Identity and Access Management as a Service (IAMaaS) Across Cloud and On-premise Environments: Best Practices for Maintaining Security and Control
Enterprises Are Leveraging Both On-premise and Off-premise Resources

Most organizations want to leverage the cloud, but also recognize that migrating all their applications all at once is not always practical. In taking a prudent and measured approach, they are seeking ways to utilize cloud-based applications and infrastructure while maintaining certain applications on-premise. The resulting architecture is referred to as a hybrid environment because it features both on-premise and cloud-based resources.

For organizations in this situation, one of their major challenges is providing users with the flexibility to seamlessly move around the environment while still maintaining appropriate security levels—or more specifically, ensuring consistent control and security policy between on-premise applications and cloud services.
The Network Perimeter Is Disappearing

Once organizations simultaneously leverage applications via a variety of IT models, such as on-premise applications and SaaS-based services, the traditional notion of a network perimeter simply no longer exists. And as a result, our ideas about how we manage security and identity have to change.
Identity Is the New Network Perimeter

So, how do we ensure appropriate security levels within this hybrid environment? The key is utilizing a centralized identity and access (IAM) service that provides access to all services no matter where they reside. This approach ensures that all the identity-related functions, such as authentication—and ultimately authorization—are consistently managed by the enterprise. In this new model, identity is the new perimeter and extends to all users: employees, partners, and customers, alike.
Identity Is the New Network Perimeter continued

How does one create such a security utopia? To avoid building separate identity silos solely for cloud-based services (the result of unique accounts within each of those providers and applications), enterprises should look for a centralized IAM service that can manage all users’ access and authentication before they go to any applications—on-premise or in the cloud. For employees, authentication is against a corporate directory. For partners, it could entail using identity federation via standards such as SAML that enable the users of an organization to easily and securely access the data and applications of other organizations as well as cloud services via cloud single sign-on, thus preventing the need to maintain another list of user accounts.
Identity Is the New Network Perimeter  

For customers who may already have an existing digital social identity (such as Facebook or Google) and would like to be able to leverage that identity, standards such as OpenID and OAuth would allow those users to access web-based resources using those credentials and not require additional user registration steps. For special employees or high-value transactions, a higher level of authentication might be required before allowing the user access to a particular service. There might be very sensitive data that goes into an SaaS-based HR application, for example. If the necessary level of required authentication is not native to that particular SaaS environment, the enterprise could require an additional “step-up authentication”—via a centralized identity service—before granting access.
Re-engineering Security Thinking for Today’s Realities

Within a strictly on-premise model, IT focuses on building physical infrastructures—servers, virtualization layers, operating systems, and middleware applications—and delivering security throughout the whole stack.

With a hybrid model, however, IT must change its perspective and style, treating any and all IT components (cloud-based or otherwise) as services that are available for the business to consume. In doing so, IT security needs to ensure consistent protection between and among the organizations and all the instances of applications where sensitive data exists (i.e., the broader and fragmented data center).

At first blush, it might seem that the role of IT security is significantly diminished by this process. The reality, however, is that securely enabling the access to and interaction of cloud services provides much more value to the business. In doing so, IT is enabling an organization to move more quickly. Furthermore, IT is facilitating the adoption of the consumer-oriented IT capabilities that employees are demanding. In other words, utilizing more cloud-based services puts the IT security function front and center in the day to day of a company’s planning activities.
Integrated Identity and Access Management

Understanding and embracing the need for a centralized identity service spanning on-premise and off-premise resources is the first crucial step. But, the next step of assessing how to implement such a solution is equally as important.

CA Secure Cloud was designed to work as a standalone service or in conjunction with on-premise IAM components to support hybrid environments. It supports a variety of use cases, such as requiring customers, employees, and partners to authenticate centrally prior to being provided access to on-premise components or cloud services via federated single sign-on.

As hybrid environments become the norm, the need for solutions that can interoperate in on-premise and cloud environments will be paramount. And, it will be especially attractive to those companies lacking the resources and infrastructure to deploy extensive local security.
Practical Examples of Hybrid IAM Best Practices

The following scenarios illustrate how a centralized, best-practice-based identity service might be implemented by an organization.
Secure Single Sign On (SSO)

This example illustrates SSO for an employee to on-premise and cloud-based applications. With this approach, federated SSO is employed to enable convenient access across application types.

In this scenario, the user:
- Authenticates to the on-premise directory/database
- Launches an intranet website
- Uses SSO to access a cloud-based IAM hub
- Sees a homepage with icons representing available services
- Connects seamlessly with multiple applications and services
Simple Access Request and Approval for New Applications

This example illustrates the simple process for end users to request access to additional applications on their Single Sign-On page.

In this scenario, the user:
- Authenticates to the CA Secure Cloud instance
- Clicks on “My Request” and selects a desired application from a list of available services
- Initiates the back-end workflow request to the administrator to approve access to new services
- Once approved, re-authenticates to CA Secure Cloud and is given SSO to the new service
Basic User Management

Ideal for large user populations, this example illustrates the simple self-service processes for user management including updating profile information or creating a new password.

In this scenario, the user:
- Authenticates to the CA Secure Cloud instance
- Clicks on the “My Profile” icon and makes changes
- Clicks on the “My Password” icon and enters a new password
- Receives an email that the password has been successfully changed
About the Solutions
From CA Technologies

CA Secure Cloud offers cloud security solutions that enable organizations to more efficiently manage the entire identity lifecycle across multiple application types. CA Secure Cloud services enable organizations to centrally control users’ identities and their access to both SaaS services and on-premise applications in a hybrid environment with a common consistent security policy. This helps organizations utilize the cloud with confidence and adopt a best-of-breed approach that relies on existing on-premise applications and SaaS applications, while also helping to reduce the cost of security administration.

These services enable organizations of all types and sizes to realize efficiency gains while still protecting their critical digital resources, regardless of whether those resources 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
- Ability to move to the cloud on a comfortable schedule
For more information, visit ca.com/securecenter.

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.