Executive Buyer’s Guide to Identity and Access Management Solutions

Managing identity across the enterprise and cloud

Issue 1

2  Foreward
3  A New Era for Identity and Access Management
5  Identity Management Solutions for Employees
5  Identity Management Solutions for Customers and Partners
6  What to Look for in an Identity and Access Management Solution
7  Success Stories
9  From the Gartner Files
   Predicts: Mobile, Social and Federation Drive Identity and Access Management
17  About Ping Identity and Glossary
Foreword

Evaluating identity and security solutions can be a daunting task. How do you know that what you need now will still be applicable in two years? One year? As new technology emerges, you have more options than ever.

We’ve been in identity for 11 years and have seen major changes in thinking around identity, access management, security and integration. We’ve witnessed the shift from users having a handful of credentials for applications managed and controlled in-house, to an explosion of cloud-based applications controlled beyond the reach of the IT team.

Your world has changed dramatically too. Remember five years ago when it was unheard of for a department to purchase software without your knowledge or input? Identity management plays a critical role in how companies acquire and use software applications now and in the future.

Change is inevitable, so the best you can do is to think about how you see your business evolving in the future. Future-proofing your enterprise against the evolving world of technology requires careful consideration.

To help you with these decisions, we gathered research by Gartner that outlines the identity trends they’re watching. Together we created a buyers’ guide to help you ask yourself some questions to evaluate your own identity needs. We’d be happy to help you identify your security requirements when you’re ready.

Bill Dedrick
President
Ping Identity
A New Era for Identity and Access Management

Identity is the new security perimeter.

Yesterday’s Security Model

For years, your IT department led your organization’s efforts to create and secure corporate data and user information within a protective firewall, keeping a tight rein on access to applications and data and enforcing strong user credentials. But over the past decade, the landscape has dramatically changed. With the rise in cloud services, mobile access, API access and social networking, users, applications and data are just as likely to reside outside the corporate network as within it. The strategy of “securing and controlling behind a firewall” is no longer enough.

According to Gartner, federation technologies, mobile computing and social identity acceptance will have major effects on the practice of identity and access management in 2013 and beyond. Make sure you are ready.

CIO Challenges

Despite changes to the enterprise, your IT department must create and support security policies to prevent unauthorized access to corporate resources while still enabling the business. Saying “no” to forces like BYOD and business-driven IT projects is counterproductive.

Challenge 1 - You must focus on the top line without adding to the bottom line.
More than ever, your company is focused on top line revenue. As budgets for new systems shrink, you are challenged with aligning your goals with the business initiatives that are focused on growth. As more of your business moves online, enabling revenue-generating initiatives that attract and retain customers can be a challenge if you don’t have the infrastructure to enable the online experience that users expect.

Challenge 2 – Secure Single Sign-On is a Must-Do.
Dealing with multiple log-ins and passwords for access to cloud and internal web applications from desktop and mobile devices is no longer acceptable for users. Neither is proprietary SSO, especially if it means that passwords are stored and shared with applications to gain access. Your department’s solutions must make it easier for employees and partners to conduct business.

Challenge 3 – Shadow IT puts your organization risk.
Business initiatives happening outside of corporate IT also presents a challenge. Employees are bringing their own apps and devices to work. Business units are building or outsourcing websites and mobile apps to stay competitive. You bear the responsibility if a security breach should happen and your organization has inconsistent or insecure IAM practices.

Challenge 4 – You have many old systems in your data center.
Your IT team understands that modifying an existing on-premises IAM system to accommodate today’s agile environment is expensive and time-consuming — starting over with a new system is not an option.
Challenge 5 – Multiple logins to your web and mobile apps affect your customers (and the bottom line).
If you’re like most enterprises, you’ve added many services and applications that customers and partners need to access. If your customers and partners are required to maintain yet another account, or log in for each service, chances are it’s impacting your user satisfaction.

Fortunately, identity and access management solutions have become more sophisticated to help you confront these challenges. Identity has become the new security perimeter.

With the increased pressure on businesses to improve the customer experience online, secure SSO to SaaS applications is a top priority for enterprises. According to Gartner:

“Federated SSO to SaaS applications for employees is now the No. 1 requirement identified by Gartner clients wanting SSO. Clients want to leverage internal authentication infrastructures to give their users SSO to SaaS applications. There has also been a smaller, but significant, increase in client needs to support consumer authentication using social media identities. This is another use case for federated SSO or reduced sign-on (users must overtly authenticate, but they can reuse an existing ID and password).”


Source: Ping Identity
Identity Management Solutions for Employees

Enable secure access to apps for your employees

With the surge in cloud-based business applications, your employees are forced to manage more usernames and passwords than ever. Recycling weak passwords leaves your enterprise vulnerable to data breaches. Furthermore, employee productivity suffers as employees are forced to contact the helpdesk for resets in order to access their work applications. An effective identity management solution for your workforce will eliminate multiple passwords to improve productivity and reduce risk.

Identity Management Solutions for Customers and Partners

Enable customer access to apps

Customers and external users are also feeling the pain of navigating through multiple login screens. The rise in popularity of APIs, mobile applications and social media engagement is driving more revenue opportunity for companies who make it easy for customers to get access to their products and services. In order to compete, it’s critical for your identity management system to enable and encourage access to your apps and data through secure SSO.
What to Look for in an Identity Management Solution

Evaluate your needs
IAM vendors offer a wide variety of services and solutions to enable user access. In choosing a solution, you should consider features and capabilities, as well as how the solution will integrate with the systems you already have in place. Before making any decision, consider the following factors:

1. **Where do your identities live today?**
   Most enterprises need to accommodate identities that live internally in an on-premises repository or directory, as well as accept partner, client or consumer credentials based on identities that reside elsewhere. You need an identity management solution that will leverage your existing infrastructure—and extend it to handle a broad range of credentials from customers, partners and social media sites.

2. **Where do your applications live today?**
   **Who needs access?**
   Like identities, the applications that your users access likely reside on-premises as well as in the cloud. Internal, partner, software-as-a-service (SaaS), private- or public-cloud applications all need to be seamlessly accessible to your users without requiring them to jump through unnecessary hoops.

3. **Do your users access applications on mobile devices? Do you have remote users?**
   Chances are your users require access to your applications from local and remote locations and using any number of devices. Look for a solution that gives your users the same secure access regardless of location or device. Be sure to customize your security policies wherever and whenever you deem appropriate.

4. **Will your new solution integrate with your existing identity management infrastructure? What happens if (or when) you to move to the cloud?**
   If you’ve invested with a stack vendor or are using a combination of identity and access management solutions today, the ideal identity management solution should leverage that architecture investment to make it easier for IT to scale its resources. Look for a solution that allows your IT team to take advantage of existing identity security products and practices to extend functionality without requiring extensive re-investment.

5. **What about deployment? On-premises, cloud-based or both?**
   Some identity management systems are “all or nothing”—all cloud or all on-premises. They aren’t flexible enough to manage identities across both cloud and on-premises applications. But what if you just want to push a few of your customer-facing apps to the cloud and keep the rest on-premises? When searching for a new system, you should consider this and determine whether you’ll need the flexibility now or in the future.

According to a recent report from Gartner Research:

“All enterprises offering consumer-facing services, as well as government agencies offering citizen portals, should assess the benefits of accepting social network identities for customer/citizen registration and login, and weigh these against the risks posed by the lack of identity proofing and weak authentication for social network identities. Potential cost savings may be offset by the cost of mitigating these risks. This assessment should also consider alignment with other business use of social networks; while it can be independent of other initiatives, greater value can come from exploiting synergies. Enterprises deciding to pursue this approach should evaluate specialist vendors that directly support it, or press their IAM vendors for protocol support to enable in-house development to support this approach.”


Source: Ping Identity
Success Stories

We invite you to explore our customer use cases.

TRUIST

Use case: Cloud SSO

Challenge: After providing secure SSO to its clients for years through an on-premises solution, Truist wanted to transition to a cloud-based SSO solution to improve redundancy, availability and security for its clients and gain operational benefits for its IT department.

Solution: PingOne®

Results:

• Doubled clients using Ping Identity
• Supports 4,000 logins every day
• Reduced time and resource requirements to onboard clients

"PingOne not only lets us offer secure, highly available SSO to our clients, it also lets us onboard a new client in about 5 minutes. My job just got easier." Katie Boswell, Director of IT Infrastructure, Truist

Read the Truist story.

LAND O’LAKES, INC.

Use case: Workforce SSO

Challenge: As Land O’Lakes adopted more and more SaaS applications, employees began complaining about the rising number of login passwords. Help desk costs rose and adoptions dropped. The company’s IT team set out to increase user happiness (and acceptance of new applications) by adding seamless access. They also needed a solution that could establish SSO connections quickly.

Solution: PingFederate®

Results:

• 6500 users empowered with secure SSO to the applications needed to do their jobs
• Dramatic cuts in Help Desk password reset calls and routine IT administration
• Increased user adoption of their licensed SaaS applications
• Mobile workforce was enabled with real-time access to Sales ordering system

Read the Land O’Lakes story.
Opower

**Use case:** Customer SSO

**Challenge:** With 75 utility clients globally, Opower’s online information helps users understand their energy usage, lower bills and increase efficiency. Opower needed to provide simple and secure access to their application for existing user accounts while preserving their utility partners’ online brands. But with millions of customers already using utility websites, a streamlined user experience was critical to maintaining convenience and increasing adoption.

**Solution:** PingFederate®

**Results:**
- Seamless portal-to-portal customer experience
- Immediate customer authentication using existing identities
- Rapid implementation and smooth partner integration

“We went with PingFederate because it is based on standards like SAML, which are important for a secure implementation,” said John Davidson, Senior Product Manager, Opower. “We’re a company of developers. We knew that with Ping Identity, we wouldn’t have to worry about scalability as our client base grew.”

**Read the Opower story.**

According to Gartner, Federated SSO will be the predominant new SSO technology needed by 80% of enterprises through 2016.

“The identity standard landscape continues to evolve and at an accelerated pace. Choose a vendor that is committed to supporting identity standards to provide more ways to differentiate their user experience, lower operating costs, and improve security — now and in the future.”


Source: Ping Identity
Federation technologies, mobile computing and social identity acceptance will have major effects on the practice of identity and access management in 2013 and beyond.

**Key Findings**

- The rise of mobile computing creates a user authentication challenge, to the device itself, and to networks and downstream applications.

- Allowing enterprise customers and other users to, where possible, use a social identity for authentication lowers friction, and thus improves the user experience. Enterprises also benefit through a fall in the number of abandoned registrations and logins.

- Using techniques based on consumer Web fraud detection for enterprise authentication can provide a higher level of assurance without requiring users to use a traditional (and expensive) higher-assurance authentication method.

- The ubiquity and diversity of mobile devices, form factors, and OSs is creating problems for identity and access management (IAM) planners seeking consistent and secure approaches for authenticating both employees and customers.

- Federated SSO to software as a service (SaaS) applications for employees is now the No. 1 requirement identified by enterprises wanting SSO.

**Recommendations**

- Determine if the combination of power-on password and X.509 device authentication is reasonable and appropriate across all enterprise mobile remote access use cases.

- Retail customer services enterprises should weigh the benefits of accepting social identities for customer registration and login against the risks posed by their lack of identity proofing and weak authentication.

- Enterprises should identify the use cases where contextual authentication is a reasonable and appropriate choice for workforce remote access and make revisions to user authentication strategies and architectures.

- Enterprises should implement standards-based identity federation to mediate disparate access management systems, SaaS applications and mobile clients.

**STRATEGIC PLANNING ASSUMPTION(S)**

**Through 2015,** 50% of enterprises allowing BYOD for external employee access will use only power-on passwords with X.509 device credentials for authentication.

By year-end 2015, 50% of new retail customer identities will be based on social network identities, up from less than 5% today.

By year-end 2016, over 30% of enterprises will use contextual authentication for workforce remote access, up from less than 2% today.

Through 2014, 85% of enterprises allowing employees to use their own mobile devices to access enterprise and SaaS applications will not achieve SSO.

Federated SSO will be the predominant new SSO technology needed by 80% of enterprises through 2016.

**ANALYSIS**

Gartner’s security analysts have developed a set of key identity and access management (IAM) predictions for 2013 and beyond. Chief information security officers (CISOs), network managers and other enterprise decision makers should consider these forward-looking Strategic Planning Assumptions when allocating resources and selecting products and services.

**What You Need to Know**

Every year, Gartner analysts offer their predictions on what they see as the key issues facing the
market spaces they cover. Gartner’s security analysts have once again developed a set of Strategic Planning Assumptions for IAM — the security discipline concerned with enabling the right individuals to access the right enterprise resources for the right reasons.

IAM continues to mature as a strategic discipline and as a set of technologies. However, the maturation process has been complex, difficult and expensive for many enterprises. Major changes to the IAM markets and environment during the next few years will come mainly from adoption of cloud services and mobile devices, as well as the increasing use of social identity by enterprise participants. IAM decision makers should consider Gartner’s predictions for 2013 and beyond when making strategic investment and implementation decisions.

**Strategic Planning Assumptions**

**Strategic Planning Assumption:** Through 2015, 50% of enterprises allowing BYOD for external employee access will use only power-on passwords with X.509 device credentials for authentication.

**Analysis by:** Ant Allan, Gregg Kreizman

**Key Findings:**

- The rise of mobile computing creates multiple challenges for enterprises, especially where BYOD policies are in effect, which obliges the enterprise to support a wide range of hardware and mobile OSs. Apple iOS, Google Android and RIM BlackBerry are dominating, and Microsoft Windows 8 is in the offing, and various mobile OS versions (some vendors are still shipping hardware with Android 2) exist. One particular challenge lies in user authentication, to the device itself — weak, short numeric passwords are the default — and to networks and downstream applications. Stronger power-on passwords can be enforced by mobile device management (MDM) tools, which Gartner recommends should be used to manage all mobile devices, including BYODs, connecting to enterprise networks.

- Enterprises face multiple challenges when trying to implement higher-assurance authentication methods. Those that are commonly used for workforce remote and local access — typically one-time password (OTP) hardware tokens or phones-as-a-

token authentication methods (OTP apps for smartphones or out of band [OOB] authentication) in the first case; X.509 smart tokens in the latter — don’t migrate well for many reasons:

  - Poor user experience (UX) in most cases (and users’ UX expectations are higher on mobile devices)
  - Depreciated assurance in the case of phone-as-a-token methods
  - Difficulty in, and cost of, technical integration of X.509 smart tokens

  - Pragmatism is driving enterprises to implement methods that may not be classically “strong,” but which are technically feasible, lower cost and provide better UX. Most MDM tools can provision and validate X.509 credentials to the devices, and since there are multiple reasons to use MDM tools anyway, exploiting them to provide device authentication is a facile decision (in both senses of the word). In the absence of widely available and proven “mobile apt” authentication methods, this approach will likely dominate for the next two to three years.

**Market Implications:**

- The combination of power-on password and X.509 device authentication doesn’t provide the 2FA that is seen as the norm for remote access and that is demanded by many regulations (such as PCI Data Security Standard [DSS]) and auditors: (1) the X.509 credentials are associated with the device, not the user (although concatenation is possible by explicitly associating the user with the device); (2) the power-on password and X.509 device authentication are evaluated at different times (leaving the enterprise open to an opportunistic attack where someone gains possession of an employee’s device after power-on login). Thus, enterprises may be exposed to greater risk than they are from PC-based remote access with conventional 2FA in place.

- One way of mitigating this risk may be to use network segmentation, enforced by MDM or network access control tools, to restrict access to sensitive, critical and high-value assets from mobile endpoints. However, such restrictions may not always be acceptable for operational or business reasons. Nevertheless,
this approach may be an efficient compromise until mobile-apt authentication methods (likely some combination of “passive” biometric authentication and contextual authentication methods become established in the midterm). This avoids costly and unwieldy attempts to “make” existing authentication methods work in the mobile context.

- This deferment will also allow time for the market to establish workable patterns, if not best practices, for integrating user authentication and SSO technologies with mobile applications, especially resident mobile apps (RMAs), in contrast to mobile Web apps (although adoption of HTML5 might, by then, allow troublesome RMAs to be avoided).

**Recommendations:**

- Enterprises must determine if the combination of power-on password and X.509 device authentication is reasonable and appropriate across its mobile remote access use cases. For higher-risk use cases, enterprises must determine if it is feasible and acceptable to end users to block access from mobile devices or if implementing other controls (such as granular activity monitoring) will sufficiently mitigate the risks; otherwise they must “bite the bullet” and demand the use of more traditional higher-assurance authentication methods. This could be what they’re already using for PC-based remote access or something different. Bold enterprises might implement emerging, candidate mobile-apt authentication methods in the short term, but which of these are truly viable will likely not be clear for two to three years.

**Related Research:**

“Supporting Mobile Device Authentication and Single Sign-On to the Enterprise and Cloud”

“Market Trends: The Impact of Mobile Computing on User Authentication”

“Good Authentication Choices: Evaluating Phone-as-a-Token Authentication Methods”

**Strategic Planning Assumption:** By year-end 2015, 50% of new retail customer identities will be based on social network identities, up from less than 5% today.

**Analysis by:** Ant Allan

**Key Findings:**

- For increasingly many Internet users, social networks are the Internet. Using “login with Facebook” (or other popular social networks) lowers friction, and thus improves the UX for customer registration and subsequent login:
  - For registration, required personal information can be imported from the users’ social profiles, reducing — if not eliminating — form filling
  - For login, using the social network identity means that users don’t have to remember yet another rarely used password and don’t have to go through convoluted password reset processes if they forget them.

- Enterprises also benefit through a fall in the number of abandoned registrations (because new customers balk at form filling) and logins (because returning customers have forgotten their passwords). Login with preferred social network identities makes it easier for customers to browse and buy — especially where “merchant is present” on other social networks (such as Facebook and Pinterest). Thus, using social network identities significantly helps enterprises to attract and retain customers.

- The use of social network identities can lower customer administration costs — this can be a business enabler, making profitable services that wouldn’t be if they had significant overheads. Gartner sees a small but growing number of enterprises taking this approach, enabled by specialist vendors (such as Gigya and Janrain) that prepackage support for a broad range of popular social networks and integrate other social network capabilities (such as gamification). Basic user attribute collection (for registration) and authentication with social identities are also being supported by Web access management products.
Market Implications:

• Lack of identity proofing and weak authentication for social network identities expose merchants to more fraud. Service providers still have to defend themselves. So, they may accept/allow for social network registration, or login, but augment the process with additional controls when the retail customer site provides access to sensitive data and monetary transactions.

• Nevertheless, merchants may accept risk without additional controls because of the potential increase in the number of customers and volume of purchases. This “passes the buck” to payment card companies, which will be exposed to more fraud, but these already have robust fraud detection and management tools and processes in place.

• However, it is important to remember that social network identity proofing and user authentication are no worse than the practices followed by many enterprises; higher identity assurance may be needed anyway. In fact, social network identities might offer better identity proofing than “raw” customer registration, because social network analysis can potentially identify bogus social identities and some vendors (for example, Trulioo) can exploit the “wisdom of crowds” to verify a claimed social network identity. There will be increased demand for specialized vendors that support this use of social network identities, as well as for support for the OAuth and OpenID Connect specifications in traditional IAM vendors’ Web access management and federation products.

• Customers without a social network identity may feel marginalized and disenfranchised, and may switch to less heavily “socialized” merchants. Enterprises must ensure that “nonsocial” customers are well looked after. Enterprises will also need to find a way of managing “social” and “nonsocial” identities; some of the specialist vendors already provide this capability. A niche, but important, requirement comes from potential customers (such as dissidents and refugees) who need to compartmentalize their identities.

Recommendations:

• All enterprises offering consumer-facing services, as well as government agencies offering citizen portals, should assess the benefits of accepting social network identities for customer/citizen registration and login, and weigh these against the risks posed by the lack of identity proofing and weak authentication for social network identities. Potential cost savings may be offset by the cost of mitigating these risks.

• This assessment should also consider alignment with other business use of social networks; while it can be independent of other initiatives, greater value can come from exploiting synergies. Enterprises deciding to pursue this approach should evaluate specialist vendors that directly support it, or press their IAM vendors for protocol support to enable in-house development to support this approach.

• They should also evaluate layered controls, such as fraud detection and prevention mechanisms, as well as low-friction, medium-to-high-assurance user authentication methods (such as phone-as-a-token, “passive” biometric and contextual authentication), to mitigate risks where customers will have access to personal or other sensitive information.

Related Research:

“Technology Overview for Federated Identity Management”

“Choosing Among Federated Identity Management Options”

“2012 Strategic Road Map for Business Gets Social”

Strategic Planning Assumption: By year-end 2016, over 30% of enterprises will use contextual authentication for workforce remote access, up from less than 2% today.

Analysis by: Ant Allan
Key Findings:

• Web fraud detection (WFD) tools, widely deployed in retail banking in the U.S. and elsewhere, established the idea of using contextual information (such as endpoint identity and geolocation, typically inferred from the IP address) as a way of corroborating a user’s claimed identity.

• These WFD tools have been adopted by a relatively small number of enterprises in other use cases, including remote access by workforce and external users. Some vendors (notably RSA, The Security Division of EMC) now offer versions of these tools tailored for enterprise remote access use cases; and some vendors (including well-established players such as RSA and Symantec, as well as smaller new entrants, such as SafeLayer) have embedded this mechanism into “pure” user authentication products. RSA already offers this mechanism within RSA Authentication Manager Express, and will add it to its flagship product, RSA Authentication Manager, in 2013, which will give a huge boost to market adoption.

• A key benefit of this approach is that it provides a higher level of assurance than a password alone, without requiring users to use a traditional higher-assurance (“two-factor”) authentication method. In some use cases with low to medium risk, and for workforces with highly consistent work patterns, this may be sufficient. However, in many use cases, unless the enterprise is willing to block access, it will still be necessary to invoke a higher-assurance method when the contextual information varies outside of norms (unknown endpoint, unusual location or one unreasonably distant from last known location, and so on) or when the user is attempting to access higher-value assets. Nevertheless, the burden of authentication on users is reduced (along with support overheads).

Market Implications:

• Adoption of contextual authentication will provide further impetus for the migration from legacy OTP hardware tokens (such as RSA SecurID, SafeNet SafeWord and Vasco Digipass) toward “tokenless” solutions. If users will be using this more rarely, it is harder to justify investing in relatively costly tokens with high logistical overheads.

• Thus, we expect to see further interest in and adoption of phone-as-a-token authentication methods (OTP apps for smartphones, especially where these are provided at zero cost; out-of-band authentication by SMS, voice telephony and push notification; and so on), as well as biometric authentication technologies that can exploit available inputs from the endpoint device (such as voice recognition via microphones, face topography via user-facing cameras, keyboard and touchscreen interactivity), which are very suitable for mobile computing use cases. Gartner projects that major user authentication vendors will make significant strides in the breadth and depth of these “contextual authentication” frameworks during the next four years.

• The range of contextual information sources used is rapidly expanding (with mobile computing providing a rich seam), and leading business intelligence (BI) vendors are exploring how they can leverage their analytics to “feed” contextual authentication frameworks. In this framework, an authenticated social network identity may be consumed as further corroboration of identity. Multiple authenticated social network identities provide higher confidence — but the authentication engine needs to avoid double counting (that is, using the same social network identity for initial login and corroboration). Relevant identity data from a broader range of social profiles can also be folded into the mix. Use of smartphones, either as endpoints or as active components of user authentication, will potentially make available a further set of identity-relevant information.

• With increasing numbers of independent sources of contextual information, the confidence this provides increases exponentially because of consilience effects — for example, consistency between IP-based geolocation, GPS and cell tower information. This shift in emphasis will create opportunities for new vendors, and existing user authentication vendors that don’t support contextual authentication will increasingly find themselves at a disadvantage in the market.

Recommendations:

• Identify the use cases where contextual authentication is a reasonable and appropriate choice for workforce remote access (and other use cases). Revise your user authentication strategy and architecture accordingly.
• If appropriate, ask your authentication vendor if it already supports contextual authentication or, if not, where it fits in its product road map. In either case, evaluate alternative vendors. If this is not a good fit in the short term, plan to monitor the maturity and adoption of contextual authentication during the next two to three years.

Related Research:

“Defining Authentication Strength Is Not as Easy as 1, 2, 3; Update”

“Maverick* Research: The Death of Authentication”

“Good Authentication Choices: Evaluating Phone-as-a-Token Authentication Methods”

Strategic Planning Assumption: Through 2014, 85% of enterprises allowing employees to use their own mobile devices to access enterprise and SaaS applications will not achieve SSO.

Analysis by: Gregg Kreizman

Key Findings:

• The ubiquity and diversity of mobile devices, form factors, and operating systems, as well as the variety of use cases, have presented many challenges to enterprises that must support these devices for application development, data management and access. The same circumstances are creating problems for IAM planners who seek consistent and secure approaches for authenticating employees and customers, and for providing SSO from mobile devices to applications within the corporate data centers or in the cloud.

• Enterprise strategies must account for mobile Web applications (that use the browser as the user interface) and resident mobile applications that are being developed by enterprises and SaaS vendors. Enterprises have little or no control over the application architectures for third-party-developed applications. Differences in mobile OS architectures, their authentication method handling, and the lack of mature standards combine to make true SSO a near impossibility for enterprises that support BYOD policies that allow for a broad range of devices to be used.

Market Implications:

• Currently implemented Web access management tools can be used for mobile Web applications, but they do not readily support mobile resident applications.

• Many enterprises are coping by using a combination of power-on passwords and X.509 device authentication as “good enough” authentication to applications. Gartner has spoken with some clients that have implemented proprietary authentication layers for their own mobile resident applications using passwords and authentication tokens held in databases to manage session state. This approach does not readily support third-party mobile resident applications, such as those provided by SaaS vendors for access to their application services.

• Access management vendor solutions generally require a proprietary device resident software development kit (SDK), which is designed to communicate with the vendor’s back-end access servers. This approach is consistent with other types of market disruptions, and proprietary solutions are the first to fill gaps. New identity specifications, such as OAuth and OpenID Connect are emerging, but do not completely address needs. Proprietary and custom solutions will be needed for the next two to three years.

Recommendations:

• When possible, use mobile Web applications — rather than RMAs — so that established access management systems can be used.

• Use standards-based authentication and federation protocol libraries of established commercial application development environments, where these libraries are available.

• Implement standards-based identity federation to mediate protocols and token formats among enterprise access management systems, SaaS applications and mobile clients.

• Get access management and mobile device or mobile OS vendors’ road maps for supporting OAuth and OpenID Connect.
Related Research:

“Supporting Mobile Device Authentication and Single Sign-On to the Enterprise and Cloud”

“Good Authentication Choices: Evaluating Phone-as-a-Token Authentication Methods”

“Technology Overview for Federated Identity Management”

Strategic Planning Assumption: Federated SSO will be the predominant new SSO technology needed by 80% of enterprises through 2016.

Analysis by: Gregg Kreizman

Key Findings:

• Federated SSO to SaaS applications for employees is now the No. 1 requirement identified by Gartner clients wanting SSO. Clients want to leverage internal authentication infrastructures to give their users SSO to SaaS applications. There has also been a smaller, but significant, increase in client needs to support consumer authentication using social media identities. This is another use case for federated SSO or reduced sign-on (users must overtly authenticate, but they can reuse an existing ID and password).

• Web-architected applications have gradually and inexorably expanded their presence, within the enterprise, due to a strong SaaS adoption trend. Organizations have transitioned out legacy architected applications, or believe that these applications will be retired soon enough to leave these applications out of scope for an SSO initiative. Enterprises have also reduced the password burden for some legacy applications through methods such as Active Directory integration, Lightweight Directory Access Protocol (LDAP)-based directory integration or password synchronization.

Market Implications:

• Prior to 2012, Web access management (WAM) tools had been adopted by most organizations that needed them. These tools use a proxy or agent architecture to support authentication, SSO and coarse-grained authorization to Web-architected applications that run on a variety of Web application servers. This was a slow, decelerating growth market to 2011, but organizations increased their need for mobile device support, and SaaS applications have pushed WAM vendors to develop more-attractive features to meet these needs. The requirements to support federation, particularly for SaaS applications, have also kept the WAM market active. Most WAM tools now support federation inherently.

• However, federation capabilities have also been delivered through open source, Microsoft Active Directory Federation Services (ADFS), stand-alone federation products, extension of established authentication products, and identity and access as a service (IDaaS). Thus, federated SSO is taking its first steps toward commoditization.

Recommendations:

• Enterprises with no access management tools, but that want to leverage Active Directory authentication for federation based on SAML 2.0 or WS-Federation, should strongly consider Microsoft ADFS 2.0.

• Enterprises that have deployed WAM tools should consider using the federation capabilities that are included or sold as add-on products for possible cost-benefits over other options.

• Consider open-source federation capabilities, but recognize that there is no “free lunch”; support contracts will likely be needed.

• IDaaS should be considered when the enterprise does not want to manage an on-premises IAM infrastructure or many federation partnerships themselves.

Related Research:

“Choosing the Best Approach for Single Sign-On”

“Choosing Among Federated Identity Management Options”

“Technology Overview for Federated Identity Management”
A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

On Target: 2010 Prediction — Through 2013, the focus of IAM will shift from operational improvements to critical intelligence for business process improvement.

Core IAM functions, such as access management and identity administration, are becoming mainstream as IAM products and solutions are integrated into more-mature IT organizations and structured processes. Business use of such core functions is increasing, and enterprise awareness of the value of IAM is rising. As the foundations for IAM are established in more enterprises, new demands by the business have shifted the focus away from incremental operational improvements to a broader discussion of the governance and analytics of identity. The Nexus of Forces (cloud, mobile, social and information) impacts are contributing to this shift, particularly the requirement for better intelligence from an IAM system to address specific business decisions.

Enterprises are increasingly adopting identity and access governance (IAG) tools that provide the foundations of an identity data and log model, analytics tools, and improved reporting functionality to deliver intelligence used in business processes. IAG tool purchases are growing at twice the rate of core IAM tools, and analytics is becoming a key skill requirement for mature IAM organizations. The intelligence derived from identity analytics is being used to improve business processes in HR, internal auditing, and risk management. The improved quality of identity data information is contributing to more effective regulatory compliance processes as well.

Missed: 2010 Prediction — By the end of 2012, 60% of small and midsize businesses (SMBs) and 20% of enterprises will use VPN vendors’ natively supported authentication methods.

SMBs and enterprises did not turn to these solutions as Gartner anticipated. We see two reasons for this:

- Although more VPN vendors like Check Point — as well as UTM vendors like Fortinet — offer natively supported authentication methods, very few call out this feature clearly enough to find it on their websites or in their marketing materials: Gartner clients are largely still completely unaware that these methods are included in the offering.

- These vendors rarely, if ever, have the end-to-end quality of service for OOB authentication that dedicated vendors, such as PhoneFactor (recently acquired by Microsoft), can offer. Traditional vendors and service providers (often now the same entities) continue to perform well, with significant growth among the smaller vendors and adoption in the midmarket.

Gartner RAS Core Research Note G00230389, R. Wagner, A. Allan, G. Kreizman, E. Perkins, 30 November 2012
About Ping Identity

We can help your business.

Ping Identity believes secure professional and personal identities underlie human progress in a connected world. Our identity and access management platform gives enterprise customers and employees one-click access to any application from any device. Over 1,000 companies, including half of the Fortune 100, rely on our award-winning products to make the digital world a better experience for hundreds of millions of people. For more information, dial U.S. toll-free 877.898.2905 or +1.303.468.2882, email sales@pingidentity.com or visit pingidentity.com.

Ping Identity Headquarters
1001 17th Street
Suite 100
Denver, CO 80202

Direct: 303.468.2900
Fax: 303.468.2909

Web: www.pingidentity.com
Email: sales@pingidentity.com
Facebook: www.facebook.com/pingidentitypage
Twitter: @PingIdentity

ACRONYM KEY AND GLOSSARY TERMS

Authentication – Process for determining and validating user identity for both on-premise and cloud solutions.

Authorization – Process for determining what the user can do. Authorization can be based only on user identity but in most cases requires additional attributes (such as role or title) about the user.

Cloud identity management system – On-premises or cloud-based hardware or software that administers user identities and access to on-premises or cloud-based information and computing resources. Capabilities might include identity synchronization, provisioning, de-provisioning and the ongoing management of user attributes, credentials and entitlements.

Cloud identity – Established identity from sites such as Facebook, Google, LinkedIn, Salesforce.com or Twitter that can be used for website registration and login purposes.

Distributed computing environment – Environment in which user accounts, identity management services or applications are dispersed across on-premises and cloud-based environments.

Federated identity – A standardized way for companies to share user and machine identities among disparate authentication and authorization systems and across corporate boundaries.

Identity management – Management of individual identities, authentication, authorization, roles and privileges within or across system and enterprise boundaries.

Identity management as a Service (IdaaS) Software-as-a-service (SaaS) – Offering that provides identity management capabilities (e.g., access, provisioning) for a variety of user cases (e.g., employees, partners, customers) and types of applications (e.g., on-premises, cloud).

Open standards – Non-proprietary formats or specifications approved by a recognized standards organization or accepted as the de facto guidelines by the industry. Key identity and access management standards to look for include:

- LDAP: Lightweight directory access protocol
- OAuth: Open authentication
- REST: Representational state transfer
- SAML: Security assertion markup language
- SCIM: Simple Cloud Identity Management / System for Cross-domain Identity Management

© 2013 Ping Identity Corporation. All rights reserved. Ping Identity, PingFederate, PingOne, PingEnable, the Ping Identity logo, and Cloud Identity Summit are registered trademarks, trademarks or service marks of Ping Identity Corporation. All other product and service names mentioned are the trademarks of their respective companies.