identity and access management for the cloud: CA Technologies strategy and vision

J. Tony Goulding
CA Security CSU
Jeff Broberg CA Security CSU, Matthew Gardiner CA Security CSU
table of contents

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

SECTION 2: Security observations and challenges  5

SECTION 3: CA Technologies cloud strategy for identity management  9

SECTION 4: Summary and conclusions  15

SECTION 5: Appendix A  16

SECTION 6: About the author  17
executive summary

Challenge

With all its inherent value, the cloud introduces significant security challenges for both consumers and providers of cloud services in public, private, and hybrid cloud configurations.

A challenge for enterprises is how to leverage existing IAM solutions and extend their reach to the cloud in a hybrid on-premise/off-premise world.

For smaller organizations, the challenge is how to manage users and their access to cloud services without deploying IAM systems on-premise.

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

Opportunity

Current IAM solutions from CA Technologies and our overall vision for IAM can help:

- The enterprise extend its IAM footprint to the cloud
- Cloud service providers secure their cloud infrastructure
- Organizations of all sizes consume IAM services from the cloud

Benefits

Existing IAM solutions from CA Technologies offer consumers and providers of cloud services a proven solution to protect critical IT assets within public, private, and hybrid clouds today.

In concert with our vision and strategy for IAM in the cloud, CA Technologies offers organizations of all sizes the following important benefits:

- Reduced security risk through improved controls
- Eased regulatory compliance through transparency
- Reduced administrative expenses and improved efficiency
- Improved IT agility through automated security processes
Section 1:
Embrace the cloud in a managed and secure fashion

Introduction
CA Technologies has long been a leading force in the identity and access (IAM) 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 could throw at us.

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.

The cloud is a disruptive, business-driven IT phenomenon created in response to the economic realities and mounting pressures to reduce costs and increase efficiency and agility with computing. It introduces new (yet familiar) models for consumption and delivery of applications that have a democratizing effect: applications and other IT services that were once only available to companies with deep pockets and large IT shops are now accessible to all...and for seemingly much less cost.

While the cloud addresses many problems, however, it also brings up many new ones.

As a visionary in the area of IT and IT management, CA Technologies has spent years anticipating these new dynamics. We have been carefully shaping our product strategy accordingly and continue to execute on it. As an IAM market leader, we are helping drive industry activity that will establish standards and best practices to instill user and enterprise trust.

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 share our experiences and understanding of the challenges, and to provide the reader with an overview of the CA Technologies strategy and vision for Identity and Access Management for the cloud.

Target audience
Traditionally, IAM challenges and the products that address them have been focused on large enterprises and governments that contain large, dedicated IT infrastructures and lots of applications and users. For many years now, these organizations have recognized the challenges of giving and controlling users access to applications in large, heterogeneous environments. However, with the cloud, the audience that needs to seriously consider IAM expands to other communities, including smaller organizations, cloud service providers, and government entities.

Small organizations now face IAM challenges too as they move from the homogeneous Microsoft Active-Directory-centric identity world that they currently inhabit to one where their IT services will come from a varied and heterogeneous world of the cloud.
Cloud service providers are also trying to take advantage of the move to the cloud to deliver identity-based and enabled services externally and internally to secure virtualized and multi-tenant systems.

Around the world, governments are providing citizen identity cards, which work equally well online as in the physical world. Identity plays a big part in that too.

Organizations (large and small), cloud service providers, and governments are thus the target audiences of this paper. Each type of organization is asking questions related to identity and the cloud, for:

- **Large organizations** How to extend their existing IAM systems to manage users and their access to cloud-based applications and services.

- **Smaller organizations** How to leverage a multitude of cloud services without encumbering your users and losing control of your organization.

- **Cloud service providers** How to provide your customers with the visibility and control they require to enhance their trust in your cloud services.

Please note that this paper is not intended as a general primer for IAM (authentication, authorization, SSO, etc.) or cloud concepts. Such introductory concepts are best pulled from other sources.

---

**Section 2:**

**Security observations and challenges**

In this section, we outline a few of the bigger issues that have acted as catalysts for our IAM cloud strategy.

The Ponemon Institute reports: “IT practitioners lack confidence in their organizations’ ability to secure data and applications deployed in cloud computing environments (especially public clouds).”

Like the majority of large enterprises, CA Technologies is a consumer of cloud services. As a consumer, our experience is consistent with what we hear from our customers, analysts, and the press—security, trust, compliance, and transparency are top concerns. How much of these concerns are perception vs. reality is a matter for debate. What we do know is that development and adoption of the cloud is outpacing the security systems and processes that are needed to secure it. In addition, cloud consumer visibility into cloud service provider infrastructure is limited; thus it is currently the worst of worlds, control and visibility are both severely limited. This is not a situation which leads to more trustworthy computing.

For some, these concerns represent substantial barriers to cloud adoption. For others, they represent potential risks as they forge ahead anyway, driven by the demands of the business. As CA Technologies dug deeper into the security concerns of the cloud we asked a fundamental question:
Is IAM equally central for cloud security as it has been for the enterprise?

The answer is yes. Well-developed IAM areas such as automated user account on- and off-boarding, user self-service, strong authentication, access control, single sign-on, segregation of duties, data protection, privileged user management, data loss prevention, and compliance reporting are all extremely relevant to the cloud as well.

For those of you who have worked with traditional on-premise IAM solutions, these areas will be very familiar. One fundamental conclusion to draw, then, is that:

In the cloud we are not dealing with an IAM revolution, but an evolution. Although the cloud introduces a new set of usage scenarios, the business problems are familiar.

Closely tied to this observation is the question of whether existing IAM products can still play a critical security management role as the enterprise reaches out to the cloud. For large enterprises with a significant investment in on-premise IAM, this is a particularly burning issue. The fact is that business-critical applications are still (and will be for some time) hosted on-premise. IT still needs to manage user access to them. Enterprise directories and HR systems are still acting as sources of record for enterprise identities. Compliance and cost reduction is still driving enterprises to automate internal IAM processes. Users are still looking for automated sign-on to internal applications. External users still need access to enterprise applications.

Thus, the cloud doesn't devalue or negate on-premise IAM; it introduces new dynamics that lead us to look more holistically at the challenges across the hybrid cloud/enterprise landscape. Our conclusion at CA Technologies is that:

Existing IAM technology is extremely relevant going forward. It will play a critical role for the enterprise as it reaches out to the cloud to build and deploy applications.

According to the Ponemon Institute: “IT practitioners in both the US and EMEA admit they do not have complete knowledge of all the cloud computing resources deployed within their organizations today. This occurs because cloud computing deployment decisions are often made by end users without conducting a thorough review for security.”
It is imperative that IT organizations in general, and IT security departments in particular, take the lead in addressing cloud security issues for their organizations, or they risk being bypassed by the business owners, to the detriment of both the enterprise and the IT organization.

A huge challenge for enterprises when moving to the cloud is loss of control. Security best practices and compliance mandates require you to implement security controls. You can't do this traditionally without access to the applications and systems.

Traditionally, you have that access (Figure A); in a dedicated IT infrastructure, you have physical charge. In the cloud, however, not only do you lose some (if not all) access, but you may have no clue where any of the actual systems physically reside.
The cloud can be very opaque, giving you little or no real visibility into how and where that service is deployed, or how it is controlled, or who is getting access to it. The cloud service may very well consist of a “mashup” of many services from multiple vendors, physically hosted in separate data centers in different geographies. This decoupled model significantly impacts the customers’ ability to implement their own controls and even have visibility over the controls implemented by the cloud provider.

How, then, as cloud consumers, can we satisfy ourselves that the cloud service providers are doing the right thing and implementing sufficient and effective security controls? How can enterprises be in a position where they can not only trust but verify? Unfortunately, there is no silver lining to that cloud (yet\(^1\)). Cloud service providers are not currently held accountable to any cloud-specific security standards or regulations, and so, they’re pretty much left to their own devices and what the market demands of them.
Another huge issue, then, is insufficient visibility into cloud services to allow cloud consumers to quantify risk and make informed decisions on risk tolerance.

For both the consumers and providers of cloud services, all these concerns translate to the following kinds of real-world questions:

- “How do I manage my users’ SaaS accounts and their access?”
- “How do I collect and analyze SaaS security logs?”
- “How do I define and enforce access policies in PaaS applications without creating more security silos?”
- “How do I control privileged users in IaaS—both theirs and ours?”
- “How do I satisfy my auditors that my applications and data are secure?”

Sound familiar? They should as they are the same basic questions organizations have been asking about their traditional on-premise applications for a long time.

Section 3:
CA Technologies cloud strategy for identity management

In this section, we will review how CA Technologies can help enterprises and cloud service providers both today and, with our vision for IAM, in the future.

One of the biggest enhancements to our IAM strategy is in the target customer. As was mentioned in the Target Audience section, the CA Technologies IAM focus has expanded beyond the large enterprise to now include smaller organizations cloud service providers. Each of these communities has different business goals and needs, thus we had organizations “and” cloud service providers to look closely at each one and how they leverage the cloud.

To better get our minds around the challenges, we worked with analysts and customers to explore various use case scenarios and split them into three broad IAM/cloud categories:

- Extending the enterprise up to the cloud (IAM up to the cloud)
- IAM to secure cloud service providers (IAM inside the cloud)
Cloud Security Solutions from CA Technologies

**What it is** This model sees enterprises migrating applications and data off-premise to the cloud, whether standing them up themselves for dedicated use in a cloud such as Amazon EC2 or subscribing to public cloud SaaS services such as Salesforce.com.

**Key challenges** Enterprises will find themselves in a hybrid (mixed on-premise and cloud) state for a long time (it may be that some critical applications will never make their way to the cloud), with some business applications on-premise and some off-premise.

Some of the biggest challenges come with needing to manage new silos of identities, automating user on- and off-boarding to cloud services, extending SSO to the new SaaS services, and the lack of visibility into the layers of the cloud stack for auditing and reporting purposes.

**How CA Technologies can help today** Our existing IAM product suite is highly relevant in this model. User identities and roles, authentication, access control, federated SSO, data loss prevention, and web services security can all be managed with the existing IAM products. For example, CA Federation Manager can be used to federate users to Salesforce.com, Google Apps, and any other cloud service that supports SAML. CA Identity Manager can be used to onboard users through multiple options (e.g., SPML, custom connector, web services).
Strategic areas of focus Capabilities that allow the enterprise to manage privileged user access to SaaS applications and provide session recording; additional provisioning connectors to common SaaS services; just-in-time provisioning during user federated SSO; an enhanced administration model to better manage federations to the cloud, identity certification and attestation to SaaS applications; auditing access to SaaS applications.

Per the Ponemon Institute: “IT practitioners believe the security risks most difficult to curtail in the cloud computing environment include...restricting privileged user access to sensitive data.”

What it is In this model, a cloud provider can be a third-party offering public cloud services or an enterprise providing and managing its own private cloud. So, like any other organization, public cloud service providers need to secure and manage users and the resources they access.

The private cloud is typically an evolution of a dedicated IT infrastructure, and thus is still dedicated to a single tenant—the enterprise. The public cloud serves multiple tenants, and so, there is a greater emphasis on virtualization security and segregating discrete communities of users (customers, IT operations, and administrative staff) to preserve and protect such things as user and data privacy, intellectual property, sales forecasts, and financial and health records.

Key challenges Cloud providers are concerned about managing their evolving virtualized environment, their extensive user community, and users gaining access to the cloud infrastructure and customer...
data. Back-door access (legitimate or fraudulent) can expose development environments, production, storage, databases, management, and reporting subsystems as well as physical infrastructure components such as routers and firewalls to compromise.

As customers and industry groups demand greater security controls, public cloud services providers will be challenged with securing their cloud infrastructure more comprehensively and transparently.

Also, for the enterprise, when data migrates to a public cloud, IT must take steps to satisfy itself that the security controls in place are sufficient based on the value of the data. For high-value data, IT should confirm that the cloud service provider has implemented security controls that are at least as strong as the enterprise’s. The provider needs to be more transparent, making security reports available to consumers in an ongoing fashion to satisfy this requirement.

How CA Technologies can help today As in the prior model, our existing IAM product solutions are highly relevant to both public and private cloud providers. The kinds of IAM controls that make the most immediate sense for securing the cloud include identity federation, log management, advanced authentication, user management, web access management, and provisioning.

In addition, CA Access Control, with its Privileged User Management capabilities, is of particular relevance to harden and secure physical and virtual operating systems and provide suitable change control around privileged user passwords. The latter goes a long way to help instill trust for consumers by preventing cloud operator and admin abuse of superuser accounts.

Strategic areas of focus CA Technologies is enhancing its products to provide the cloud service provider with identity and access management capabilities better suited to managing a large, hierarchical, multi-tenant cloud system. Some of the more general capabilities include a tenant portal to provide visibility and transparency of the cloud service provider infrastructure (e.g., who is logging into my virtual machines), smart deployment of control and logging capabilities, auto-discovery (e.g., of virtual machines), extended policy management to manage virtual machine objects, and support for compliance requirements such as SAS-70 and OWASP.

Similarly, we plan future enhancements to CA Access Control in the areas of controlling Active Directory authentication, controlling access to the virtualization console, fine-grained access control to files in the virtual machine, controlling access to hypervisor management commands, and controlling network segmentation.
In order to execute on this, CA Technologies envisions an Identity Intelligence dashboard that will enable much greater visibility and control of identities, access, and information. It will enable more effective identity governance, enhanced control, and automation.

This is enabled through our unique Content-Aware IAM capability, that enables us to mine more deeply into these transactions, classify the data, and use the resulting knowledge to make more intelligent decisions such as the ability to dynamically adjust policies.
What it is This model puts discrete IAM services in the cloud for on-demand consumption...essentially becoming IAM SaaS services. It is clear that this model, more than the others, opens the door for a new breed of services that help democratize IAM, making it a function that every organization (large and small) can consume.

Key challenges This model can offer a host of IAM services that parallel those developed for on-premise IAM. However, not all IAM services will be ideal candidates for SaaS. Time will tell what customers demand as the cloud continues to evolve.

While we can expect some IAM SaaS services to operate with autonomy in the cloud, others will need to integrate with enterprise systems on-premise. Thus, effectively supporting the enterprise hybrid model will be a key need. For example, on- and off-boarding users into their on-premise applications; pulling security events from the enterprise into the cloud for reporting; synchronizing identities between commercial SaaS services and a corporate directory on-premise; and integrating IAM business processes between on-premise IAM and cloud-based IAM. Many of these are technical challenges; however, other challenges exist, such as the need for an effective and widely adopted open standard for user provisioning across domains.

How CA Technologies can help today Cloud service providers and ISVs are starting to look for a mature and broad IAM foundation upon which to build discrete IAM SaaS services or to mashup IAM services with other services. Having breadth and flexibility will enable them to be creative in bringing to market new and exciting offerings for users and their organization, some being geared towards specific verticals such as healthcare or financial service, to give but two examples.
CA Technologies today provides an advanced authentication identity service from the cloud. This service is a versatile authentication service that can quickly and easily upgrade the security of any authentication process. It offers a variety of authentication methods that protect your users while accessing Web portals, VPNs, or shopping online. Organizations can choose the authentication methods, such as certificate based, OTP, or smartphone-based that best fits the risk profile and user requirements.

Again, time will tell how the market evolves, but the kinds of services that make good sense for delivery from the cloud will likely include, federation, SSO, identity proofing, and user management and directory services. Existing from CA Technologies—CA SiteMinder, CA Identity Manager, CA Federation Manager, are ideal foundations for these services.

**Strategic areas of focus** CA Technologies is working very closely with organizations to better understand the dynamics and anticipate future IAM SaaS needs. Some areas of initial focus will be to enhance user and administrative GUIs for self-service and ease of use, improve multi-tenancy, and develop some new services to better support trust in the cloud.

Aside from the technology needed for this strategy, CA Technologies recognizes that we can’t do all this alone. We are working closely with cloud providers who specialize in specific IAM-related capabilities and with service providers who are critical for service delivery and access to new market segments. It is only through strong partnerships with flagship providers that CA Technologies can deliver on the promise of trust and security in and from the cloud.

---

**Section 4:**

**Summary and conclusions**

The cloud presents organizations and service providers alike with tremendous value and opportunity. When one considers the loss of control that is inherent in the move to the cloud, questioning security readiness is entirely reasonable.

As a component of our corporate Cloud Connected Enterprise strategy, CA Technologies is tackling these issues through a combination of enhancements to existing IAM products, development of new IAM services, partnerships with cloud providers, and driving best practices and standards in the industry.

The foundations of all three models (*IAM up to the Cloud, IAM inside the Cloud, IAM down from the Cloud*) are available today, and CA Technologies will continue to be aggressive in executing on its roadmap to deliver IAM products and services to the public, private, and hybrid cloud communities.

**CA Technologies advantage**

Unlike other security products that only provide partial solutions and are not proven at scale, the CA Technologies cloud security solution provides an end-to-end system for managing identities and their access to information and applications TO THE CLOUD, INSIDE THE CLOUD, and FROM THE CLOUD. The CA Technologies solution is used in some of the largest web and cloud deployments in existence.
Cloud Computing Can be defined as “a style of computing where massively scalable IT-related capabilities are provided ‘as a service’ using Internet technologies to multiple external customers.” Think resources on demand, when you need them, paying for only what you consume.

SPI In an attempt to make more sense of the cloud from an architectural perspective, the terms “Software-as-a-Service,” “Platform-as-a-Service,” and “Infrastructure-as-a-Service” (or SPI for short) are finding their way into common vernacular. Many cloud providers are now using these terms to market their offerings in a way that cloud consumers can better understand.

Software-as-a-Service (SaaS) In which the applications are accessible from various client devices through a thin client interface such as a web browser.

Platform-as-a-Service (PaaS) In which end users develop or deploy applications on top of cloud infrastructure.

Infrastructure-as-a-Service (IaaS) In which the provider manages the hardware, but allows the end user to manage the operating systems, storage, and/or application deployment.
Mashup A web service that uses or combines data or functionality from two or many more external sources to create a new service.

Private Cloud A closed cloud infrastructure purely for the use of an organization. It could be on-premise or off-premise, managed by the organization or outsourced to a third party. Note that many large organizations have been building private clouds with shared infrastructure and services (including IAM) for years as a natural organic evolution of their siloed IT infrastructure.

Community Cloud A closed “community of interest” cloud infrastructure shared by several organizations with common concerns such as business partnerships, industry consortia, or mission. It could be on-premise or off-premise, managed by the organization or outsourced to a third party.

Public Cloud An open cloud infrastructure generally available to the public, owned and operated by an organization selling cloud services.

Hybrid Cloud A composite of multiple clouds (e.g., private + public). Each cloud retains its own unique characteristics and functions but they are integrated to enable sharing of applications and data (e.g., cloud bursting).

Cloud Bursting For example, an application defaults to using on-premise data storage but in times of high demand is able to leverage incremental storage, on demand, from cloud-based storage services.

OWASP The Open Web Application Security Project. This is an open-source application security project.

Cloud Security Alliance A nonprofit organization formed to promote the use of best practices for providing security assurance within Cloud Computing and education on the uses of Cloud Computing to help secure all other forms of computing.

Section 6:
About the author

Tony Goulding is a Senior Director working in the security business unit at CA Technologies Inc. With over 25 years in the computer industry and over 15 years in the security field, he has touched many facets of the business, including consulting, professional services, strategy, sales, and product management. He has chaired and participated in expert panels and presented on a wide range of IAM topics at trade shows and industry events internationally such as Interop, RSA Conference, ISSA, and ISACA. He is a member of the Cloud Security Alliance and the OASIS ID Cloud Technical Committee. Tony has a B.Sc. (HONS) from the University of Keele, England.
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.

1. The Security of Cloud Computing Users—The Ponemon Institute, April 2010
2. Organizations such as the Cloud Security Alliance are stepping up to “promote the use of best practices for providing security assurance within cloud computing.”
3. “Security technologies respondents see as most important for securing the cloud” from “Security of Cloud Computing Users” by the Ponemon Institute, May 2010
4. Definition per Gartner
5. Definition per NIST