

Roundup of Identity and Access Management, 3Q09: Topics and Technologies

Ray Wagner

Gartner's comprehensive body of research on identity and access management includes a broad array of guidance on specific topics and technologies. Use the research surveyed in this updated document to make informed technology deployment and resource-allocation decisions.

ANALYSIS

Identity and access management (IAM) — the security discipline that Gartner refers to colloquially as "letting the good guys in" — is highly mature, yet extremely complex and often misunderstood. Security professionals should refer to the extensive body of research brought together in this document when making IAM technology deployment decisions or simply working to understand the trends shaping this critical area of security. IAM budgets, like every other aspect of enterprise IT spending, continue to come under intense scrutiny, and security professionals must be prepared to justify their investments in technologies and topic areas. (Note that some of the research referenced in this regularly updated document is archival and is provided for historical perspective. Portions of these documents may not reflect current conditions.) Security professionals should focus on aligning IAM initiatives, projects and technologies with the enterprise's business needs, regulatory and other compliance requirements, and other real-world factors that will help to justify IAM spending. And they should use every means possible to optimize IAM expenditures, recognizing that IAM represents not only a target for cost cutting — like every other area of IT and IT security — but also an opportunity to realize cost savings and improve performance across the enterprise.

Gartner clients need actionable, real-world guidance on specific IAM topics: technologies and tools, industry and market trends, and key drivers of technology adoption. This section offers assessments — sometimes highly granular and detailed — across many of the areas of IAM that our analysts are currently being asked about most often. Gartner's IAM research is so extensive that any "roundup" of current, applicable research would be too large to present as a single document. This research focuses on specific topics and technologies. A companion document will cover core issues and IAM governance (see "Roundup of Identity and Access Management Research, 3Q: Core IAM and IAM Governance").

IAM Topic and Technologies

Digital and Electronic Signatures

"Electronic Signature Suites and Services Mature"

By Gregg Kreizman and Kristen Noakes-Fry

Enterprises with customer-facing electronic signature requirements are increasingly interested in using suites and services rapidly, to automate signature-oriented business processes and implement required controls.

"EU Enterprises Face Obstacles in Using Electronically Signed Invoices"

By Gregg Kreizman

Digital signatures can fulfill the authentication and integrity requirements of the European Union (EU) e-invoicing directive and help provide automation efficiency gains. However, legal requirements in different countries and disparities in enterprise payment systems hinder broad adoption.

"The Long and Winding Road for PKI and Digital Signature in Spain"

By Gregg Kreizman

Several government agencies in Spain have slowly and collectively built a set of infrastructure services for authentication and digital signature that is now being leveraged by both government

and the private sector. Despite a slow start, momentum is building around a set of national services that are helping to spur adoption and interoperability. Other governments can use Spain's experiences to guide public-key infrastructure (PKI) development and to avoid projects that will likely fail to deliver promised benefits.

Secure Sockets Layer (SSL) Virtual Private Networks (VPNs)

"Magic Quadrant for SSL VPNs"

By John Girard

Remote access creates continuous market demand for new VPN products and services. Every company is working through upgrade and replacement cycles that bring opportunities to replace legacy remote-access VPNs, as well as in-between-cycle projects, such as business continuity and teleworking. IPsec VPNs are still popular for remote access, but the most interesting and visible market innovations continue to center on using SSL VPNs to replace or augment legacy VPNs. SSL VPNs are easy to set up in their default role as application portals, and they offer decent performance for tunneled Layer 3 traffic.

"Q&A: Implementation Advice for SSL VPNs"

By John Girard

SSL VPNs expand beyond the standard use of SSL for protecting login connections from browsers to websites. SSL VPNs are persistent encrypted tunnels over insecure networks, such as the Internet, using the SSL protocol, rather than the IPsec protocol, which has traditionally been used in VPNs. They offer many advantages, but must be implemented carefully, avoiding common mistakes, such as making enrollment too easy and failing to perform a predeployment risk assessment.

Consumer Authentication and Fraud Detection

"Bank Spending on Fraud and Authentication Rises, but Not Due to Red Flag Regulations"

By Avivah Litan

A Gartner survey of 50 U.S. banks shows that spending on fraud prevention and customer authentication is increasing. Top priorities include protecting money transfers and preventing online banking fraud. More than half the banks surveyed believe they are already compliant with the new "red flag" regulations.

"Banks Need to Strengthen User Authentication While Appeasing Consumers"

By Avivah Litan and Steve Cramoisan

A Gartner survey indicates that U.S. banks typically use weak consumer authentication methods — for example, passwords and "secret" questions and answers — that are increasingly threatened by malware-based attacks against customer PCs. Many of the banks surveyed, however, are planning to strengthen call-center authentication and shore up website security.

"Best Practices in New Account Fraud Detection"

By Avivah Litan

Detecting new account fraud in non-face-to-face environments requires a layered-security approach that screens out suspect account applicants and steps up reviews of transactions deemed high-risk. New U.S. "red flag" regulations will enforce more-rigorous fraud screening in

the banking industry by the end of 2009. This will drive adoption of fraud detection technologies in other sectors, particularly e-commerce.

"Consumers Don't Want to Change the Ways They Manage Online Passwords"

By Gregg Kreizman and Avivah Litan

A recent Gartner consumer Internet security and fraud survey shows that U.S. consumers would rather use insecure password management practices than convert stronger ones. Two-thirds of the respondents actually use the same one or two passwords for all the sites they access that require authentication. Enterprises should recognize this reality and use the survey findings when developing authentication strategies for their consumer-facing applications.

"Critical Capabilities for Enterprise Fraud Management Tools"

By Avivah Litan

Comprehensive fraud detection functions don't come in one package yet. Several products help enterprises manage fraud, but they must typically be supplemented by niche solutions to work. Five vendors support enterprise fraud management, and they are differentiated by their products' analytics, extensibility, business user interface, case management and data management capabilities.

"Fraud Detection and Customer Authentication Market Overview"

By Avivah Litan

Rising fraud rates and fast-moving criminals mean more-effective fraud detection and customer authentication are needed. Today's fraud detection and customer authentication market is characterized by dozens of point solutions supported mainly by niche vendors. Enterprises need a multichannel fraud management strategy — typically piecing together solutions from numerous vendors — to keep up with and stay ahead of the potential criminals.

"Magic Quadrant for Web Fraud Detection"

By Avivah Litan

Web fraud detection vendors are experiencing high sales-growth rates, driven by increasing cyberattacks in a weakened global economy. Larger security vendors are refocusing their efforts in this area, while smaller, low-cost competitors typically provide better customer service and more innovation.

"Transaction Verification Complements Fraud Detection and Stronger Authentication"

By Ant Allan and Avivah Litan

Transaction verification provides a means for enterprises to confirm the legitimacy of transactions that are identified as risky. It can significantly reduce the impact of online fraud attacks that stronger authentication does not prevent. Gartner believes that financial institutions that invest in additional controls beyond stronger authentication, such as fraud detection and transaction verification, will see fraud reductions that exceed the cost of those controls by at least 25%.

"Using SIEM for Fraud Detection"

By Mark Nicolett and Avivah Litan

Security information and event management (SIEM) technology can be applied to fraud detection, but this is an emerging use case that requires specific SIEM technology capabilities and

implementation project work. SIEM can be deployed effectively by enterprises that require such capabilities as transaction blocking or activity profiling and rescoring.

"Voice Biometrics Can Bring Banks Better User Authentication and Transaction Verification"

By Stessa Cohen and Avivah Litan

Voice biometrics shows real promise for bank user authentication and transaction verification, especially online. But this still-maturing technology should be deployed only as part of a tiered approach that recognizes different levels of risk and different types of user interaction. Banking decision makers with security and risk responsibilities should familiarize themselves with the potential benefits and limitations of this technology.

Network Access Control (NAC) and Identity Networking

"MarketScope for Network Access Control, 2008"

By Lawrence Orans, John Pescatore and Mark Nicolett

Approximately half of the vendors in the NAC market in 2008 were startup companies, and most were expected to grow. The overall market will begin to consolidate in 2009, as established network and security vendors enhance NAC functions and embed them in their products. NAC can be deployed less expensively and more widely throughout the enterprise when it is an embedded feature, rather than a separate product, but security requirements should not be compromised.

"Network Access Control in 2009 and Beyond"

By Lawrence Orans and John Pescatore

NAC is often misunderstood and represents different things to different people. Gartner clarifies NAC by outlining four key usage cases and by highlighting the criteria that are important to each one.

"Simplify the NAC Vendor Selection Process"

By Lawrence Orans and John Pescatore

Selecting an NAC solution can be confusing, because of the multiple uses for NAC and the number of vendors in the market. Defining the use case is key to selecting the best solution. The four most common uses for NAC are guest network services, endpoint baselining, identity-aware networking and monitoring/containment.

"SIEM and IAM Technology Integration"

By Mark Nicolett and Earl Perkins

Integration of IAM and SIEM technologies can improve IAM user and role management capabilities, enable SIEM exception monitoring, and provide audit capabilities that are much broader than what IAM alone can deliver.

User Provisioning and Role Management

"Automation Hype vs. Manual Reality With User Provisioning"

By Earl Perkins, Ant Allan, Ray Wagner and Perry Carpenter

Fully automated connections to user provisioning are not a reality for most enterprises. Bridged connections of mixed manual and automated process workflow can extend provisioning usability and value. To complete the connections, manual intervention is required somewhere within the workflow.

"Magic Quadrant for User Provisioning"

By Earl Perkins and Perry Carpenter

User provisioning delivers capabilities to manage users' identities across systems, applications and resources. In this market, demand is driven by compliance requirements for security effectiveness and security efficiency, but identity governance and role-based access concerns raise new issues for customers.

"Q&A: Role Life Cycle Management"

By Earl Perkins and Ant Allan

Role life cycle management is a set of processes and technologies used to develop and maintain business and technical roles. This discipline is key to most successful user provisioning and IAM governance implementations.

Web Access Management (WAM)

"Findings: The WAM Market Needs More-Realistic Pricing"

By Ray Wagner

Most WAM vendors' pricing options don't reflect the ways that enterprises use WAM products. The vendors' unrealistic approaches to pricing often limit the adoption of these valuable security technologies. For enterprises deploying extranets, concurrent-user pricing is more appropriate than the common enterprise-licensing and per-user pricing models.

"Key Issues to Consider When Deploying a Web Access Management System"

By Ray Wagner

Enterprises selecting WAM products must understand their critical functionality requirements and the key architectural issues they will face. These issues include the size and complexity of the planned deployment, the enterprise's established vendor preferences and commitments, and whether the WAM system will serve an external user group, an internal user group or both.

"Magic Quadrant for Web Access Management"

By Ray Wagner, Earl Perkins and Perry Carpenter

The WAM market has matured and is slowing, with few vendors experiencing strong customer base growth. Future vendor success in this market will require a focus on specific use cases or generalized WAM architectures for enterprise WAM needs.

"Web Access Management User Survey Insights, 2007"

By Ray Wagner and Perry Carpenter

When preparing the 2007 WAM Magic Quadrant, Gartner surveyed Web access management (WAM) users about how their enterprises deploy and manage these technologies. This research presents insights gained from that survey, among them that enterprises typically used WAM solutions for internal or external users, but rarely for both.

Enterprise Single Sign-On

"Active Directory and Unix Integration: Options for Reduced Sign-on and Administration"

By John Enck and Gregg Kreizman

Using Active Directory for Unix administration and authentication reduces user repository complexity and simplifies the user sign-on experience. However, IT managers are faced with a number of choices to implement an integration.

"Consider Present and Future Access Requirements for RSO/SSO"

By Ray Wagner, Gregg Kreizman and John Girard

The complexity of signing on to receive access to IT resources — systems and data — can be a significant problem for enterprises. Reduced sign-on (RSO)/single sign-on (SSO) solutions can help to solve this problem if they are chosen carefully and recognize present and future access needs.

"MarketScope for Enterprise Single Sign-On"

By Gregg Kreizman

This market has matured in 2009, with market leaders accelerating their growth at the expense of smaller players. ESSO remains a valid choice for enterprises with users who must manage an unacceptable number of passwords for two or more years.

"Options for Single Sign-On to SaaS Applications"

By Gregg Kreizman and Ray Wagner

Enterprises are increasingly adopting software-as-a-service (SaaS) applications. Enterprises have several options for providing SSO to SaaS applications. A combination of established SSO infrastructure, SaaS providers' SSO capabilities and the enterprise's future direction for federation informs the choices.

"SaaS IAM Gateways Begin to Take Hold, and New Solutions Join the Market"

By Gregg Kreizman

A market for IAM gateway services to SaaS applications has emerged. These services can offer an alternative to premises-based IAM solutions. But enterprises should review their specific drivers and inhibitors to adoption, as well as vendors' capabilities, to determine whether these services can provide enough value.

"Toolkit: Request for Proposal for Enterprise Single Sign-On Tools"

By Gregg Kreizman

This Toolkit includes a customizable request for proposal (RFP), a vendor questionnaire and vendor response templates to help an enterprise successfully procure an ESSO tool. It should be used when the enterprise is ready to procure an ESSO tool and has identified a shortlist of vendors to consider.

Password Management

"Blindly Increasing Password Strength Is Futile"

By Ant Allan

Most enterprises try to address authentication weaknesses by increasing password length and complexity, often in response to explicit guidance from auditors. Although such a password policy is a visible control, the security benefits are not as valuable as many enterprises expect. Even with compensating controls, too many vulnerabilities remain for passwords to be reliable across all use cases.

"Eliminate Hard-Coded Passwords"

By Ant Allan and Ray Wagner

Eliminating hard-coded passwords for software accounts significantly reduces risks, but eliminating software-account passwords altogether is difficult. Wherever migration from software-account passwords is inappropriate, enterprises must adopt a more effective and more efficient way of managing them.

"Management Update: Eight Security Practices Offer More Value Than Password Aging"

By Ray Wagner, Ant Allan and Jay Heiser

The commonplace enterprise decision to use password aging to improve security represents a bad strategy based on flawed assumptions. Automatic PC session locking and login failure lockout are two of eight Gartner-identified best practices, which vary in cost and benefits. Implemented separately or together, they ensure the higher level of user account security that password aging typically will not deliver.

"Market Overview for Password Management Tools"

By Gregg Kreizman and Perry Carpenter

Password management tools can help users get back online when locked out of their accounts and can reduce the number of passwords they have to remember. These tools can reduce call volume to the help desk, but user training and subsequent encouragement are needed to maximize use.

"Market Overview: Shared-Account/Software-Account Password Management Tools"

By Ant Allan

These tools enable enterprises to manage passwords for shared and software accounts more effectively and efficiently than manual processes. This market has shown major growth recently, attracting new vendors from the IAM space.

"The Twilight of the Passwords: A Timetable for Migrating to Stronger Authentication"

By Ant Allan

Passwords are certainly in their twilight years, but the sun will not set on all passwords in all enterprises at the same time. Enterprises should prioritize migration to stronger authentication according to risk — and where passwords must persist, complementary controls will be required.

"Toolkit: Basic Password Policy"

By Ant Allan and F. Christian Byrnes

Passwords continue to be used extensively for enterprise user authentication, even though they are not adequate to protect mission-critical assets. Security managers should use this Toolkit to establish a basic password policy to reduce the risks of password usage.

"Toolkit: Request for Proposal for Shared-Account and Software-Account Password Management"

By Ant Allan

This Toolkit includes a customizable RFP, a vendor questionnaire and vendor response templates to help an enterprise successfully procure a shared-account/software-account password management tool. It should be used when the enterprise is ready to procure a tool and has a shortlist of vendors to consider.

Authorization Management

"Best Practices for Managing Superuser Privileges"

By Ant Allan, Perry Carpenter and Jeffrey Wheatman

Accidental misuse and deliberate abuse of superuser privileges carry critical compliance and privacy risks, with potentially severe financial and reputational impacts. Best practices call for the adoption of tools that can limit misuse and active monitoring of all superuser activity.

"Superuser Privilege Management Tools for IBM i, Unix and MS Windows Server Operating Systems"

By Perry Carpenter and Ant Allan

Many tools enable enterprises to effectively manage superuser privileges for system administrators and other users across IBM i (formerly known as i5/OS), Unix operating systems and Windows. Newer tools generally have a broader focus, and many can span mixed Unix and Windows environments.

"Tear Down Application Authorization Silos With Authorization Management Solutions"

By Neil MacDonald, Ant Allan and Roberta J. Witty

Most IAM projects have focused on identity management, and application authorization management has largely been missing. Implementing application authorization management solutions can reduce redundant administration, improve policy compliance and enable agility.

Authentication

"Adaptive Access Control Emerges"

By Ant Allan and Earl Perkins

Adaptive access control is an emerging concept that builds on the concepts of risk-appropriate authentication and fine-grained, context-aware authorization to provide an extremely flexible approach to access control.

"A Taxonomy of Authentication Methods"

By Ant Allan

More and more enterprises are looking for authentication methods that are stronger than simple passwords. During the past few years, the variety of authentication methods has increased significantly, making it more difficult for enterprises to ensure like-to-like comparisons of different authentication products and services. Gartner's taxonomy of authentication methods can be used as a guide to describe with precision this broad range of authentication products.

"A Taxonomy of Authentication Methods: Quick-Reference Outline"

By Ant Allan

This outline can be used as a quick-reference guide to Gartner's authentication taxonomy (see "A Taxonomy of Authentication Methods").

"Best Practices for Automated Customer Account Reset"

By Ray Wagner and Greg Young

Enterprises are increasingly using automated customer account reset to achieve customer convenience and cost savings. But automating these functions — for which many enterprises do not even have robust manual processes in place — almost always lowers an enterprise's resistance to attack. Enterprises must follow best practices to address the reductions in security levels that accompany automation of these processes.

"Best Practices for Question-and-Answer Identity Verification Methods"

By Ant Allan

Question-and-answer methods are widely used for online authentication and identity verification in several use cases: online consumer authentication, identity verification for self-service password reset and caller verification for help desk password reset. But poorly chosen questions remain a significant weakness. When a Q&A method is used for password reset, it must be at least as strong as the passwords themselves, so as not to provide a weakness that an attacker could exploit.

"Defining Authentication Strength Is Not as Easy as 1, 2, 3"

By Ant Allan

Authentication methods are often classified by the number of factors. This approach allows broad distinctions between methods, but it is no longer granular enough to differentiate clearly among the broad variety of authentication options. For this and other reasons, it is ambiguous and cannot be used alone to quantify authentication strength.

"Formal Evaluation Methodology Will Add Value to Common Definition of 'Strong' Authentication"

By Ant Allan

The language used to describe authentication strength may be used inconsistently among regulations and in other use cases — and is frequently misunderstood. A commonly agreed-on nomenclature for authentication will have wide applicability, but a methodology for assessing the strength of an authentication method in a particular implementation will be fundamentally more useful.

"Gartner Authentication Method Evaluation Scorecards"

By Ant Allan

Choosing the right authentication method for a given use depends on matching authentication strength to the level of risk, the total cost of ownership to budgetary constraints, and the ease of use to the wants and needs of the users. Gartner Authentication Method Evaluation Scorecards provide a set of scorecards that information security architects and other security practitioners can use in the evaluation and selection of authentication methods and products.

"How to Choose New Authentication Methods"

By Ant Allan

Enterprises are seeking authentication methods that are stronger than simple passwords, but no single method is appropriate for all use cases. Every enterprise needs to identify a portfolio of authentication methods that meets its specific needs.

"Identity Proofing Is an Essential Precursor to Credentialing and Authentication"

By Ant Allan

Identity proofing is necessary to uniquely identify a person before an enterprise provisions an identity. But identity-proofing strength must be concomitant with access control needs. Just like authentication strength, identity-proofing strength can be used in an authorization decision before access to high-value assets or services is allowed. This is particularly important in federations where an enterprise relies on a third-party identity provider to authenticate users. Enterprises must know that the identity provider followed a sufficiently rigorous registration process.

"Market Overview: Authentication"

By Ant Allan

The number and variety of syndication products have increased dramatically during the past seven years. Established vendors have expanded their portfolios, and many new vendors have entered the market. Many of the newcomers — and some of the established vendors — are notable innovators.

"Using One Card for Access Control"

By Rex Murphy

The use of a single common access card for physical and logical access control offers enterprises many benefits. However, to ensure success, the enterprise must precisely define and implement a system that considers the needs of users and the functionality of the common access card.

"Ways of Integrating New Authentication Methods Within a Heterogeneous Environment"

By Ant Allan, Gregg Kreizman and John Enck

Integrating new authentication methods across a heterogeneous IT environment can raise significant problems. There are several ways to accomplish integration, but none is ideal, and most enterprises will be best served by a hybrid approach.

Identity Federation

"Case Study: Is Norway's FEIDE a Step Toward a National IAM Solution?"

By Jan-Martin Lowendahl

The Norwegian higher education identity federation solution has evolved into a government-backed IAM solution for the education community. The experiences of its developers and the lessons learned offer working solutions and insights into increased quality in, and use of, IT.

"Frequently Asked Questions About Federated Identity"

By Ray Wagner and Gregg Kreizman

Enterprises face the challenge of managing ever-larger numbers of internal and external user identities. This is causing Gartner's clients to seek guidance on basic issues concerning

federated identity, including its place in an overall IAM strategy and the drivers of and obstacles to adoption.

"Lessons Learned From Higher Education and Public-Sector Identity Federations"

By Gregg Kreizman and Jan-Martin Lowendahl

Education institutions and governments have done significant foundational work on identity federation projects. The lessons learned from that work can be used in any industry to help set realistic expectations for product outcomes, plan appropriately and reduce implementation time and expense.

"Take the Best, Leave the Rest for Identity Federation Governance and Controls"

By Gregg Kreizman and Ant Allan

The evolving Liberty Identity Assurance Framework (LIAF) provides a good, although incomplete, set of baselines for identity federation governance. Enterprise relying parties that are planning federations and using external credential and identity-proofing services can use the LIAF in mapping application assurance requirements and selecting identity providers.

"The State of User-Centric Identity, 2H08"

By Gregg Kreizman and Ray Wagner

User-centric identity frameworks, such as OpenID and information card architectures, remain immature compared with today's identity federations. Slow, steady progress is being made, but enterprises must understand the gap between current and promised capabilities to avoid too-early, too-risky investments.

"The U.S. Government Restructures Identity Federation Program"

By Gregg Kreizman

The U.S. federal government's E-Authentication program has been redesigned to reduce its operations role and focus on providing acquisition services and program governance. Other governments and enterprises considering identity federation initiatives can learn from the U.S. government's experience.

"The U.S. Government's Adoption of SAML 2.0 Shows Wide Acceptance"

By Gregg Kreizman, John Pescatore and Ray Wagner

The U.S. federal government's adoption of Security Assertion Markup Language (SAML) 2.0 sends a strong signal of mainstream acceptance of the federation standard. Vendors are building support for the standard, and the U.S. government and enterprises are moving to implement it.

Acronym Key and Glossary Terms

ESSO	enterprise single sign-on
EU	European Union
IAM	identity and access management
LIAF	Liberty Identity Assurance Framework
NAC	network access control

PKI	public-key infrastructure
RFP	request for proposal
RSO	reduced sign-on
SIEM	security information and event management
SaaS	software as a service
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
SSO	single sign-on
VPN	virtual private network
WAM	Web access management

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509