White Paper

Cloud Identity Buyer's Guide

Managing identity in the cloud

Table of Contents

The Software-as-a-Service (SaaS)[1] application delivery model is growing rapidly. SaaS is taking over the world. That's the good news. However, customers who adopt the SaaS model struggle to manage the overwhelming number of user accounts they have to create. Their users are constantly forgetting their passwords and calling the help desk. They are unhappy because they have to reenter their user ID and password every time they logon to an application during the day. Overwhelmed IT administrators take too long to create accounts for new users. When a user leaves the organization, their SaaS accounts remain active, increasing the risk of data exposure.

All this consumes resources, increases enterprise risk, and costs your organization time, money, and effort. You need help to reduce the complexity of managing the hundreds or thousands of SaaS accounts your users require—not just employees, but others too, like contractors, partners, distributors, and customers.

This Buyer's Guide discusses the issue of identity and access management (IAM) for cloud applications. It outlines the issues that need to be addressed, suggests some approaches to solving those issues, and provides an overview of the McAfee products that are designed to help companies manage their SaaS account identities more effectively and efficiently.

"…the need for trusted identities and secure and efficient management of these identities while users' privacy is protected is a key element for the successful adoption of any cloud solution."

National Institute of Standards and Technology

Problem Statement

Enterprises of all sizes are embracing cloud computing because of the many advantages it provides. These include lower costs, greater business agility, reduced IT administrative overhead, access to best-of-breed applications, and more. Industry analyst firm IDC reports the SaaS market reached $16.6 billion in revenue in 2010, and is projected to grow at more than 25% per year between now and 2015.[2]

The cloud contains solutions that address virtually any conceivable business need: Sales, marketing, human resources, collaboration and communication, finance, legal, etc. However, this proliferating profusion of solutions has created a daunting operational challenge: How to efficiently manage the profusion of identities that users require—one for each cloud application they access. If you have 1,000 employees, each accessing 10 cloud applications on average, that's 10,000 unique identities to manage.

In the "*Cloud Computing Technology Roadmap*," the National Institute of Standards and Technology (NIST) advises that "…the need for trusted identities and secure and efficient management of these identities while users' privacy is protected is a key element for the successful adoption of any cloud solution."[3] The best way to address these concerns is to deploy strong identity management processes and technologies to ensure that only authorized users have access to cloud applications.

In this Cloud Identity Buyer's Guide, McAfee discusses how your organization can design, deploy, and manage an effective, efficient IAM solution for SaaS applications in two different scenarios:

- *To the cloud*—IAM for SaaS applications from an on-premise platform
- *In the cloud* —IAM for SaaS applications from an on-demand platform

We discuss some of the technologies available to:

- Manage the end-user identity lifecycle—from creation to termination
- Provide users with greater convenience by eliminating the need for them to remember passwords for multiple systems
- Protect sensitive systems with strong multi-factor authentication

- Empower IT administrators to easily monitor and manage all SaaS access activities and ensure compliance with relevant regulations

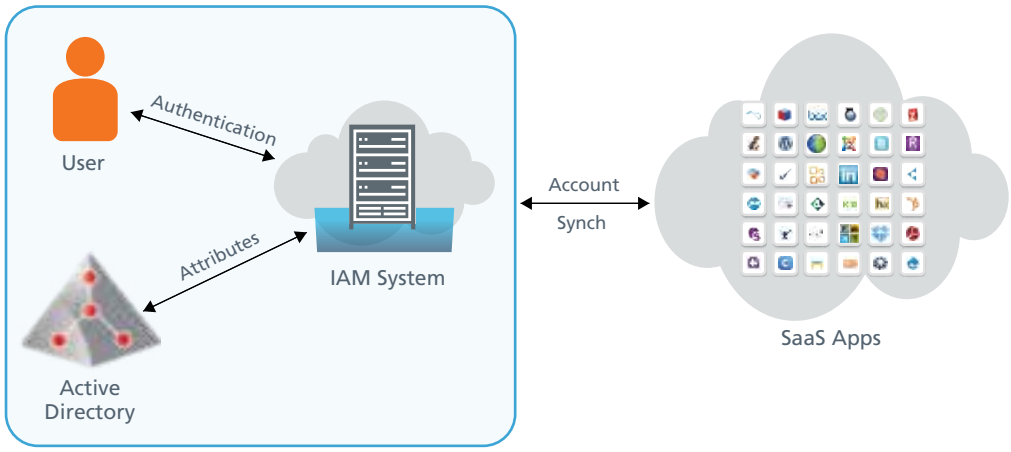

Figure 1. Identity to the cloud.

We evaluate various identity management standards, such as Service Provisioning Markup Language (SPML), Security Assertion Markup Language (SAML), OpenID, and OAuth which help ensure that ability to access enterprise SaaS solutions will keep pace as the industry matures.

By making these fundamental capabilities an essential part of your overall cloud initiative, you will be able to enjoy the many benefits of the cloud, while simultaneously protecting your vital corporate assets from unauthorized access, improving your user's cloud experience, and controlling costs.

Automating IAM for SaaS

As you expand your utilization of SaaS and accumulate more and more applications with varying underlying security and architecture models, you may quickly find yourself dealing with a wide variety of user interfaces, application programming interfaces (APIs), security policies, and management tools.

Automating IAM for SaaS applications can simplify these problems in a number of ways.

Internet Single Sign-On (SSO)

As more SaaS applications become part of the enterprise portfolio, users desire the convenience of a single entry point into all their applications.

Users are notorious for unsafe password practices:

- They may use the same password for more than one application, increasing the risk to multiple applications if one of them is compromised
- If they have to remember a large number of user ID/password combinations, they may write them down and post them in a convenient, yet insecure, location, such as under their keyboard
- They may choose passwords that are easy to remember and, therefore, easy to break

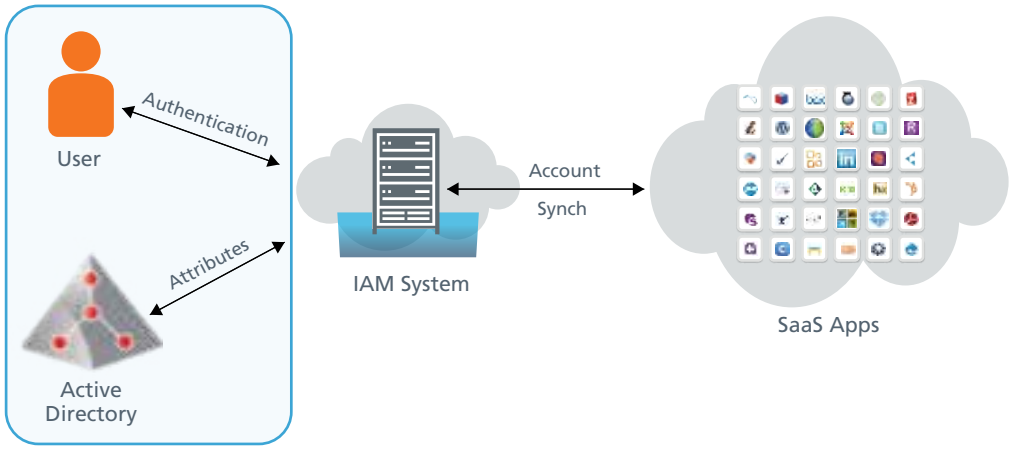

Figure 2. Identity in the cloud.

Implementing single sign-on for SaaS apps relieves end users of the responsibility of managing their passwords while providing a high level of assurance that they have been properly authenticated. SSO reduces time wasted logging on and logging off work systems. It virtually eliminates password reset calls to your IT administrator or help desk, freeing up those resources to focus on more value-added work. And, it eliminates many of the potential security risks associated with weak passwords.

Strong authentication

One of the leading reasons for not outsourcing IAM to the cloud is concern for the security of user credentials. In cases where the risk associated with access is high, even the strongest password management practices may be regarded as insufficient to adequately protect user credentials in the cloud.

What organizations are looking for is the ability to invoke strong, multi-factor authentication (MFA) in situations where it is essential to validate a user's identity with more than a user ID and password. Candidates for strong authentication include users who are accessing a particularly sensitive app, who are located outside the firewall, who are contractors or other temporary hires, or who belong to a particular group.

Implementing SSO gives you the ability to provide users with access to hundreds of external sites using a single set of credentials, through a single portal. If those credentials are compromised, then all the target sites are at risk. In this use case, where simply entering a user ID/password may not be sufficient protection, MFA provides an excellent strategy to protect multiple apps by controlling access to the SSO portal. It enables your organization to secure the cloud-based portal, bringing it up to enterprise security standards.

This need has led to the emergence of various strong authentication technologies, as listed in Table 1.

Table 1. Multi-factor authentication models.

Approach	Description
Biometrics	Relies on physical characteristics (iris, face, fingerprint, voiceprint, etc.) of the user. • Low administrative overhead—for solutions that use no client software and existing standard hardware • Easy and natural for the user—no special training or extra information to remember • The user's presence is verified, and credentials can't be lost, shared, or stolen

Approach	Description
Hardware Token	Uses a dedicated device, such as an RSA SecureID token. • High administrative overhead—may be complicated to install, configure, distribute, and manage • Customers have to replace all their tokens in the event the vendor sustains a breach • Supports a single application, which limits usefulness when you are deploying multiple cloud applications using multiple service providers
Software Token	Delivers a one-time password (OTP) using a device your user (employee, contractor, customer, business partner, etc.) probably already has, such as a mobile phone. • Low management overhead—doesn't require you to purchase, distribute, and manage multiple single-use hardware devices • Flexible—can be delivered through multiple channels: Smart phone app, SMS text message, email, IM, and more • Difficult environment for hackers to penetrate

Identity lifecycle management

Identity lifecycle management encompasses all the activities that IT administrators and security personnel perform to manage the user accounts—from creating the SaaS application account to terminating it when the user leaves the organization. This identity lifecycle is often referred to as the CReate-Update-Delete (CRUD) process (see Table 2).

Ordinarily, when a new employee comes on board, your IT administrator or application owner must use the SaaS application management interface to create an account for your users containing their user ID, password, and other useful attributes (department, phone number, manager, location, etc.) This process, which is the first step in the CRUD cycle, is typically referred to as provisioning.

Table 2. CRUD process.

Stage	Description
Create	Provisioning new hires quickly is important, since a delay in provisioning users results in a loss of employee productivity. Other employee lifecycle events, such as open enrollment for healthcare benefits, can also drive the need to create large numbers of identities in a relatively short period of time.
Update	As your user's attributes change (for example, transfer to another department or relocation to a new office), they should be updated in their identity profile, where appropriate.
Delete	When your employee leaves the organization, you need a mechanism to delete or disable their accounts on the target system(s). Otherwise, your organization risks allowing non-employees to access corporate data through these orphan accounts. Orphan accounts can also cost money in excess license or subscription fees.

Over time, employee attributes change, which often requires updates to their application profiles.

Finally, the employee leaves the organization, which results in the need to block them from being able to access sensitive SaaS apps.

The effort and expense required to manage the CRUD process is affected by a number of factors: Number of employees, number and variety of target SaaS applications, employee turnover, and seasonal hiring/firing patterns. As companies expand over time, they typically reach a point where the cost and inconvenience required to manage this process becomes high enough that it makes sense to consider automating it.

Other automation features can include a management console which provides provisioning/de-provisioning tools, as well as the ability to monitor user access activities, generate alerts, and collect event data logs.

Logs can be used for various purposes, such as capacity planning, audit, and compliance reporting. The latter are particularly important in certain regulated industries.

Regulatory requirements

Automating IAM processes can help your organization comply with various industry requirements and government regulations.

Privacy laws

Many jurisdictions in the United States and other countries require companies that capture and store private personal information to take specific steps to protect that data from unauthorized access.

Industry-specific requirements

Certain regulated industries have requirements for protecting private, personal, or financial information from unauthorized access. In some instances, these requirements are published by industry organizations, while in others they are mandated by the government.

A few examples include:

Table 3. Regulatory requirements.

Industry Requirement	Description
PCI DSS	The Payment Card Industry Data Security Standard is an example of non-government industry requirements. PCI DSS was developed by a consortium of payment card vendors (American Express, Discover, Visa, Mastercard, etc.) It specifies processes to protect personal information on credit cards or debit cards, including access controls and provisioning/de-provisioning of user accounts with access to payment card data.
HIPAA	The Healthcare Insurance Portability and Accountability Act mandates that healthcare providers implement procedures to protect personal health information data from disclosure. These include managing and monitoring access rights and enforcing secure password policies.
FFIEC	The Federal Financial Institutions Examination Council standards require multifactor authentication (MFA) to protect against the tactics of increasingly sophisticated hackers, particularly on the Internet.
GLBA	The Gramm-Leach-Bliley Act states that, "…each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."

Use Cases and Integration Requirements

SSO for cloud apps

Cloud SSO improves end-user convenience and productivity—users log on once to a trusted, secure portal controlled by their enterprise (either on-premise or in the cloud), and access authorized SaaS applications with a single click.

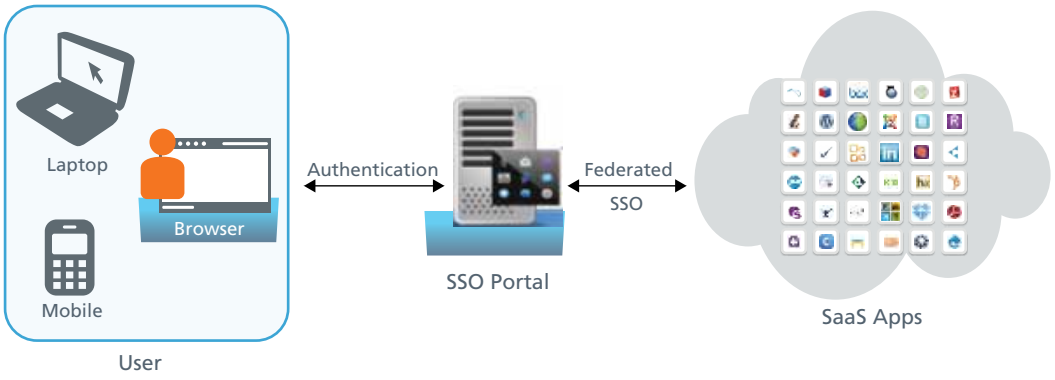

Figure 3. Federated SSO in the cloud.

Cloud single sign-on requires a high degree of integration between the IAM/SSO system and the target application(s). The Security Assertion Markup Language (SAML) is the standard of choice for authentication and authorization between domains. SAML has several important attributes:

- SAML is a widely adopted standard which is supported by most major SaaS application vendors
- SAML is based on a proven federated trust model
- SAML doesn't require a password. A SAML-protected service provider (SP) relies on the ability of a trusted identity provider (IP) to verify a user's identity.

Ideally, the solution should provide out-of-the-box SSO for a wide variety of popular SaaS applications. Buyers should seek out SaaS solutions which support SAML and ensure that their IAM solution also supports it in order to provide the foundation for secure federated SSO. Other authentication standards to consider include OAuth and OpenID. Most standards-based SSO is sometimes referred to as federated SSO, since there is a trusted relationship between the user and the various systems responsible for authentication.

If the SaaS application vendor does not support federated SSO using a standard, such as SAML, OAuth or OpenID, they may provide support for HTTP forms authentication or a proprietary API. When considering an IAM solution for SaaS, make sure the vendor supports the authentication model(s) supported by your SaaS app vendors.

Table 4. SSO authentication models.

Authentication	Description
SAML	Uses industry-standard assertions (SAML token) provided by trusted target platforms, ensuring future compatibility as technology evolves; reduces risk (since SAML assertions contain no passwords) and address cloud identity regulatory compliance concerns.
OpenID	OpenID is used by a resource provider (typically a website) to authenticate a user by redirecting the user's browser to an identity provider, which provides an authentication token used to obtain access. OpenID is designed for use over HTTP, so its use is limited to browsers.
OAuth	Unlike OpenID, OAuth is designed to be protocol-independent. Applications using OAuth can theoretically request/receive authentication tokens through a REST API using various protocols, including SAML, JSON (JavaScript Object Notation) or proprietary APIs.
HTTP Forms	Thousands of SaaS applications require users to authenticate by entering a user ID/password via a web form. SSO that works with HTTP forms enables the user to enter their user ID and password once. Their credentials are then stored in a secure password vault and transparently replayed whenever the user logs in after that.
Native API	A smaller number of applications support SSO by exposing an API that can be called by the SSO software.

Strong authentication for cloud apps

Strong authentication in a cloud environment can be performed using hard or soft tokens. Using a soft token for MFA, rather than a hardware token, has a number of advantages:

- There is no need to purchase, distribute, manage, or handle break/fix issues with a soft token
- A self-service portal can be provided where users can register their mobile device or download a smart phone app
- If a device, such as a phone, is lost or stolen, the user can replace the old phone number with a new one, effectively disabling the missing phone
- Soft tokens can be configured to work with multiple apps, while hardware tokens are typically associated with a single application

The most popular method of delivering a soft token is via an out-of-band mobile device, such as a smart phone app or a standard cell phone using SMS text messaging.

In this scenario, a user is challenged to enter a one-time password (OTP) as part of the authentication process. The system sends the OTP to the device. Without physical possession of the mobile device, the user (or a hacker) is unable to log on.

Integration requirements include a secure service-based architecture which can prompt the user to enter an OTP, generate the OTP, deliver it to the device for the user to retrieve and verify it once entered. Secure authentication depends on maintaining the integrity of the data flow across the network, as well as user training on how to protect their cell phone, or other mobile device, from compromise. Buyers should evaluate the complexity of the system, as well as the ease and convenience of the end-user registration process.

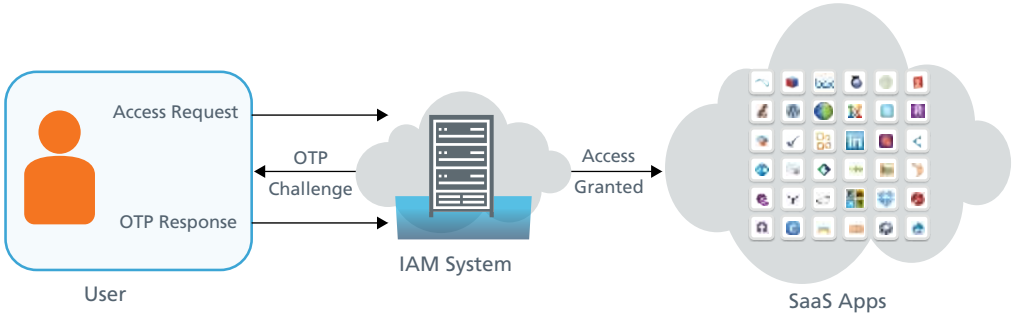

Figure 4. Strong authentication with OTP.

Context-aware authentication

With most vendor solutions, strong authentication is available as an all-or-nothing approach. What some IT administrators desire is the ability to selectively invoke MFA in particular scenarios. For example, it may make sense to invoke MFA for a specific group of users; when a user is in an insecure location or on a public network; or is accessing the SaaS application from a previously unknown device or IP address. Context-aware authentication allows you to define business rules that selectively enforce MFA, based on user identity-related attributes.

Identity lifecycle management for cloud apps

The basic identity lifecycle for SaaS applications consists of provisioning, managing, and de-provisioning user accounts in the cloud. Provisioning requires tools and processes to create user accounts on target SaaS platforms. The SaaS application administrator should have the ability to create multiple target accounts in as few steps as possible. Similarly, when the user leaves the organization, the system should support an automated process for disabling or deleting their SaaS application accounts.

There are two basic provisioning models for SaaS applications: To the cloud and in the cloud. Provisioning to the cloud from an internal site requires the ability to establish a connection between the provisioning engine (typically based on AD or some other identity repository) and the target application(s). This connection will be responsible for creating the user account on the target system and maintaining that account over time.

Provisioning in the cloud means implementing the provisioning engine as a cloud-based service offering. This is commonly referred to as Identity-as-a-Service (IDaaS). In this scenario, the system administrator uses the cloud service to create and maintain SaaS application accounts.

Most enterprises have an authoritative enterprise identity repository. Depending on business requirements, the IDaaS service may require establishing a connection to this repository. Integration with this repository is useful to keep user identities in the repository synchronized with the various identities managed in target applications. The repository typically contains information such as the user's identifier (user ID), password (in encrypted format), name, location, phone, department, logical groups, and other user-specific attributes. In most organizations, this data is held in Active Directory (AD) from Microsoft*, an enterprise LDAP directory, or in a database managed by a human resources (HR) system, such as PeopleSoft* or SAP*.

There may be instances where the identity attributes of different categories of users are stored in different repositories. An organization may keep the identities of regular employees in an HR system of record, contractor identities in a relational database, and customer identities in a customer relationship management system, such as Salesforce*. It's also not unusual for a single user's identity attributes to be stored in multiple locations, such as an employee name, ID number, manager, location, and phone number in the HR system of record, while their network user ID, network password, and email address are stored in AD.

When evaluating your integration requirements, it may be necessary to examine multiple systems to determine where relevant user identity attributes are stored.

Integration with internal repositories addresses multiple purposes: Provisioning, profile synchronization, and authentication. For example, when provisioning a SaaS account for a user, the attributes in the various repositories may be passed along to the target system, and kept in synch with the target system as they change over time (for example, a user transfers between departments or moves to a new location.)

Figure 5. Management portal.

Centralized user authentication relies on the user being authenticated once when they log onto their PC or a network. Once the user is reliably authenticated, that can provide the basis for enabling secure SSO to various target SaaS applications.

Regardless of which scenario (IAM in the cloud or on-premise) is used, the basic lifecycle is the same: an administrator uses the system to establish one or more SaaS application accounts on behalf of users, manages those accounts over time, and deletes or disables the accounts when the user leaves the organization. You should evaluate the ability of each vendor to support both provisioning AND de-provisioning for key SaaS applications.

Provisioning standards

The Service Provisioning Markup Language (SPML) standard was established to facilitate a vendor-neutral process for provisioning and managing accounts on target applications. Unfortunately, it is not widely supported by application vendors. As a result, IAM solution vendors have needed to create customized provisioning interfaces for each target application. Recently the System for Cross-domain Identity Management (SCIM) provisioning protocol has emerged. This new protocol is expected to be supported by influential SaaS providers, including Salesforce and Google.

Given the uncertain state of provisioning standards, you should carefully evaluate what provisioning capabilities are exposed by your SaaS vendors and whether the IAM solution you are considering supports those capabilities. Otherwise, you will need to work with your IAM vendor to create and maintain customized provisioning connectors.

Operational management

Management portal

The system should provide a management console (see Figure 5) that enables administrators to manage the identity lifecycle and monitor all identity-related events.

The console should deliver real-time utilization data, indicating recent successful and unsuccessful access attempts, as well as historical data that can be analyzed and provides a basis for utilization and compliance reporting. If your organization is subject to industry regulations you may want to use this data for compliance reporting purposes.

Figure 6. End-user SSO portal.

SSO portal

Many organizations provide employees with access to an enterprise portal used to provide convenient access to various applications. Common examples include IBM Websphere, Oracle WebLogic, and Microsoft Sharepoint. In many instances, the portal is responsible for authentication of a user's identity, or it may rely on another authentication system, such as Windows.

When selecting an on-premise IAM system, you should ensure that it will be compatible with your existing or planned enterprise portals. Implementing an IAM system that supports your enterprise portal enables you to create personalized portal pages, where authenticated users can have secure access to the various SaaS applications they are authorized to use. One advantage of using a personalized SSO portal approach is that users can be blocked from access to apps they are not authorized to use.

The same approach can be taken to an on-demand SSO portal by providing users with a personalized landing page in the cloud. Once the user authenticates to the page, they will see all the SaaS applications they are authorized to access, and click on the icon to log on.

In today's cloud access environment, it has become standard to provide users with access to dozens or hundreds of pre-configured cloud apps. During the evaluation process, determine whether you or your vendor can provide this capability, since without it, your IT team will have to design and implement web links and other features of the portal.

On-premise deployment

An on-premise solution is the traditional approach to implementing IAM. The major advantage on-premise systems have is their ability to integrate with various internal systems behind the firewall, such as an authoritative identity repository.

Some organizations consider user credentials to be the "keys to the kingdom," and feel more secure knowing that they are held internally and are relatively safe from external attack. However, this advantage may not be as strong as it might have once been. More than one organization has been broken into by a skilled hacker and user identities and passwords stolen, exposing the enterprise to further attacks.

Like most other on-premise systems, an on-premise IAM solution typically involves acquiring dedicated hardware, a perpetual software license, and paying for ongoing annual maintenance fees.

These up-front costs can be ameliorated by using virtualization technology to enable greater utilization of existing systems, and obtaining an annual subscription license rather than a perpetual software license. In addition, if extensive customization or configuration is required, you may wind up paying the vendor or a system integrator for deployment, integration, and other professional services. Finally, operational expenses tend to be higher, since dedicated IT personnel with specialized skills or training are typically required to manage and maintain the system, including backup/recover, patching, configuration management, updates, and more.

In-the-cloud deployment

As the cloud has become more popular over the past several years, more companies are considering the advantages of outsourcing their IAM software to a cloud-based services provider:

- On-demand computing services convert fixed costs to variable costs—the customer buys services as they are utilized, not for the fixed capacity available for use that must be amortized over the useful life of the asset
- Most service providers utilize a multi-tenant architecture, which enables them to cut costs and pass those savings on to customers

- Service delivery is elastic and responsive to dynamically changing business circumstances—customers can expand service volume without worrying about adding more internal hardware capacity
- Operational complexity is eliminated—the service provider is responsible for operational details, such as backup/recovery, updates, patches, and the like. Service Level Agreements (SLAs) are available to meet demanding availability and reliability requirements.
- Shifting from owned assets to contracted services may improve the company's balance sheet by increasing both return on assets and financial leverage—raising the company's return on equity
- Implementation is relatively quick. On-demand customers can start small with a trial and expand as needed. Full deployment can occur in less than 30 days for fast, visible return on investment (ROI).

There are several commonly seen adoption scenarios for IDaaS.

In one scenario, a large enterprise might start using IDaaS to manage external workers (such as contractors, temps, or business partners), or in support of a merger or acquisition. IDaaS in this scenario may be a good way for an enterprise to test the waters and validate the usefulness of IDaaS. Some companies, such as small to mid-sized businesses (SMB), have adopted a "Cloud First" model and are comfortable with building their infrastructure in the cloud. These companies are likely to have a relatively unsophisticated on-premise identity infrastructure, consisting primarily of an enterprise directory, such as Microsoft AD. By adopting an IDaaS approach, they get the ability to leverage best-of-breed features provided by leading edge IAM vendors in the cloud.

There are two major issues that companies should consider when moving their user identities to the cloud.

The first is security. Evaluation of a vendor's service offering must include a rigorous security review to ensure the vendor's infrastructure and operational procedures deliver the highest level of asset protection, commensurate with the cost.

The other is the risk associated with the vendor's business model. Companies considering moving IAM functions to the cloud should consider more than feature/functions offered by competing vendors. In particular, the vendors' strength and viability on a number of dimensions: Financial, engineering, support services, and more should be evaluated. Placing critical business functions, like identity, into the hands of a fast-growing startup requires explicit consideration of their ongoing viability. When negotiating with a vendor, be sure you understand what will happen to your assets in the event the vendor is acquired, encounters cash flow or other growth-related problems, or goes out of business.

Hybrid deployment

Some companies choose to deploy a hybrid solution. There are a variety of available scenarios, such as moving the IAM function to the cloud, but maintaining a link to an internal repository for automated identity provisioning and synchronization. Another is to use an internal solution for managing the identities of employees, while using an IDaaS solution to manage identities of external users.

Regardless of the model you select, you also need to consider the vendor's support for enterprise-class features, such as:

- *Security*—the system should protect all networked transactions with strong encryption using SSL
- *High availability*—the system should support clustering and other technologies that ensure continued operations in the event of a component failure
- *Performance*—the system should be able to scale up to support thousands of transactions per second without noticeable degradation of end-user response time

Cloud Security Ecosystem

One element that's important for organizations to consider when moving their identity and other IT assets to the cloud is the emerging role of the cloud security broker (CSB). A CSB shields the internal enterprise from the complexity of consuming 1-n cloud services from multiple providers. As an enterprise adopts cloud services billing, SLAs, integration, web service governance, and identity functions become too complex to manage internally at scale. Just as EDI evolved from expensive internal integration groups to third-party operating exchanges to aggregate and simplify consumption, the cloud and SaaS services are following a similar pattern. CSBs can be third parties that aggregate, integrate, and customize service offerings from multiple cloud providers or in large enterprises—these can be IT departments that set up CSB infrastructure to service 1-n internal departments.

CSBs are relatively new but the technology platforms that CSBs utilize are based on mature technologies such as federation gateways, IDaaS operators, monitoring billing applications, and e-catalogs. Security Gateways are the most important CSB technology in that they can expose, govern, and secure cloud application APIs. Today almost one-third of all enterprise traffic to the cloud is API based. Below, we outline some of the identity functions of a security gateway at the API level.

Cloud security gateway

There are several areas where a security gateway adds value to cloud identity models:

- *Security Token Services:* As web services are used to transact data from the enterprise to the cloud or to partner applications, they are crossing different security domains. Each domain relies on a particular identity token format for authentication. A Security Token Service (STS) validates enterprise security tokens, like Kerberos tickets from Active Directory, and can exchange one identity token format for another so that a transaction can be authenticated to process. In many cases this is called identity brokering or identity mapping.
- *Cloud API Management:* The mantra of "reusing" existing application assets as services has become established as part of the common language associated with cloud-based infrastructure sharing. The key to exposing application functionality is through APIs and this is well understood by developers. Cloud-based API management presents a new discipline with added security, visibility, integration, and scale requirements. As applications are shared outside the protective firewall to/from the cloud and among cloud providers, traditional firewalls do not provide the mediation or XML threat protection required to expose these applications safely. Features that manage cloud APIs provide a new means to meter, throttle, and audit how services are consumed. A cloud service broker can provide the backbone for a cloud provider or an enterprise to create an API monetization program that bills back departments or charges other entities for API usage.

More Info and Other Resources

McAfee provides a wide variety of online assets for you to investigate your cloud identity and access management options. They include:

- *Analyst research*—access to research reports published by firms like Gartner, Forrester, IDC, 451 Research, and others
- *Demo videos*—short clips with subject matter experts describing topics like SSO and strong authentication
- *Product briefs*—downloadable descriptions of specific IAM products for the cloud
- *White papers*—white papers, such as this Buyer's Guide, covering a variety of identity and security topics
- *Customer case studies and videos*—assets with detailed descriptions of how McAfee customers have met the challenges of cloud identity and asset management

For more information, visit www.mcafee.com/identity.

Appendix I—Sample RFP

Section I. Company background information

1. How long has your SaaS IAM solution been on the market?
   a. What is the current release version of your IAM product?
   b. List how many prior versions of your product have been released to the market.
   c. Please include any relevant awards or analyst coverage your solution has received.
2. Please provide three (3) customer references. Ideally, these clients should be organizations with a size and scope similar to our environment.

Company Name	
Name/contact information	
Number of users under management on the system	
General description of their deployment (number of users, systems they are provisioning, type of workflows)	
Date they went into full production with your system	
Business results that have come from the deployment of your solution	

3. Did your organization develop your SaaS identity management solution in-house or was it acquired from other vendors? If acquired, please answer the following:
   a. What different products or vendors were acquired to build out your solution?
   b. How do the products work with one another?
   c. How will you ensure seamless interoperability of the products moving forward?
4. Provide a brief history of your solution, highlighting milestones and unique features your company has introduced to the market.
5. Provide a product roadmap highlighting future plans for your IAM solution.
6. Are you willing to complete a free trial? Provide an overview of your trial process.
7. Describe the various software modules that come packaged with your IAM solution (for example, provisioning, password management, strong authentication, reporting, etc.)
8. What industry standards (for example, SAML, XACML, OAuth, OpenID, etc.) does your product support?
9. Describe your product's support for high availability and scalability.

Section II. User provisioning capabilities

10. Describe your solution's provisioning capabilities. For each requirement below, indicate whether this is out-of-the-box functionality, requires customization, requires a third-party product, or is not available.
    a. How will the administrator initiate the provisioning workflow? Please include screenshots.
    b. Does your product provide the capability to delegate provisioning?
    c. What are the various types of provisioning actions your solution offers (for example, create, change, disable, delete, etc.)?
    d. Can your SaaS application provisioning system integrate with existing on-premise identity and access management systems?

e. What are the various types of provisioning workflows your solution offers (for example, requestor/approver, self-service, bulk, etc.)

f. What is the process to create or change a provisioning workflow? What type of skill set does this process require (for example, coding or development)? Please include screenshots.

11. Describe how your provisioning solution will integrate with our target SaaS applications to automatically provision user accounts. For each requirement below, indicate whether this is out-of-the-box functionality, requires customization, requires a third-party product, or is not available.

    a. Please list all SaaS applications that your solution can provision out of the box.

    b. What is the level of detail your provisioning connectors provide?

    c. What options do we have for creating provisioning connectors for systems not currently supported by your product? Who would build these connectors (for example, your company or ours)?

    d. Does your provisioning solution support integration with our on-premise identity repository? Can your solution automatically provision/de-provision user SaaS accounts if the user profile in the identity repository changes (add, change, delete)?

Section III. Single Sign-On (SSO) capabilities

12. Describe your SSO capabilities. For each requirement below, indicate whether this is out-of-the-box functionality, requires customization, requires a third-party product, or is not available.

    a. Identify whether or not you support SSO for the following SaaS authentication models: SAML, HTTP POST forms, OAuth, proprietary API.

    b. Do you have a mechanism for users to view SaaS applications they are authorized to access? How do you restrict their view to only authorized applications?

    c. How do you handle password errors, expiration, or reset notices from the target SaaS application?

    d. Does your solution support SSO based on Windows authentication?

    e. What happens if a user changes their password natively in Active Directory? Will the passwords get out of synch?

    f. Can we choose to establish an end-user SSO portal on our intranet or in the cloud?

    g. What tools are available for the system administrator to deal with password issues?

    h. Describe your support for native target platform password policy requirements (length, strength, dictionary use, password reuse, password expiration, etc.).

Section IV. Strong authentication capabilities

13. Describe your strong authentication capabilities. For each requirement below, indicate whether this is out-of-the-box functionality, requires customization, requires a third-party product, or is not available.

    a. Describe how your solution supports strong authentication.

    b. What out-of-band channels are supported for strong authentication via one-time password (OTP) soft token?

    c. Can your solution selectively invoke strong authentication, based on user attributes defined by the system administrator (for example, user group, user ID, network IP address, etc.)?

Section V. Architecture overview

14. Please provide a general overview of your IAM architecture.

    a. Will your IAM solution require us to implement or maintain any proprietary infrastructure?

    b. Will we need to consolidate our information into one directory to deploy your IAM product?

    c. Can your product simultaneously work with multiple directories or data sources?

d. If we integrate your product with Active Directory, will it require (and would you recommend) that we modify our AD schema?

e. How is your product architected to deliver enterprise-class reliability, availability, and performance? Does it have support for a distributed IT infrastructure?

15. Connectors

a. Describe the breadth of your portfolio of connectors to SaaS platforms.

b. How many connectors are available?

c. Are connectors bundled with your suite or sold separately?

d. How many connectors work out of the box?

e. How many will require customization to work in our environment?

f. Describe the process of maintaining connectors as our environment changes.

g. Describe the process of making new, custom connectors available for our systems.

Section VI. Deployment and management

16. Describe the implementation process for your solution.
17. Can your solution be integrated into our corporate portal using our look-and-feel?
18. Does your solution provide the flexibility to be deployed either on-premise or as a service?
19. How does your solution capture corporate security policies and incorporate them into the system?
20. Describe your suite's audit and reporting functionality.

a. What type of reports come standard with your solution?

b. Does your suite support standard reporting tools?

c. Does your solution have the capability to create a secure, full audit trail for any identity-related operation?

Section VII. Implementation services

21. Describe what professional services will be required to deploy your solution. Will professional services be provided by your organization, a sub-contractor, or a third party?
22. What resources will your firm assign to our implementation? Describe their roles and responsibilities during the implementation.
23. How long do you anticipate it will take an organization of our size and scope to deploy your solution?
24. Describe your standard implementation methodology.

a. What are your best practices for minimizing project risk, while demonstrating incremental value and "quick wins" throughout the project lifecycle?

b. How will you assist us in collecting and analyzing data to demonstrate the ROI of your solution?

25. What is the pricing model for professional services: Fixed-fee or time-and-material?

Section VIII. Post-deployment

26. Describe the post-deployment support services available from your company.

a. Can we get support 24x7?

b. What SLAs are available to us as a customer?

c. Describe how you track and manage customer issues to ensure high-priority problems are addressed in a timely fashion to minimize disruption to our business.

Section IX. Licensing and pricing

27. Describe your licensing and pricing model.
    a. Software licensing—provide software pricing for the relevant software modules provided by your company that would satisfy the requirements in this RFP.
    b. Does your software licensing include unlimited application connectors, or is there a charge for each additional SaaS application?
    c. Does your licensing model provide the flexibility for either an on-premise or on-demand service deployment for the same price point?
    d. Maintenance and support—provide pricing for your maintenance and support options. Is 24x7 support provided as part of the base license, or will it cost extra?
    e. Provide a description of what is included with your maintenance and support options. Provide maintenance costs for year one and future years as well.
    f. Professional services—provide pricing for the installation services your company will deliver. List what types of resources would be assigned to this project and their hourly billing rate. List pricing for any additional post-deployment services.
    g. Administrative or end-user training—provide course descriptions and fees of the various administrator or end-user training options your company provides. Indicate whether these training courses are held at your company or if they can be onsite at our facilities.

Appendix II—Industry Glossary and Acronyms

Acronym	Meaning	Additional Info
CRUD	CReate, Update, Delete	Refers to the major lifecycle operations applied to a user's identity.
IaaS	Infrastructure-as-a-Service	Delivers relatively raw hardware, operating systems, storage, and network capacity as a service via the web.
IAM	Identity and access management	A technical business process which encompasses the CRUD lifecycle of a user's identity, regardless of delivery model.
IDaaS	Identity and Access Management-as-a-Service	IAM functions outsourced to an external service provider.
IDaaS*	Identity-as-a-Service	Similar to IDaaS, but may provide certain limited aspects of IAM, such as authentication or authorization.
OAuth	Open Authorization	An open standard for authorization. (Wikipedia)
OOB	Out-of-band	An alternate channel used to deliver an OTP, which is separate from a primary authentication channel.
OpenID	Open ID	An open standard used by web identity providers (Facebook, Google, etc.) to share credentials with other entities. (OpenID.net)
OTP	One-time password	A technique of challenging a user to enter a one-time password delivered via an OOB channel, such as a cell phone. The user authenticates by demonstrating possession of a device or token.
PaaS	Platform-as-a-Service	Delivers higher-level IT services (for example, security, management, middleware, etc.) layered on top of IaaS. IDaaS is a form of PaaS.
SaaS	Software-as-a-Service	The delivery of an application by an external service provider without the need to acquire, deploy, or manage hardware or software internally, other than a web browser.
SAML	Security Assertion Markup Language	The leading industry standard for managing federated SSO between applications. (OASIS)
SCIM	System for Cross-domain Identity Management	An emerging standard for managing provisioning and de-provisioning SaaS accounts. (SCIM)
SPML	Service Provisioning Markup Language	An XML-based framework for exchanging provisioning information between cooperating organizations. Has not been widely adopted due to implementation complexity, hence the emergence of SCIM. (Wikipedia)
SMS	Short Message Service	A system that enables cellular phone users to send and receive text messages
XACML	eXtensible Access Control Markup Language	An open XML-based access control framework designed to abstract and separate the authorization process from an application. (Wikipedia)

[1] See *Appendix II—Industry Glossary & Acronyms* on pg.17.
[2] "*Worldwide Software as a Service 2011–2015 Forecast*", IDC, August 2011
[3] "*US Government Cloud Computing Technology Roadmap, Volume I*", National Institute of Standards and Technology, Special Publication 500-293, Nov. 2011

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60167wp_cloud-sso_0413_fnl_ETMG