

**SOLUTION BRIEF**

CA's Solution for Cloud Security

# how can I secure my cloud services?

we can





**CA Identity and Access Management solutions enable you to control users' identities, their access, and their information usage within both private and public IT clouds. This helps to accelerate the adoption of your cloud services by increasing your cloud consumers' visibility and trust, while reducing your cost of security administration.**



# executive summary

---

## Challenge

How to provide sufficient security for cloud services? When one considers the loss of control that is inherent in the move to the cloud, questioning security readiness is entirely reasonable. It is imperative that IT organizations take the lead in providing sufficient security processes for their organizations or they risk being bypassed by the business owners, to the detriment of all.

---

## Solution

The CA security solution helps private and public cloud providers:

- Control identities
  - Control access
  - Control information
- 

## Benefits

The CA security solution provides a proven solution for protecting your critical IT assets within your private or public cloud service, delivering these 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
- 

## CA advantage

Unlike other security products that only provide partial solutions and are not proven at scale, the CA cloud security solution provides an end-to-end system for managing users' identities and their access to information and applications that is used in some of the largest web and cloud deployments in existence.

## Section 1: Challenge

### **How to provide security for private and public clouds?**

The move of IT to the cloud appears to be inevitable. While the exact role the cloud will take—what applications, services, and data will/won't move there—isn't yet known, the explosion of creativity around and within the cloud harkens back to the early days of the web. The question today for the cloud, as it was then for the web, is “what form will it take,” not “will it happen.” Reacting to the inevitability of the cloud, security professionals are asking today, as they were then, how will sufficient security controls be created and managed given this new approach to building and deploying applications?

How to provide sufficient security is the question that nearly everyone is asking. When one considers the loss of control that is inherent in the move to the cloud, questioning system security is entirely reasonable. Cloud survey results consistently show that the #1 inhibitor to wider cloud adoption is security—closely followed by uncertainty over other complex IT issues such as availability, performance, and interoperability. These issues aren't new, they just need to be reconsidered and evaluated in the cloud context. It is imperative that IT organizations in general, and IT security departments in particular, take the lead in addressing these issues for their organizations, or they risk being bypassed by the business owners, to the detriment of both the enterprise and the IT organization.

### **Private vs. public clouds**

Enterprises have been building what are now thought of as private clouds for many years. The trend toward shared centralized data centers, common hardware and software platforms, and other shared IT services such as the helpdesk, security, and performance management, is a long-standing one. For example, many mature IT security organizations positioned their identity and security services as being shared enterprise security services, well before the term “private cloud” was invented and in common usage. The more recent trend toward the use of virtualization platforms is best thought of as the continuation and technical acceleration of this cloud trend.

Of course, conceptually what can be centralized and shared at enterprise scale privately can be further centralized and shared publicly. This is also a long-standing trend in the computing industry. This fact has given rise to a marketplace for public IT cloud services that are available for purchase by both consumers and enterprises. These services are best further categorized in what is commonly known as SPI—SaaS, PaaS, and IaaS—Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service.

While the trend to cloud computing appears to be unleashing a wave of investment and creativity, as already discussed, it is also raising many complex issues that must be addressed for cloud services to reach their full potential. Specific to security and identity, organizations need to have confidence and proof that their applications, services, and data are being secured appropriately.

Sound identity and access management (IAM) practices within the cloud, both private and public, provides the foundation for effective security by controlling that all users have only the appropriate level of access rights to all protected resources, and that those rights are enforced appropriately. It helps lower administration costs by automating many system administration functions, as well as the provisioning and deprovisioning of accounts and access rights. IAM also enhances regulatory

compliance by automating your security controls, and helping to simplify your compliance audits. Finally, it can enable business growth and help you solidify your relationship with your cloud consumers.

The key questions that must be answered by any identity and access management solution are:

- Who has access to what?
- What can they do with that access?
- What can they do with the information they obtained?
- What did they do?

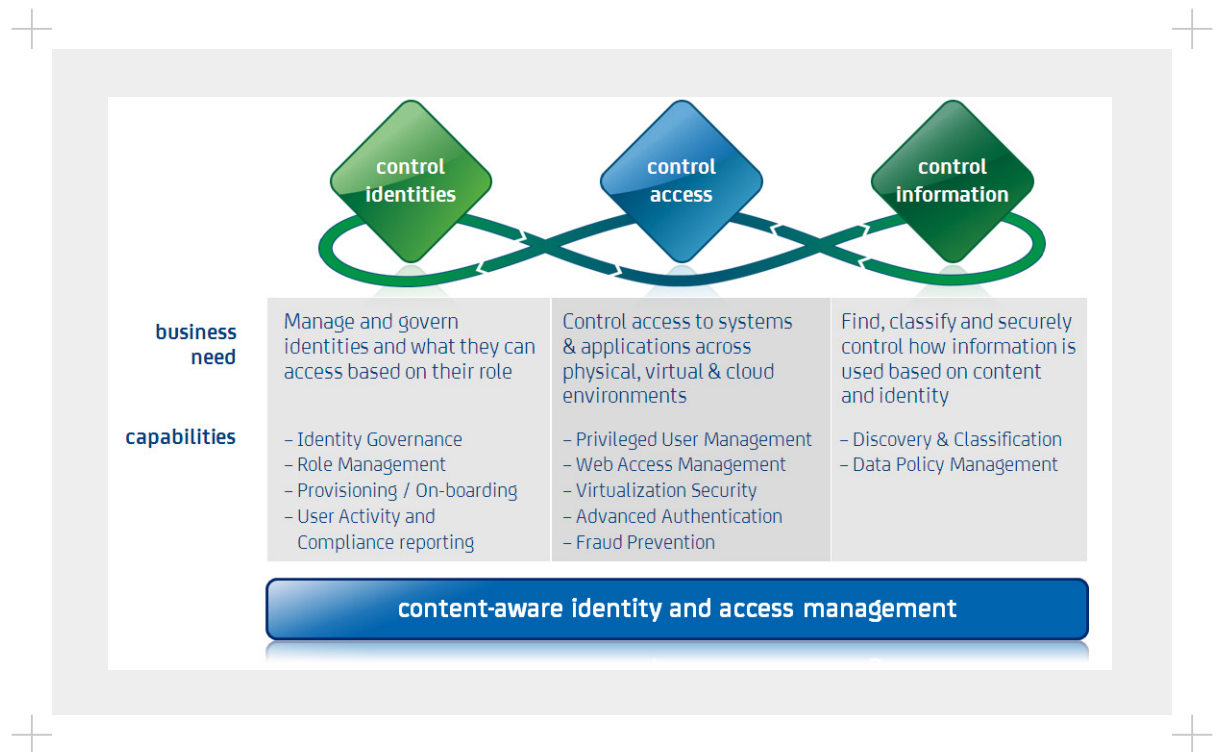
By answering these questions, you can identify and remediate inappropriate access rights, as well as control that your cloud-based IT assets are appropriately protected.

## Section 2: Solution

### Control identities, access, and information in private and public clouds

There are three key issues that need to be addressed when planning a strategy for identity management in the cloud, as represented in the following graphic:

**Figure A**  
Control identities, access, and information in the cloud



To provide effective security, you must:

- **Control identities** Manage users' identities and their roles, provision users for access to resources, enhance compliance with identity and access policies, and monitor user and compliance activity.
- **Control access** Enforce policies relating to access to web applications, systems, system services, and key information. Also, provide for the management of privileged users to avoid improper actions.
- **Control information** Discover, classify, and prevent leakage of confidential corporate and customer information.

These three elements are essential for a comprehensive approach to IAM security in the cloud, whether private or public. Unfortunately, most IAM vendors provide some elements of only the first two categories—but they don't enable you to provide control down to the data level. CA provides the solution for all of these critical areas.

### Control identities

Cloud service providers, both private and public, struggle to keep up with the explosion in the number of users of various types from multiple organizations and the complexity of managing access rights for all these users, as well as with the need to prove to auditors that each user has only the appropriate level of access. Unfortunately, many approaches to these problems amount to poorly coordinated manual processes that expose providers to higher costs and risks. Poor management of user identities also negatively impacts users, as inefficient processes reduce user satisfaction and productivity.

To eliminate these inefficiencies, the entire identity lifecycle of users needs to be automated. Through capabilities such as automated provisioning and workflow processes, cloud providers can gain significant efficiencies, because users become more productive and administrators are freed up to focus more on activities that will meet the needs of the organization.

CA provides a robust and integrated approach to identity lifecycle management. The CA solution includes capabilities for identity governance, role management and mining, and user provisioning. This end-to-end approach includes the initial creation of users' identities, the allocation of accounts and access entitlements that they require, the ongoing modification of these entitlements as the users' roles change, and the timely removal of these rights and accounts upon user termination.

Another key problem in managing users relates to user activity and compliance reporting. Many organizations are drowning under excessive amounts of system log information. Manual processing of this information not only wastes huge amounts of time, but hinders effective identification of significant security events. In addition, many regulations have requirements for collection, storage, and reviewing of system log data that are almost impossible to meet with a purely manual approach. To effectively comply with these requirements, you need to have an automated and repeatable process for identifying and addressing policy and controls violations.

The CA products that enable you to effectively control user identities in private or public clouds include:

- **CA Identity Manager** Provides identity administration, provisioning/deprovisioning, user self-service, and compliance auditing and reporting. It helps you establish consistent identity security policies, simplify compliance, and automate key identity management processes across multiple independent

tenants. Furthermore, it can manage user accounts in both on-premise applications and other cloud services, such as Salesforce.com.

- **CA Role and Compliance Manager** Provides role management and discovery, privilege cleanup, entitlements certification, and compliance reporting. It helps you validate that users have appropriate privileges continuously, while enforcing consistent identity compliance policies across all users and tenants.
- **CA Enterprise Log Manager** Provides log file collection, filtering, correlation, and analysis. It helps you automate the arduous task of user activity analysis so as to reduce costs, and reduce the risk of an undiscovered security event. It also provides comprehensive compliance reporting to streamline audits.

### Control access

Controlling access to critical IT resources is required not only for effective compliance, but also to protect shareholder value, customer information, and intellectual property. Without effective access policy enforcement, improper access (either intentional or inadvertent) can have disastrous effects. There are two important areas to consider across the three categories of cloud services—SaaS, PaaS, and IaaS:

- Controlling access to web-based applications and services
- Controlling access of privileged users to information, applications, and services

### Web access management

Organizations today face two seemingly contradictory imperatives. In order to boost performance and revenues, they must expand their reliance on the Internet and web applications that connect them with their customers, partners, and employees. On the other hand, an organization that opens up its systems to potentially millions of users inside and outside the enterprise also exposes its applications, networks, and data to significant risks, which can jeopardize the whole organization.

CA SiteMinder, the industry-leading web access management product for over ten years, provides an essential foundation for user authentication, single sign-on, authorization, and reporting for both private and public clouds. It enables you to create access policies that can control access to critical applications based on a flexible set of static or dynamic criteria. This flexibility is what makes it easier to control user access to your applications, and helps eliminate the need for security-related code within each application itself. The result is faster application development, and reduced maintenance and administrative costs. CA SiteMinder has been successfully deployed in some of the largest and most complex IT environments in the world. It has been proven to scale to millions of users with high performance and reliability.

Particularly important for IT clouds which must interoperate with other security domains or cloud services, the CA solution also includes capabilities for standards-based identity federation, to enable growth through the expansion of comprehensive partner ecosystems. By allowing partners to securely access your applications, and vice versa, you can streamline value chains, but more importantly take advantage of growth opportunities available through integrated online partnerships. In addition, security for SOA/web services-based architectures is provided so that both web applications and web services can be protected with a common security infrastructure.

The CA products that enable you to effectively control access to private and public cloud-based web applications include:

- **CA SiteMinder®** Provides centralized management and enforcement of user authentication, authorization, single sign-on, and reporting. It enables you to easily secure your key applications, improve your user experience, and simplify your compliance audits.
- **CA Federation Manager** Extends the capabilities of CA SiteMinder to standards-based federated partner relationships, which enables your cloud service to interoperate with applications in other security domains or other cloud services, such as Salesforce.com and Google Applications.
- **CA SOA Security Manager** Protects access to XML-based web services by providing authentication, authorization, and audit services by inspecting the content of XML messages.
- **CA Arcot WebFort and RiskFort** CA Arcot WebFort® Versatile Authentication Server allows you to deploy a wide range of strong authentication methods in an efficient and centralized manner. It can increase security and improve your compliance profile without burdening users or your help desk. CA Arcot WebFort is integrated with CA SiteMinder® to provide a robust set of functionality which includes the management, execution and tracking of multiple authentication methods.

CA Arcot RiskFort™ provides real-time protection against identity theft and online fraud via risk-based, adaptive authentication. It evaluates the fraud potential of online access attempts (including everything from enterprise online services to consumer e-commerce transactions) and calculates the risk score based on a broad set of variables. All of this is done transparently without inconveniencing legitimate, low-risk users.

#### Privileged user management

One of the most important areas of IT risk relates to privileged users (IT and security administrators). This is equally true in both private and public clouds—virtualized or not. Whether inadvertent or malicious, improper actions by privileged IT users can have disastrous effects on IT operations, and on the overall security and privacy of corporate assets and information. Therefore, it is essential that administrators be allowed to perform only those actions that they are authorized for, and only on the appropriate assets. And it is important that these security controls can scale over large physical or virtualized environments.

In addition, administrators often share (and sometimes lose) their system passwords, leading to an even larger risk of policy violations. And, when these users all login as “Root” or “Admin,” their actions, as reported in the log file, are essentially anonymous. These conditions not only pose a significant security risk, but hinder compliance efforts, because improper actions cannot be prevented nor associated with the offending person.

What is needed is very granular access control on administrator users. Unfortunately, native server operating system security does not provide sufficient control over who can access what resources, nor does it provide the granular auditing needed to meet compliance requirements.

The CA solution for privileged user management, CA Access Control, secures both physical and virtual servers by providing more granular entitlements for administrators across platforms than are offered

by operating systems. This facilitates improved compliance through granularity of policy-based access control and enforcement that includes segregation of duties. The solution controls who has access to specific systems, resources on those systems, and critical system services (for example, it is important that administrators not have the ability to turn off the system logging process in order to hide an inappropriate activity). It also simplifies management through a single user interface to manage all your server platforms.

The solution also supports extensive privileged user password management (PUPM), which helps provide the accountability of privileged access through the issuance of passwords on a temporary, one-time-use basis, or as necessary while providing user accountability of their actions through secure auditing. PUPM is also designed to allow applications to programmatically access system passwords and, in so doing, remove hard-coded passwords from scripts.

#### **Control information**

Enforcement of access control over sensitive information is only the first step in providing a comprehensive approach to information security within the cloud. Once users have gained legitimate access to data through an application for which they are authorized, many cloud services have little or no control over what those users can do with it. These organizations often are not fully aware of all the places their sensitive information is stored, and have no protection against this information being exposed or disclosed to unauthorized people, either internally or externally. Something as simple as a social security number can have significant negative impact if disclosed inappropriately. For this reason, many organizations believe that their own employees pose a more serious data security threat, via either inadvertent or malicious behavior, than do outsiders.

CA DLP helps you get control of your massive amount of information and, most importantly, protect sensitive data from inappropriate disclosure or misuse. It protects data-in-motion on the network, data-in-use at the endpoint, and data-at-rest on servers and repositories, whether in private or public clouds. It enables you to define policies that determine which data should be checked, what type of data item should be monitored, and the action to be taken if inappropriate activity is detected. It also includes a collection of pre-built policies based on real business use cases that make quick deployment simpler. It can significantly reduce information security risk, and make it easier to prove compliance with certain security-related regulations and best practices.

---

## Section 3: Benefits

### **Enabling strong, efficient, and flexible security for the cloud**

The CA Identity and Access Management solution provides a proven solution for protecting your critical IT assets within your private or public cloud service, delivering these important benefits:

- **Reduced security risk through improved controls** CA's IAM solution helps ensure that your critical IT resources are protected and that only properly authorized users can access them, and only in approved ways. It also enables you to manage and analyze security event information to quickly

identify and remediate potential security issues, including improper disclosure or use of sensitive organizational or customer information. These enhanced security controls, when combined with centralized and automated reporting capabilities, help to increase cloud consumer trust with your cloud services.

- **Eased regulatory compliance through transparency** CA's IAM solution provides your organization with the tools necessary to support both cloud providers' and cloud consumers' compliance with regulatory mandates. In addition to comprehensive auditing and reporting, your compliance challenges are simplified, because you can regularly provide the proof of controls to your auditors as well as to the auditors of your cloud consumers.
- **Reduced administrative expenses and improved efficiency** CA's IAM solution also can help to automate many of your key IT administrative processes, especially those related to managing user identities and access rights of tenant users. Along with automated filtering and analysis of security log information, these capabilities can bring significant administrative efficiencies, thereby reducing your overall IT costs. They can also help to improve user and management productivity, since less time has to be spent in manual security administration.
- **Improved it agility through effective security processes** Cloud consumers, both internal and external, will only do business with you via your cloud service if they believe that you can provide a secure environment for the personal and proprietary information for which they are responsible. CA's IAM solution can help your cloud service secure its applications, as well as deliver new applications and services more quickly. The CA security solution can help to provide a personalized and more positive user experience, thereby strengthening your customer and partner satisfaction and helping you grow your business and partner ecosystem.

---

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and physical 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](http://ca.com).