

WHITE PAPER

Cloud Security - The CA Technologies Strategy and Vision | April 2012

CA Technologies strategy and vision for cloud identity and access management

Sumner Blount
CA Security Management

agility
made possible™





table of contents

executive summary

SECTION 1: 4
Embrace the cloud in a managed and secure fashion

SECTION 2: 4
Three perspectives on cloud security

SECTION 3: 8
CA Technologies strategy for cloud security

SECTION 4: 11
Conclusions

SECTION 5: 12
About the author

executive summary

Challenge

With all its inherent value, the cloud introduces new security challenges for both consumers and providers of cloud services in all types of IT environments.

A challenge for enterprises is how to leverage existing investments in identity and access management (IAM) solutions and extend their reach to the cloud in a hybrid on-premise/off-premise world to reduce operational costs and enable enterprise agility.

Challenges for cloud service providers include how to secure an evolving virtualized environment and how to maintain the integrity of tenant information.

Note: Identity and Access Management is the set of processes and the supporting infrastructure for the creation, management, and use of digital identities and enforcement of access policies.

Opportunity

The key opportunity offered by the cloud is the increased efficiencies that can be gained from leveraging cloud-based services. However, these efficiencies come with concerns relating to the security of applications and information that are stored in the cloud and that span the hybrid environment. The CA Technologies vision and strategy for cloud-based identity services enable organizations and service providers to:

- Securely provision to, and access, cloud-based services and on-premise apps
- Choose the IAM deployment option (on-premise, hybrid, or cloud) that meets their unique business and security needs
- Simplify the management of IAM services across both on-premise and cloud deployments

The cloud also provides opportunities for smaller organizations which have previously viewed on-premise IAM as out of reach for reasons of cost of complexity or lack of internal skillsets. IAM delivered as cloud services gives smaller organizations that ability to leverage IAM capabilities without significant hardware investment, IT knowledge, or long deployment cycles.

Benefits

CA Technologies offers cloud security solutions that can enable organizations to access cloud applications and enterprise resources securely. These solutions enable organizations to increase business agility and efficiency by deploying cloud-based identity services to protect their critical resources, whether they are on-premise or in the cloud. This can result in:

- Reduced security risk for all systems, applications, and information
- Reduced administrative expenses and improved efficiency
- Improved IT agility through flexible deployment options across on-premise and cloud environments
- Reduced time-to-value

Section 1:

Embrace the cloud in a managed and secure fashion

CA Technologies has long been a leader in the identity and access market as part of our overarching strategy to help the enterprise govern, manage, and secure IT. For years we have been expanding our set of IAM products to address the most demanding business challenges that our enterprise customers face, and to incorporate new and evolving technologies.

Just when organizations thought it was safe to coast forward incrementally with their IAM strategy, however, along came the cloud with a new set of business opportunities and challenges to disrupt the status quo.

One thing that is clear is that identity, and the management and controls dependent on it, are absolutely central to the secure adoption of cloud services. The goal of this paper is to provide the reader with an overview of the CA Technologies strategy and vision for identity and access management for the cloud.

Section 2:

Three perspectives on cloud security

TO THE CLOUD - Extending enterprise security systems to the cloud

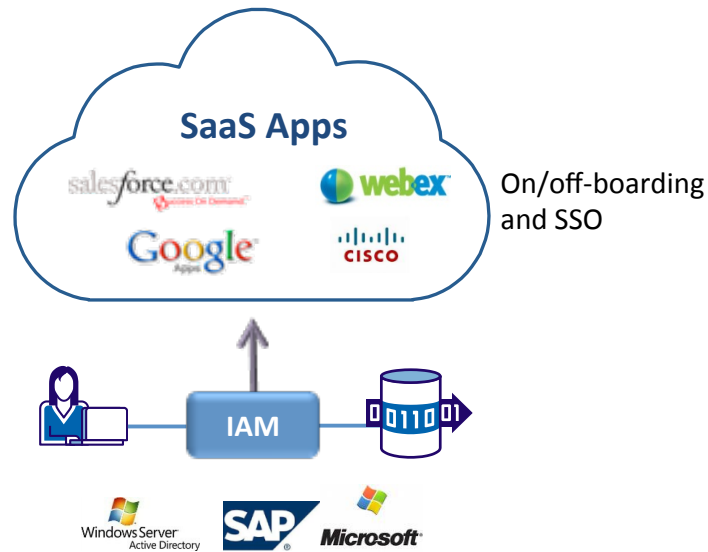
From the perspective of cloud-consuming organizations—many of which already have hundreds of deployed, on-premise applications—cloud-based services are implemented in addition to, rather than in place of, existing applications. Security and audit professionals at these organizations are challenged to extend consistent existing security systems and practices—which may have continually evolved and improved over the years—to encompass their cloud services, whether they are SaaS-, PaaS- or IaaS-based.

An example of this would be enabling controlled access to cloud services by leveraging the established user identity, authentication and provisioning processes of their on-premise applications. In this instance, access to cloud services can be managed as part of existing security systems and processes, thus satisfying relevant security and compliance requirements. The common theme with these examples is that cloud security controls and processes can be implemented by extending existing enterprise systems and processes to the cloud. This approach depends on cloud consumers and providers being able to easily integrate their security systems with one another, normally through standard protocols.

The following illustrates extending IAM services to the cloud through user provisioning and single sign-on (SSO):

Figure A.

Extending enterprise IAM *TO* the cloud



FOR THE CLOUD - Providing security systems for the cloud

If CSPs want to earn the level of trust from potential cloud-consuming organizations required to handle their most sensitive applications and data, they need to have the most effective and up-to-date security controls in place. For example, CSPs must have sufficient control over application and data access for regular and privileged users—as well as adequate control processes for user management, authentication, authorization, logging, reporting, delegated administration and more.

Privileged users in the service provider’s data center are an especially high risk area because they often have complete access to your critical applications and information. Granular access entitlements must be available that ensure that Admins can perform only those actions that they need to based on their role, and only on appropriate systems. In addition, all privileged users must be uniquely identified and not use shared accounts, in order to reduce risk and simplify compliance audits.

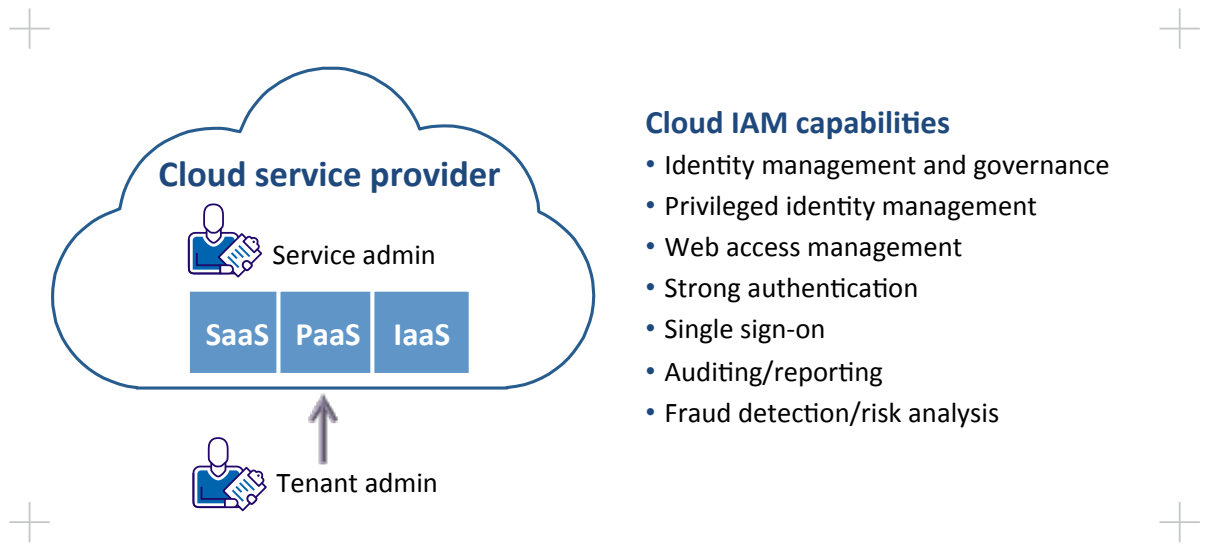
Furthermore, CSPs must be able to prove the existence and operation of these controls to both customers and external auditors in order to establish compliance with relevant policies and regulations. On top of that, CSPs’ security systems and processes must be open and interoperable via standards to the security systems of their cloud-consuming customers.

A robust and comprehensive identity and access management platform is necessary to provide the level of security and automation that this requirement demands. When the CSP has deployed these core IAM capabilities, the security and privacy of clients’ key applications and data is significantly improved, and therefore the compliance profile of the client is also enhanced. The client may live and die by the reputation for security controls that they can establish with their own customer base, so a robust IAM platform in the CSP environment (similar to an on-premise IAM platform) can help enhance that image.

The following highlights the key identity capabilities that cloud service providers will need to help ensure the security of their environments:

Figure B.

Providing security **FOR** the cloud



Cloud IAM capabilities

- Identity management and governance
- Privileged identity management
- Web access management
- Strong authentication
- Single sign-on
- Auditing/reporting
- Fraud detection/risk analysis

FROM THE CLOUD - Delivering security systems from the cloud

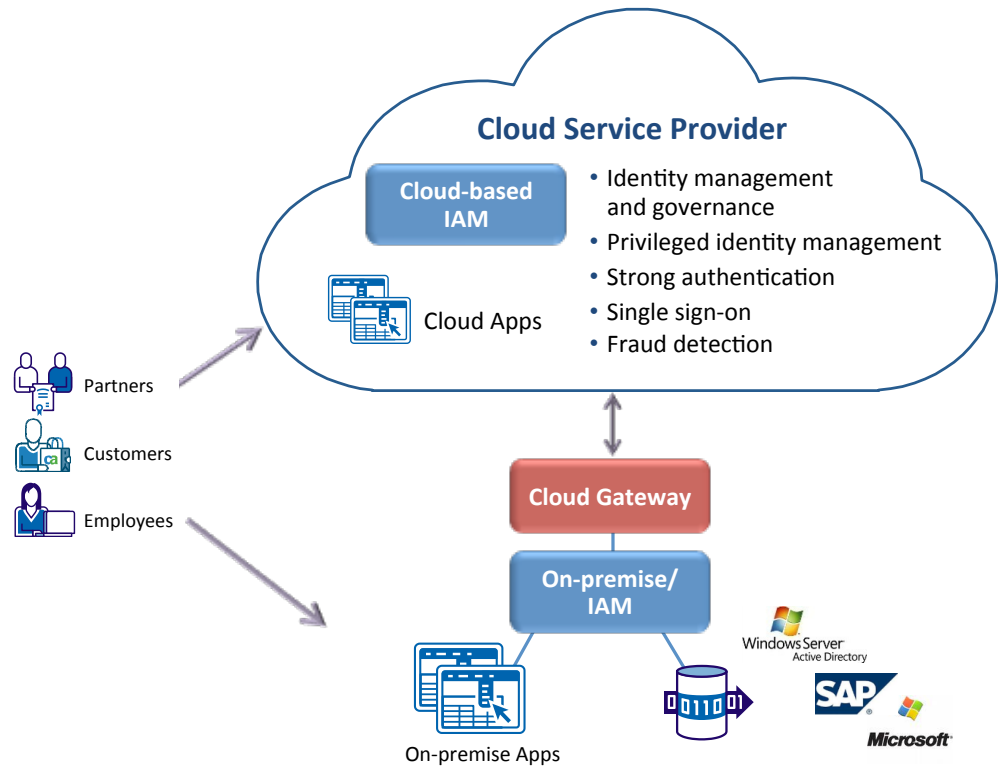
The emergence of the cloud is causing a reevaluation of all aspects of IT service delivery. Over the next couple of years, organizations will be going through their entire portfolio of IT applications, deciding which are core differentiators and value creators, and which are commodities that are better provided by suppliers. Security systems and processes are not immune to this reevaluation. In fact, it could be argued that many organizations are not particularly adept at providing their own security. And while good security is important to earning customer and partner trust, security in and of itself is not always a key business differentiator. Thus, there are many compelling business reasons to look to the cloud for the delivery of security services.

Identity services from the cloud are particularly compelling. They can provide robust security services that can communicate with on-premise IAM services and identity stores, so as to present a unified, consistent set of security services to the application user or administrator. And, by moving various IAM capabilities to the cloud, enterprises can gain the often significant efficiency and agility benefits that a hybrid approach can provide.

The following highlights the importance of cloud-based identity services, and the flexibility and agility that can be achieved by this deployment model:

Figure C.

Providing security **FROM** the cloud



Although the two previous use case examples are important, this deployment model is the one that many organizations will find the most compelling, even though it requires careful planning and a staged implementation. It is also the model that enables an enterprise to take best advantage of the business benefits that use of the cloud provides.

SECTION 3:

CA Technologies strategy for cloud security

We are entering a new world order in IT security, due in large part to the following factors:

- Demand for increased efficiency of IT operations
- Reduced IT budgets
- Increasing need for business agility to respond quickly to market changes
- Increase in the number and type of devices (particularly consumer devices) requiring support
- De-perimeterization (externalization) of the business.

These challenges have caused many IT organizations to increasingly adopt cloud-based software models. But, one major inhibitor of more widespread cloud adoption is concern about the security of applications and information that reside in the cloud. As the business organization pushes for increased adoption to help meet business growth and efficiency goals, IT security and risk organizations are often urging more caution due to the perceived security challenges in adopting cloud models.

Because of these concerns, customers are adopting cloud services in a phased approach in order to limit risk and help ensure success of their cloud initiatives. Over time, they will continue to move more applications to the cloud, possibly including mission critical ones. As identity services become available as a service, they must be able to support the security requirements of both cloud and on-premise applications in order to allow customers to gradually and gracefully adopt cloud models over time. One solution approach will not fit all needs.

In summary, organizations are adopting cloud models gradually and with caution. They need to be able to access comprehensive identity services, running either on-premise or in the cloud, in order to protect applications running either on-premise or in the cloud. Because of their phased deployment requirements, flexibility in their choice of IAM capabilities and in their choice of deployment options are essential.

CA CloudMinder™, is an IAM cloud platform that organizations can utilize for identity services regardless of whether the services, or the applications being protected, are deployed on-premise or in the cloud. Ultimately, enterprises will be able to choose whether their identity components are running on-premise, or in the cloud, or in a hybrid configuration. And, regardless of where it is deployed, this solution can control access to either on-premise or cloud-based applications. These capabilities enable organizations to have very high flexibility in their deployment options, which leads to improved business agility.

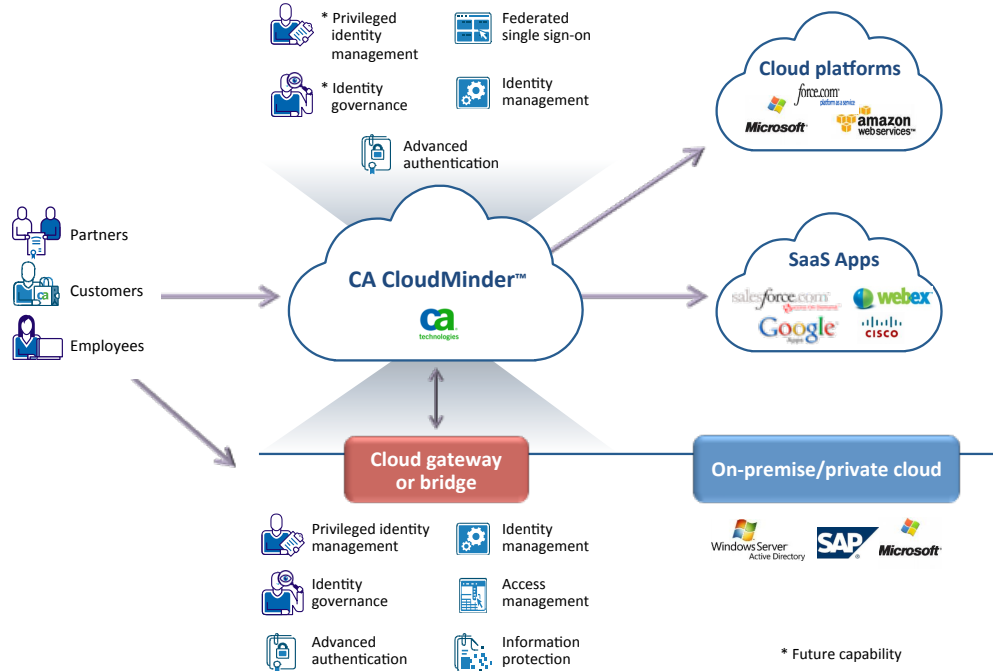
The CA CloudMinder strategy is to offer *very high flexibility* to our customers in terms of the IAM components they can choose, and how they access identity services. They can adopt cloud-based IAM services according to their own needs and timetables. They can start with a completely on-premise solution, and then migrate certain components to the cloud as their needs and security considerations dictate.

CA CloudMinder – an overview

CA CloudMinder is a suite of IAM solutions that are delivered as hosted, cloud services. These services are based on CA Technologies existing portfolio of market-leading IAM security solutions. In addition, the CA CloudMinder service infrastructure is hosted, monitored and supported by CA Technologies 24x7x365. These solutions can operate independently, but also work with on-premise security deployments.

The following illustrates the CA CloudMinder approach, and shows how it enables both access to cloud services from on-premise solutions, or identity services deployed in the cloud.

Figure D.
Providing cloud security



CA CloudMinder will provide the following capabilities as cloud services today or during 2012:

Advanced Authentication

CA CloudMinder™ Advanced Authentication provides a centralized versatile authentication service which consolidates the management of authentication methods across heterogeneous IT environments. This service provides support for a broad range of authentication methods including password, security Q&A, one-time password via SMS/email and OATH tokens. In addition, it offers unique two-factor authentication credentials that are more cost effective and user friendly than traditional methods.

The Advanced Authentication capabilities also include soft tokens that provide greater security over the familiar hard tokens, without all management hassles and expense of continually re-licensing these tokens. Software tokens provide the same user experience as passwords, while providing significantly greater security for user authentications.

In addition to strong authentication, the capability to detect and prevent potential fraudulent activities on the part of users is also important to reducing overall security risk. The risk of online identity fraud continues to grow with attackers often targeting identity credentials and using them to access sensitive systems. CA CloudMinder Advanced Authentication also includes a cloud-based fraud detection and prevention service based on our on-premise solution, **CA RiskMinder™**. This capability provides protection against online fraud by monitoring online access attempts and calculating a risk score based on a broad set of variables. The risk score can then be used to determine whether to allow access or initiate additional action. CA CloudMinder Advanced Authentication thereby provides an effective way to improve the security of user authentication while maintaining a convenient experience for users.

Identity Management

The growth in users, and systems for which they require access, is leading to a growth in digital identities that need to be managed. The management of identities throughout their lifecycle includes multiple aspects including account creation, identity proofing, assignment of access rights, fielding access requests and managing related identity attributes. Organizations require a solution which allows them to centrally aggregate and control identities for use across the IT and cloud environment.

CA CloudMinder™ Identity Management includes three critical capabilities for managing users across on-premise and cloud environments. **User Management** provides cloud-based identity management capabilities including user self-service, profile creation, password reset and distribution of forgotten user names. **Provisioning** automates the process of adding, modifying and deleting user accounts, including user attributes and role associations which can be used to assign privileges on target systems. Provisioning to popular SaaS applications such as Google Apps, Salesforce.com, and others are supported both from CA CloudMinder and from our on-premise provisioning solution, CA IdentityMinder™. **Access Request Management** provides the capability for users to submit access requests online. The cloud service can then route requests through workflow approvals based on defined policies and, where appropriate, provision the user to those systems automatically.

Single Sign-On

Business boundaries are quickly expanding beyond the IT domains directly controlled by your organization as users regularly need to access partner applications or those hosted in the cloud. Many of these sites are secured, requiring proper credentials and authentication, yet users do not want to be burdened with managing separate sets of credentials for disparate applications. The ultimate experience is a seamless single sign-on experience regardless of who actually owns the application.

CA CloudMinder™ Single Sign-On provides cross-domain single sign-on for both identity and service providers, through federation of identities across partner sites. Once users have properly authenticated, their credentials and related attributes will be securely shared to enable authentication to partner sites without requiring user action.

It also provides Just-in-Time (JIT) Provisioning that allows a user who does not have an account on a specific application to have account creation and SSO into that application via a single seamless step. This includes leveraging a user's association to a given group or role to assign them certain privileges on target systems.

CA Cloud Security – looking to the future

CA Technologies is actively and aggressively adding new capabilities to our cloud security offering in order to continue to enable enterprises and service providers to leverage the cloud for their security services. These new capabilities include: additional provisioning connectors to various SaaS services; an enhanced administration model to better manage federations to the cloud; identity certification and attestation to SaaS applications; auditing access to SaaS applications; and improved self-service.

The overall CA Technologies strategy for cloud security is to provide flexibility in how our customers access and deploy identity services, and how they transition from their current environment. To that end, we will continue to offer additional identity services as both on-premise and cloud-based services. These additional cloud services would include, for example, identity and access governance and privileged user management, among others. In this way, we will be able to provide enterprises and managed service providers with very high flexibility in how they deploy critical identity services. The business agility that results from this flexibility can enable you to more effectively leverage the efficiency benefits of cloud services, while also improving your overall security posture.

Section 4: Conclusions

Leveraging enterprise security services from the cloud can deliver many important benefits to your organization, including:

- **Elasticity** The identity services your organization needs can be expanded, or contracted, based on your current needs. In addition, cloud licensing models mean you only pay for what you use.
- **Low Cost of Entry** The cloud-based model can eliminate the need for you to procure hardware, facilities and other costly IT infrastructure that is often needed to support enterprise security solutions.
- **Quick Time-to-Value** The ability to get up and running with cloud-based security applications quickly gives you the business agility you need to effectively respond to changing competitive or market events.
- **Low Cost of Ownership** Ongoing solution support and maintenance is handled by trusted service providers—allowing you to focus your resources on initiatives that differentiate your business. The elasticity provided by this cloud model also allows you to maintain a cost that accurately reflects your usage of the service.
- **Shorter Deployment Cycles** Installation and configuration of the software solution's underlying cloud services has already been taken care of by service providers, meaning you can sign up for and implement services quickly and easily.

CA Technologies has a clear and innovative strategy and vision for providing identity services for the cloud to our customers, based on the CA CloudMinder suite of solutions. CA CloudMinder gives you the flexibility to securely adopt cloud computing on your own schedule, according to your own needs.

We provide on-premise IAM to enable secure access to cloud-based applications and information, cloud-based security services that can protect both your on-premise and cloud applications, and hybrid deployments. We empower you to securely and confidently adopt IAM in the cloud with a choice of capabilities and deployment models.

Section 5: About the author

Sumner Blount has been associated with the development and marketing of software products for over 25 years. He has managed the large computer operating system development group at Digital Equipment and Prime Computer, and managed the Distributed Computing Product Management Group at Digital. More recently, he has held a number of product management positions, including product manager for the CA SiteMinder® product family at Netegrity. He is currently focusing on security and compliance solutions at CA Technologies.

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and distributed, to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 rely on CA Technologies to manage their evolving IT ecosystems. For additional information, visit CA Technologies at ca.com.