails on a secure file share. This will initiate an ongoing process that can be refined in the future, perhaps with more sophisticated technology, when finances are better.

Budget promises made in 2008 are sure to be forgotten as many companies adjust to the new economic reality.

There are a few other important strategies for making sure the security program doesn't suffer because of financial cuts. If you have documented what your people do on a day-to-day basis in detail, now is the time that information may pay off; it may allow you to not only justify exactly why each person is important, but also clearly demonstrate what the fall-out will be if the staff is reduced. Personnel reductions may still be mandated, but data can help you make those hard decisions in an unbiased way and set management expectations from the start about the consequences of staff reduction.

Important statistics to keep may include how many accounts are under management, turnaround time for account creation and removal, reporting demands from various departments, and objects under management such as mainframe profiles and Active Directory groups. If these statistics haven't been kept in the past, start keeping them now, then pick data that will help management see the security team in the most favorable light possible. Spotlighting the hard work you do is not arrogant if it's based in fact, and more importantly, it may save someone's job.

In such a troubled economy, external threats will increase as well. There will be

plenty of talented developers out of work that may discover their skills make them excellent bot programmers or hackers. While these threats are too numerous to detail here, it's still essential to be on guard by making sure the controls for external risk mitigation are assessed as well.

It's clear that 2009 will be drastically different from 2008. Rely on what has been tried and true in the past, but be ready to innovate and improve quickly based on new threats and changing business needs.

David Griffeth is the Vice President of Business Line Integration and Reporting at RBS Citizens Bank, a financial institution that is one of the 10 largest commercial banking companies in the United States ranked by assets and deposits. As part of his responsibilities, David manages the Enterprise Identity and Access Management group and is charged with supporting the bank's growth model while maintaining compliance with several regulatory bodies. Prior to his current position, David consulted on major information risk management projects with large companies such as Fidelity Investments and CIGNA. David earned a bachelor's degree in computer science from Framingham State College and holds several certifications including CISSP and CISA. Send comments on this article to feedback@infosecuritymag.com.

thawte™
it's a trust thing™

Building Trust Around The Globe

When you want to establish trusted relationships with anyone, anywhere on the internet, turn to *thawte*. Securing Web sites around the globe with:

- strong SSL encryption
- expansive browser support
- multi-lingual customer support
- recognized trust seal in 18 languages

thawte offers outstanding value on a full range of digital certificates. Secure your site today with a *thawte* SSL Certificate.

www.*thawte*.com

LDAP Yesterday, Today and Tomorrow

The popular directory service continues to be the cornerstone for IAM.

BY JOEL DUBIN

THE POPULARITY OF LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP) as a directory service continues to grow. Its tree-like structure for grouping network users was revolutionary when it premiered in 1993. Since then, it has become the primary model for directory services, including Microsoft's Active Directory.

Not being confined to Unix and Linux where it has frequently debuted, its flexibility, allows it to mesh with other directory services—not just Active Directory—and support newer types of authentication, such as smart cards and biometric devices.

Though LDAP is the predominant directory service for Unix and Linux, it can support user access via other operating systems, and has become the main directory protocol on the Internet.

So where is LDAP headed? To answer that question, we need to see briefly where LDAP has been, as well as explain what LDAP is, what it does and why it's unique.

LDAP History

First, LDAP is defined as a standard for directories, which are services that hold user account information. Directories can also hold other structured data, but for our purposes we'll limit the discussion to user accounts. LDAP began as a gateway service between other directory services before developing into a directory specification itself, complete with standards for details down to the structure of its own user databases.

Prior to LDAP, directory services were developed by the telecommunications industry to keep track of customers. Directory services were originally seen as computerized phone books. Not surprisingly, the first standard, X.500, was developed by the International Telecommunications Union (ITU) in 1988.

LDAP was developed in 1993 at the University of Michigan as a simple way to access the first X.500 directories. Those first directories sat on servers called Directory Service Agents, which communicated with clients by the more complex X.500 Directory Access Protocol. LDAP was meant to make that easier, or more "lightweight," as the "L" in LDAP implied.

Two years later, the next version, LDAPv2, was released in a series of three RFCs. LDAPv2 removed the dependence on X.500, including changing network connectivity from the Open Standards Intercommunication (OSI) to the more nimble TCP/IP model—the communications protocol for the Internet. This made it more compatible for Internet communications.

Then, in 1997, came LDAPv3. LDAPv3 improved support for directories not based on X.500, created a format for LDAP URLs, added security features like authentication and extensions for TLS—the latest version of SSL—and cleaned up schemas and string formats.

LDAP was developed in 1993 at the University of Michigan as a simple way to access the first X.500 directories.

LDAP Features

What makes LDAP unique is its tree structure, organizing users into hierarchies of groups? Each user is called an entry with its own unique identifier, or Distinguished Name (DN). Each DN has a series of attributes about the user, making it possible to mirror fine-grained access controls to users in the directory tree.

Though the details are beyond the scope of this brief introduction, each DN is an object, making it accessible to object-oriented programming languages, and it can also be constructed in a URL, making it accessible over the Internet via DNS.

Since the flurry of activity over a decade ago, there haven't been any new LDAP RFCs, nor has a new version come out. So does that mean LDAP is dying out? Far from it. LDAP has evolved and is stronger than ever.

Its ability to mesh with object-oriented programming languages and DNS makes it perfect for today's Internet-connected world. It also forms the basis of other Internet protocols, such as XML Enabled Directory (XED) and the Directory Service Markup Language (DSML).

LDAP's tree structure inspired Microsoft to take a similar approach with Active Directory, and the software giant has since made a commitment to LDAP: Active

Directory in Windows 2000 Server was LDAP-compliant. Microsoft expanded LDAP support in Active Directory in Windows Server 2003 and included the LDAP API in the Microsoft Developer Network (MSDN) Platform SDK.

Besides Microsoft, LDAP is supported in products from a veritable who's who of IT vendors, including Sun Microsystems, Inc., IBM Corp., Hewlett-Packard Company, Novell Inc., Red Hat Inc., Oracle Corp., Apple Inc. and Siemens AG. Each of these companies offers directory services that support LDAP and are LDAP compliant.

LDAP's Future

The future of LDAP lies in refinements to LDAPv3 rather than a new version. Most recent improvements added by vendors include upgrades to management GUIs that allow easier modification of users and their attributes. In other cases, as with Windows Server 2003, Microsoft added LDAP security and dynamic directory services that were already in LDAPv3 but not in Active Directory.

LDAPv3 is not without blemishes. There have been issues with its smart referral feature, which maps a directory entry to a specific URL, but these have been due to issues with vendor implementations and not LDAP itself.

If there is a lesson to be learned for an enterprise implementing LDAP, it's to choose a vendor that can take advantage of all the features LDAPv3 has to offer. And, of course, make sure that vendor is LDAP-complaint with certification from the Open Group—a vendor-neutral organization that sets IT standards, including those for identity management. The key is in the front end to LDAP, whether Active Directory or some other product.

If there is a lesson to be learned for an enterprise implementing LDAP, it's to choose a vendor that can take advantage of all the features LDAPv3 has to offer.

Perhaps LDAP's greatest challenge is one shared with any other directory service, including Active Directory: Its ability to adapt to the changes in the delivery of identity and access management, whether through new types of authentication like biometrics or through Software as a Service (SaaS) models. Its flexibility, scalability and ability to work with new technologies are what will keep LDAP alive. LDAP remains at the core of many directory services today because of this flexibility. And, it will remain so for the foreseeable future.

Joel Dubin, CISSP, is a former independent computer security consultant. He is a Microsoft MVP, specializing in web and application security, and the author of The Little Black Book of Computer Security, Second Edition*, available from Amazon. He hosts a radio show on computer security on WIIT in Chicago and runs The IT Security Guy blog at http://www.theitsecurityguy.com. Send comments on this article to feedback@infosecuritymag.com.*

THE STATE OF THE Authentication Market

BY MARK DIODATI

5 We'll explain five leading-edge authentication technologies and where these applications make sense.

WHILE STRONG AUTHENTICATION has been around for years, regulations such as FFIEC and HSPD-12 are fueling renewed interest in the technology. As a result, many established vendors and young startups are offering innovative and cost-effective approaches to a long-standing problem: accurately giving users access to information and applications. Here we'll outline some newer technologies and how these offerings could help you secure your organization.

Facial recognition software

Facial recognition software is in its early days for sure, but it does overcome some of the personal objections to biometrics people have with retina or fingerprint scans, because it's pretty easy to use. Its application primarily is with authentication to physical access control systems (PACS) where users are coming into the building and authenticating via facial recognition.

One of challenges for the adoption of facial recognition software is if it can support a very large organization. Think about people coming into the building at the beginning of the day that need to authenticate. You'd need separate booths for people to approach the facial recognition software.

There is also a significant infrastructure investment involved—not only at the front door, but if you've got physical access control systems, controllers, door panels and readers.

The HSPD 12 smart card

This is the Homeland Security Presidential Directive 12 smart card mandated by President George W. Bush. It requires every federal employee and contractor be issued a smart card. What makes it unique is that it is really the smart card of the future. It's a card that has a single chip for storage and processing and two interfaces: one for contact, that's the gold chip that we're all used to seeing for smart cards, and contact lists, which is our proxy-style technology. What makes it so leading edge is if you can use 200 facets to a single chip, you now have more advanced authentication credibility for physical access control systems, like certificate-based authentication or biometric matching.

The problem with the technology is, while it's a sound technological choice, it's largely incompatible with most federal agency's physical access control systems. So these agencies are forced to implement things like multiprotocol door readers or they have to rip out door readers, potentially rip out controllers, or implement something like a tri-interface card, which is a dual-interface card like a HSPD 12, but also has legacy-style physical access control authentication capabilities.

Authentication as a Service

This is an authentication service that exists out in the cloud, so it's not hosted on site at all. It's like an Oreo cookie from an architectural perspective. The bottom layer is all the different authentication mechanisms that might be accepted into the service. The middle layer is what we would call a security token service, so its job is to take the authentication and then flip it over to a token type that can be accepted. The top layer is what we can log users into now that they've authenticated to the service. For example, we'll log them into Salesforce.com, federated applications, including things like Google applications, even Web applications, requiring a user name and password.

So the user authenticates to the service in the cloud, and then gets access to all the external and potentially internal applications. There's been a high degree of interest in this, particularly with small to medium businesses. Large businesses also see the value in this capability because it relieves some of the burden of the authentications they have to manage.

One problem that varies across the different vendor products is provisioning capability, which is how users are defined to the Authentication as a Service cloud. Some have provisioning capabilities and others don't. So you may have an additional administrative burden defining users to the Authentication as a Service system so they can use this capability and authenticate only once for access to many external applications.

There are some risks when moving to a third-party provider. You certainly have to look at what controls are in place for authenticating and you need to understand not only how the service provider is doing the authentication, but also what's happening on the other side: that is, what applications are users getting access to. So, for example, if you're using federation, that's relatively secure. If you're using user names and passwords, where the user authenticates maybe with a one-time password (OTP) device to get access to password-protected websites, you're storing passwords. This means you need to determine whether those passwords are going

in the clear from the Authentication as a Service provider, and so on. You definitely have to look at and understand the external controls that will be in place with the Authentication as a Service to see if they meet your needs internally.

Card-based one-time password devices

OTPs remain the most prevalent, strong authentication mechanisms within the enterprise. These devices are truly portable and you don't need client software. There are instances where a software-based one-time password device is used, but that certainly isn't the majority use case. So they're portable and easily managed administratively.

What's more, users understand this idea pretty well, replacing a static password with this password and perhaps a PIN that comes off their one-time password device.

OTPs remain the most prevalent, strong authentication mechanisms within the enterprise.

What these credit card-sized devices do is they look like a credit card, they bend like a credit card, and they have the bank and the user's account number, among other things, on them. You can print on them but they also have a battery and a liquid-crystal display so they function as a one-time password device.

The devices also mitigate the token necklace problem more prevalent in the consumer space. They could fit in your wallet, so it's not a big deal.

There are some concerns however. They're still unproven on a very large scale, specifically when it comes to battery life and durability. The price is still relatively high, although it continues to come down. As the price comes down, the cost of shipping these things could become more expensive than the devices themselves. When this happens, you'll start to see more of these devices deployed.

Personal Portable Security Devices.

A Personal Portable Security Devices (PPSD) is a USB-style smart card. This is a relatively new technology in that the smart card chip controls access to the USB flash memory. It overcomes the problems with smart cards lack of storage space. If you have 128K or 256K smart card, you'll be able to store certificates and maybe a few SSO credentials, but not much more. PPSDs also overcome the security concerns people have with USB thumb drives. Unless you put in the right PIN, there's no way you're going to access what's on that flash drive with a PPSD. Because there's a smart card present, you have the ability to do native file encryption on the device, so it's highly tamper-resistant.

In a nutshell, it overcomes the space objections of smart cards and the security objections of USB devices. What's exciting is that it's also an authenticator, so it's a smart card and you could put certificates on it. The large storage capacity provides some interesting opportunities: you could actually store a whole desktop on it. You could store a hardened Web browser on it, or a complete single sign-on application—not just the credentials but the applications.

You can also set up a public and private area. You could set up a four gigabyte PPSD where one gigabyte is public, and freely readable just like it would be for any

other USB drive. So you could pass around PowerPoint presentations or whatever else without having to worry about authenticating, and the remaining three gigabytes would remain private.

The prices are still relatively high. They cost approximately $100 for one of them but prices will continue to drop.

Customization

When creating an authentication strategy, there are three things to consider. The first is figuring out what your information classification or identity assurance levels are. From there, you can derive what authentication mechanisms are required. Lastly, look at all of your applications where you want to use the stronger authentication mechanisms and figure out what works with them.

We have found that organizations need to mix and match these things. There's not one single authentication mechanism that will work well with their user constituencies and required applications.

Looking at some use cases, we see organizations move from one-time password devices to smart cards. One of the common things they might do is rather than buy hardware-base one-time password devices, they'll actually pick up a software-based one-time password devices that will be used in conjunction with a smart card to overcome, or to provide broader application ubiquity coverage.

Verticals for these authentication methods

With the facial recognition stuff, the sweet spot seems to be high tech manufacturing, where you've got some concerns about the physical security of the things you're making, but maybe your user population doesn't typically access a workstation, or they're moving around a lot. Facial recognition might be an area to investigate.

HSPD 12 is obviously a federal government initiative, but the commercial industry is watching this very closely because there were some smart decisions made about the technology for HSPD 12 smart cards.

With Authentication as a Service, the vendors are targeting small to medium businesses that don't want to own the technology. But we are aware of some very large organizations that are looking to deploy this as well, because there are benefits for pretty much everybody if you've got external applications out there, like Salesforce.com or Google apps.

The card shaped one-time password device is clearly the domain of the financial institutions and investment houses.

The card shaped one-time password device is clearly the domain of the financial institutions and investment houses, where they're looking to improve the security of what they're trying to do, as well as meet compliance mandates.

Finally, with the personal portable security device, you're looking at certain industry verticals, for example, financial services, that have a little extra money to spend: maybe they have a paperwork reduction mandate so they could use them to do some digital signing, which pulls on the certificate-based stuff. Or maybe they have high data breach protection needs, and are concerned about data being

exposed or lost and have a highly mobile user population. A personal portable security device would overcome some of those objections, because even if you leave it in the pocket of the airline seat, that data isn't recoverable. There's no way to access it unless you have the pin or the recovery key, which is something the administrator would have.›

Mark Diodati, CPA, CISA, CISM, has more than 19 years of experience in the development and deployment of information security technologies. He is a senior analyst for identity management and information security at Burton Group. Send comments on this article to feedback@infosecuritymag.com.

PRODUCTS

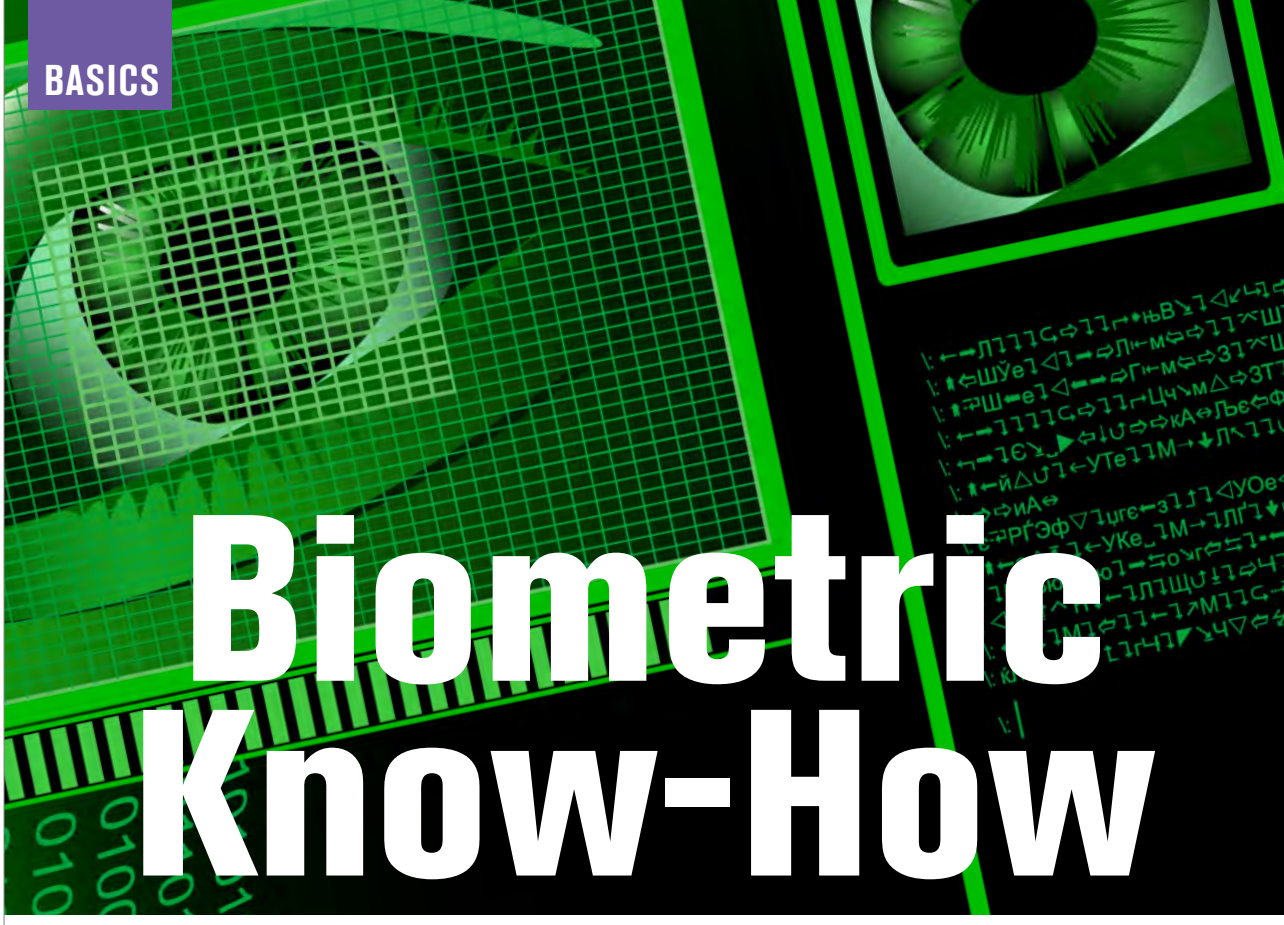
Here is a sampling of authentication offerings in the market.

COMPILED BY SEARCHSECURITY.COM EDITORS

A10 Networks, www.a10networks.com
ActivIdentity, www.actividentity.com
Aladdin Knowledge Systems, www.aladdin.com
Arcot, ww.arcot.com
Authenex, www.authenex.com
AuthenTec, www.authentec.com
Authentify, www.authentify.com
Biocert, www.biocert.com
CryptoCard, www.cryptocard.com
DataKey, www.datakeyeletronics.com
DigitalPersona, www.digitalpersona.com
Diaphonics, www.diaphonics.com
Entrust, www.entrust.com
FireID, www.fireid.com
Gemalto, www.gemalto.com
IBM, www.ibm.com
Imprivata, www.imprivata.com
Infoblox, www.infoblox.com
JANUS Associates, www.janusassociates.com
Juniper, www.juniper.net
L-1 Identity Solutions, www.l1id.com
Mocana, www.mocana.com
Phonefactor, www.phonefactor.com
Precise Biometrics, www.precisebiometrics.com
Privaris, www.privaris.com
RSA, the Security Division of EMC, www.rsa.com
SafeNet, www.safenet-inc.com
TriCipher, www.tricipher.com
Upek, www.upek.com
Vasco, www.vasco.com
VeriSign, www.verisign.com
Vidoop, www.vidoop.com

PKI/digital certificates

CA, www.ca.com
Chosen Security, www.chosensecurity.com
Comodo, www.comodo.com
Digisafe, www.digisafe.com
Entrust, www.entrust.com
Global Sign, www.globalsign.com
Opentrust, www.opentrust.com
RSA, the Security Division of EMC, www.rsa.com
Thwate, www.thwate.com
VeriSign, www.verisign.com



Biometric Know-How

Learn the ins and outs of this authentication method.

By SearchSecurity.com staff

What is biometrics?

Biometrics is an authentication method that uses fingerprint or facial scans and iris or voice recognition to identify users. A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify. Since it is more difficult for a malicious hacker to gain access to a person's biometric data, and it is unlikely that a user will misplace or misuse his or her biometric data, this form of technology a greater level of assurance than other methods of identification.

Biometrics can be used for both physical access to corporate buildings and internal access to enterprise computers and systems. Biometrics is most often used as a form of authentication in a broader two-factor or multifactor authentication system, since most biometric implementations also require employees to enter user IDs and passwords.

Biometric devices and systems

There are a plethora of biometric devices available—including fingerprint scanners, face and voice recognition, iris scans and keystroke dynamics—and it is important for an enterprise to choose a device that fits and addresses its specific needs, such as business infrastructure, system vulnerabilities and user access. Below is a brief description of some of the most popular biometric authentication devices and systems to help security managers learn the pros and cons and how to know if they are right for an organization.

Fingerprint scanners are one of the oldest forms of biometrics and have been largely reliable when is comes to authentication. These systems are easy to use, which makes them favorable among users, but like all authentication products they have some weaknesses. Fingerprints can be copied from a user's calculator or coffee mug, for example, for malicious access. They can also be troublesome if a user's fingerprint is damaged or altered (i.e. a cut or burned finger).

Face and voice recognition systems are similar to fingerprint scanners. Their ease of use makes them favorable, but a user's voice can be recorded and a face can be copied from a photograph, in some cases enabling third-party malicious access to systems.

Iris and retinal scans are considered to be a more secure form of biometric authentication, since copying a person's retinal pattern is a much more difficult task than copying a fingerprint.

Using a **keystroke dynamics-based authentication system** is another option. This technology measures a users keystroke style and speed—words typed per minute, common errors, letter sequence—and stores that information in a system directory to be used in the future to authenticate a user.

Biometric implementation

Implementation of biometric systems can be tricky and expensive, requiring corporate spending on hardware and software. The implementation and deployment processes varies for different biometric systems, so organizations must first carefully consider which type of system to deploy, and then meticulously plan the process.

Biometrics is an advanced technology intended to protect extremely sensitive data, so it should only be considered for highly sensitive material. Using biometrics for any other type of data would be a waste of time and money. Organizations should do a thorough risk analysis of their systems to determine what information is in need of protection via biometric technology, i.e. a customer's credit card information.

Organizations must also ensure secure transmission and storage of biometric data. Although biometric systems are considered one of the most advanced forms of authentication, they do have certain flaws. For instance, some people think it is impossible to duplicate a user's biometric information, but when it is converted into digital data, it can be stolen by a hacker as it transmitted through insecure networks and later replayed.

As stated earlier, organizations can decrease the likelihood of hackers gaining access to a users' biometric information by using data that is more difficult to copy, but the risk is still there. Considering, it is essential that enterprises take several precautions to ensure that the data is transmitted, gathered and stored properly.

Organizations must make sure that all information transmitted from the biometric reader to the authenticating server is gathered on a secure device, sent over an encrypted channel and stored in an encrypted database. Both Active Directory and LDAP can perform these actions. Finally, any servers running biometric applications must be patched and hardened.

Compiled by SearchSecurity.com staff. Send comments on this article to feedback@infosecuritymag.com.

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 117 Kendrick St., Suite 800, Needham, MA 02494 U.S.A.; Phone 781-657-1000; Fax 781-657-1100.

Arcot Systems, Inc.

See ad page 2

- How Arcot Solutions Protect Against Internet Threats

Digital Persona

See ad page 4

- Free Evaluation Unit
- Free White Paper

RSA, The Security Division of EMC

See ad page 12

- RSA Online Fraud Report: A Monthly Intelligence Report from the RSA Anti-Fraud Command Center
- Mitigating Man-in-the-Middle and Trojan Attacks Whitepaper
- Gartner 2009 Report: "Magic Quadrant for Web Fraud Detection"

Sun Microsystems

See ad page 18

- Sun Identity Management
- Attacking Complexity with Simplicity - Sun Identity Management - Webinar
- Keeping It Simple: A Pragmatic Approach to Identity Management - White Paper

Symark International, Inc.

See ad page 24

- From Trust to Process: Closing the Risk Gap in Privileged Access Control
- How Controlling Access to Privileged Access to Privileged Accounts Can Keep Insider Threat from Hurting Your Bottom Line

thawte Inc.

See ad page 28

- Extended Validation - the New Standard in SSL Security
- Sign your Code and Content for Secure Distribution Online
- Get a Free SSL Trial Certificate from Thawte