White Paper

Identity in the Cloud

Use the cloud without compromising enterprise security

Table of Contents

The cloud is growing at an exponential pace. Organizations of all sizes are moving IT operations and functions to the cloud and are under pressure to provide mobile and remote users with secure access to critical business applications and systems. As organizations embrace Software-as-a-Service (SaaS) applications, IT and application administrators soon become overwhelmed with the problem of ensuring managing access to those applications is consistent with enterprise security policies.

The Cloud Conundrum

Enterprises of all sizes—especially small and mid-sized businesses (SMBs)—are flocking to embrace cloud computing because of the many advantages it provides. These include lower costs, greater business agility, reduced IT administrative overhead, and more. According to industry analyst firm IDC, the SaaS market reached $16.6 billion in revenue in 2010 and is projected to grow at more than 25 percent per year until 2015.[1]

A key benefit for many SMBs is the opportunity to take advantage of hundreds, even thousands, of applications available in the cloud. There are cloud solutions that address virtually any conceivable business need: sales, marketing, human resources, collaboration and communication, finance, legal, and much more. However, as companies adopt a SaaS application strategy, they quickly realize that they need to manage users identities in the cloud for a variety of reasons.

The proliferation of SaaS solutions within the enterprise leads, inexorably, to a plethora of identities and creates a unique operational challenge: how to efficiently manage all the identities that users require—one for each cloud application they access.

> *"… 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."*
>
> —*Cloud Computing Technology Roadmap*, National Institute of Standards and Technology (NIST)

As new users join the company, they need cloud accounts that are synchronized with their internal identities. Similarly, as their roles change or when they leave, their accounts need to be appropriately updated or automatically terminated. Leaving orphan accounts active risks potential security breaches and data leaks.

The cloud is unique in that it allows an organization to extend its application infrastructure to external users. Previously, if you wanted to share internal applications with external users (suppliers, distributors, service providers, and contractors) you were forced to deploy a proprietary access solution, such as a VPN or FTP server. Now, with the cloud, you can provide partners with their own credentials and give them direct access to the application. However, you still need to maintain control over these accounts.

Moreover, as more and more applications become part of the enterprise portfolio, users desire a single entry point into all their applications, eliminating the need to remember multiple user ID/password combinations. When people must remember different credentials for different applications, some will invariably resort to writing them down and storing them in an insecure location, such as a sticky note posted on their terminal. This obviously presents a challenge for any organization concerned with security, especially in a regulated business, like financial services, government, and healthcare.

A third consideration, particularly relevant to cloud-based applications, is the need to invoke strong, out-of-band authentication for certain use cases, where users should be challenged to authenticate themselves with more than a user ID and password. For example, users who are located outside the firewall, such as contractors or business partners, who belong to a particular group, or who use a particularly sensitive application, would all be candidates for multi-factor authentication (MFA).

Managing Cloud Identity

The best way to address these concerns is to deploy identity management processes and technologies to ensure that only authorized users have access to cloud applications. In the *Cloud Computing Technology Roadmap*, the National Institute of Standards and Technology (NIST) highlights this concern: "… 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."[2]

Security is one of the leading concerns expressed by companies adopting a cloud strategy. They worry that moving critical information and documents into the cloud will expose them to unauthorized access. They need a solution that will enable them to create, manage, and terminate SaaS/cloud accounts and provide strong authentication for situations where sensitive data is stored in the cloud.

An identity and access management (IAM) solution provides administrators with the tools they need to create, manage, and terminate user accounts to popular SaaS applications. In situations where particularly sensitive data are stored in the cloud, it provides strong authentication capabilities, such as requiring a one-time password (OTP) to reliably validate the user's identity before granting access.

The Identity Lifecycle

There are three major stages in the user identity lifecycle:

- *Add*—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 the user with their user ID, password, and other useful attributes (department, phone number, manager, location). This process is typically referred to as provisioning.
- *Edit*—Over time, employee attributes change, which often requires updates to their application profiles
- *Delete*—Finally, the employee leaves the organization, which creates the need to block them from access to sensitive SaaS applications

The effort and expense required to manage the identity lifecycle process within your organization 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.

SaaS Single Sign-On

Every SaaS application has its own authentication infrastructure, and they all have one thing in common: they require a user ID and password to log on. An single sign-on (SSO) system eliminates the need for passwords.

Organizations that deploy SSO find that their users enjoy its convenience and are happy not to have to remember multiple IDs and passwords. Eliminating passwords also reduces the potential for a security breach and often results in reduced password-related help desk calls, allowing busy IT personnel to focus on more value-added tasks.

SSO increases end-user convenience and productivity, since the user only has to click an icon to be granted access to the application. Similarly, when the user logs off the SSO system, all open sessions are automatically terminated.

There are four different SSO models:

- Security assertion markup language (SAML)-based
- Application programming interface (API)-based
- Agent-based
- HTML form-based

SAML

SAML has evolved into a robust, mature industry standard. SAML establishes a trusted, federated relationship between a service provider (SP) and identity provider (IP). SAML authentication relies on the secure exchange of a software token, and no password is required.

SAML also supports SP-initiated authentication. With SP-initiated authentication enabled, the SP (the target SaaS application) can be configured to redirect a user to the IP authentication portal, where their credentials must be validated in order to enter the application.

Other identity-related standards similar to SAML which are used for authentication include OpenID and OAuth.

API

API-based authentication depends on the SP exposing a proprietary API, which the IP can use to SSO a user into the application. Netsuite is a well-known example of a SaaS application that uses API-based authentication.

Agent

In situations where a target application will allow an agent to be installed, agent-based authentication can be employed. Depending on the target application architecture, you may need to use a Java, .NET, or PHP agent.

HTML form

The lowest common denominator for authentication is an HTML form. The preferred way to provide SSO to a form-based application is for the SSO system to capture and encrypt the user credentials (user ID and password), store them in a secure password vault, and replay them transparently whenever the user tries to access the application.

Multi-factor Authentication

Multi-factor authentication (MFA) used to be limited to expensive, complex, and difficult-to-manage hardware tokens. Over the past few years, soft tokens have emerged which leverage something your users probably already have—their cell phones.

Using the soft token model, when a user attempts to access a protected application, he is challenged to enter a one-time password (OTP). He retrieves the OTP from a device, typically a cell phone or smartphone. Strong authentication using soft tokens can also be implemented using IM, chat, web browsers, and other out-of-band channels.

There are two big advantages to the soft token-based OTP approach. First, management and administration costs are much lower than with hard tokens. Most users already have a cell phone, so all they need to do is go to a self-service portal where they register their phone and, if they're using a smartphone, download an app. If users are using a standard cell phone, then they will receive the OTP via an SMS text message.

In either case, the user manages the device, not the IT administrator. Administrators don't need to purchase and physically distribute tokens, nor do they need to worry about retrieving tokens when the user leaves the organization. If the phone is lost or stolen, or the user switches to a new phone, all they have to do is update their registration profile, which immediately disables the old phone.

The second advantage is that a single soft token can be used to protect multiple SaaS applications. Hard tokens typically support only one application per token. A soft token-based device can support multiple profiles for multiple apps.

McAfee Cloud Identity Solutions Overview

McAfee is widely known as a leading provider of enterprise and consumer security software. IAM is an essential component of any enterprise security architecture. In 2012, Intel transferred its identity solutions to McAfee, enabling McAfee to deliver more comprehensive and competitive security solutions consistent with our Security Connected framework.

McAfee One Time Password

McAfee® One Time Password provides strong authentication for controlling remote access to high-value IT resources, hosted applications, websites, mail servers, and online transactions. McAfee One Time Password also supports major VPNs out of the box. Quick and easy to install, configure, and maintain, this strong authentication solution secures access to business critical information anywhere it's stored or accessed. User identity is verified because the user must demonstrate possession of a second factor—in this case a cell phone or other mobile device. When users attempt to access an application protected by McAfee One Time Password, they are challenged to enter a one-time password (OTP), which is delivered to them through the mobile device. The user then enters the OTP into the prompt, which, when verified, allows users to access the app.

McAfee Cloud Single Sign On

McAfee Cloud Single Sign On is an identity and access management solution for cloud/SaaS applications. It has four major functions out of the box.

Provisioning/de-provisioning

Provisioning and de-provisioning allow system administrators to create and terminate SaaS accounts for users. The process can be synchronized with enterprise identity repositories, including Microsoft Active Directory (AD), any LDAP-enabled directory, relational databases, or other identity sources. Multiple sources can be combined to create a single, unified identity profile for a user.

Business rules can be established that automatically create SaaS application accounts, based on changes in the repository (add, edit, delete), and to determine which SaaS accounts are suitable, based on user profiles. For example, a rule can be set up that anyone in the sales group in AD is automatically provisioned with a Salesforce.com account, while anyone in marketing gets an Eloqua account.

Single sign-on

The system administrator can configure SSO for hundreds of SaaS applications, using pre-configured identity connectors available through the management console, and assign individuals or groups of users to the SaaS application. Four SSO models are supported for maximum flexibility: SAML-based, API-based, agent-based, or HTML form-based.

The user can be authenticated to the SSO portal in a number of ways, including Integrated Windows Authentication, by logging in via the McAfee Web Gateway, or via a third-party tool, such as CA Siteminder. Once users are authenticated to the SSO portal, they land on a dynamically generated, personalized page with links for all the SaaS applications they have access to. All users need to do is click on the link to log onto the target application without having to re-enter any additional user ID or password.

Strong authentication

McAfee One Time Password is included with McAfee Cloud Single Sign On. Depending on your specific security needs, you can use OTP to protect the SSO portal or any downstream SaaS application.

Context-aware authentication

Access to a target SaaS application can be restricted depending on certain attributes:

Context	Result
OTP verification	Requires the user to verify their identity by entering a one-time password
Browser type	PC or mobile device OS (Apple iPhone/Apple iPad, Google Android, BlackBerry, and others)
IP address	Only allows IP addresses within a specific range
Intel Identity Protection Technology	Requires IPT chip on user's PC; used to validate that the user is using a known, properly configured (antivirus, OS, patch level, and more) computer
Time of day or day of week	Time-based access restriction
Authentication context	Boolean expression that retrieves one or more attributes from the authentication results and tests their values

Management console

The McAfee Cloud Single Sign On management console is used to configure SaaS applications for SSO and provisioning, monitor user access, and manage various system operations. A key function of the console is ensuring compliance with enterprise security policy or relevant regulations. Customers can define and access audit events through the Audit and Alerts features, which generate an audit log and alert log, respectively. To configure the audit log, you configure an auditing policy, which is effective as soon as it is saved. To generate the alert log, you configure one or more alert triggers. Once configured, audit events and alerts are dynamically entered in the audit and alert logs, respectively, as they occur.

McAfee includes built-in measures that summarize system data called metrics. Using the metrics page, you can select measures that summarize system data. You can configure and apply a filter, view the results, download the cloud metrics to a file for analysis with an external tool, purge or clear the cloud metrics.

Hybrid Model

McAfee Cloud Single Sign On is available in two versions: an on-premises edition and SaaS edition.

Both versions include SSO, provisioning, de-provisioning, multi-factor authentication, and a management console. Customers have the option of purchasing licenses and applying them to one version, or the other, or both. For example, a company may purchase licenses and distribute some to employees using the on-premises edition and the rest to external users (contractors, distributors, suppliers, customers) using the SaaS edition.

On-premises edition

The on-premises edition is a downloadable software package that can be installed on any suitably configured Windows or Linux server. Integration with AD or any supported identity repository can be configured for automatic provisioning/de-provisioning. The SSO and administrative portals are typically configured using any iFrame-enabled enterprise portal, such as Sharepoint, Webshere, or Weblogic.

SaaS edition

The SaaS edition is a cloud-based service offering. Both the system administrator and user log onto a cloud-based portal, and all functions and operations are available in the cloud. Both provisioning/de-provisioning and user authentication using AD is available. Integration with AD (or any LDAP-enabled directory) can be achieved either by opening a firewall port from the SaaS platform to the AD system inside the data center or by downloading an agent to an internal data center (which doesn't require opening any firewall ports). The major difference between the on-premises edition and SaaS edition are the range of available SSO connectors. Please contact McAfee for details on the SSO connectors available on SaaS edition.

Hybrid use case: protect sensitive documents in the cloud

An organization wants to use a file sharing system, such as Box, to share contracts and other sensitive documents with its outside legal counsel or business partners. While organizations are confident that the file sharing application itself is secure, they are concerned about controlling access to it.

Internal users

For internal users, the organization deploys McAfee Cloud Single Sign On, on-premise edition. Integration with AD, the enterprise's authoritative identity repository, enables IT administrators to automatically provision executives and employees in the legal department with a Box account. Users are authenticated using their Windows credentials, which grants them access to a secure SSO portal. Authorized users see a Box icon, which they click on once to access their Box account. When employees leave the enterprise, McAfee Cloud Single Sign On detects the change in the employee AD record and automatically terminates the Box account.

External users

To manage external users, the enterprise deploys McAfee Cloud Single Sign On, SaaS edition and configures the Box application to require two-factor strong authentication. This forces external users to verify their identity with a one-time password (OTP). When the IT administrator provisions the user with a Box account, the user must register a mobile device (smartphone or standard cell phone) with McAfee Cloud Single Sign On. (Note that users supply the cell phones, and the administrator has no responsibility to distribute or manage these devices.) Whenever a user wants to access Box, he authenticates to the secure SSO portal in the cloud, clicks on the Box icon, and enters the OTP, which he retrieves from his mobile device. Without a mobile device, he cannot access the system.

If the user loses or changes his cell phone, he simply unregisters it on the portal, rendering it useless to a potential hacker. When he no longer needs access, the system administrator removes the user's McAfee Cloud Single Sign On record, eliminating his ability to access the sensitive documents.

The combination of authentication methods deployed for internal and external users provide the highest level of assurance that only authorized personnel have access to sensitive applications in the cloud. System log files that allow IT administrators to monitor all access activity—including successful and failed logon attempts—can be used for audit and compliance reporting purposes.

Pricing Model

McAfee Cloud Single Sign On is available by subscription. The subscription includes:

- Unlimited use of any combination of the on-premises edition or SaaS edition
- Unlimited number of application connectors for provisioning and SSO
- Built-in multi-factor authentication support with OTP
- 24/7 support, maintenance, and upgrades

McAfee Security Integration

As organizations transition to a comprehensive cloud access model where user authentication, data, and application service security are brokered by IT or third-party providers, McAfee identity solutions for SaaS applications are aligned with the Security Connected Reference Architecture, providing enterprise-class security policy enforcement, threat protection, and collaboration across all cloud traffic channels.

As a world-class security vendor, McAfee delivers insight into emerging security technologies that can be used to build a trusted client-to-cloud connection. McAfee is unique in that, unlike any other vendor, it offers integrated preemptive protection that crosses all security layers.

Conclusion

Companies that adopt the cloud application model must be concerned with how to manage their users' access to those applications, especially remote or mobile users.

They also need to consider how best to protect those applications from unauthorized access, with a multi-layered strong authentication model.

With McAfee identity, web protection, and Security Connected solutions:

- Your organization can enjoy the benefits of the SaaS delivery model
- Your employees will be more satisfied and productive
- And, your organization will be more secure

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

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com

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

[1] *Worldwide Software as a Service 2011-2015 Forecast*, Aug. 2011, IDC
[2] *Cloud Computing Technology Roadmap*, National Institute of Standards and Technology (NIST)

60195wp_identity-cloud_0413_fnl_ETMG