BUYER’S GUIDE

Buyer’s Guide to Identity as a Service (IDaaS)
Best Practices for Achieving Security, Business Agility and an Engaged Workforce Through IDaaS

The decision to embrace Identity and Access Management as a Service (IDaaS), or cloud-based identity and access management, is a wise choice. IDaaS boosts the digital enterprise’s ability to address governance, employee satisfaction and IT operational efficiency issues, while providing opportunities for enhanced agility and workforce productivity. The right IDaaS choice can cut operational costs, reduce risk and save time. However, choosing the ideal solution calls for careful consideration of several key elements: How deep is the provisioning? How easy is it to delegate? And how effectively does the solution accommodate the hybrid enterprise environment? This guide discusses best practices in selecting the optimal IDaaS solution, and provides guidance for achieving a wealth of business-, security- and workforce-related benefits.

The New World of the Hybrid Enterprise

The move to the cloud, the mobile workforce and the unprecedented increase in application usage have created an undeniable shift that creates both high stakes and huge urgency. Called the hybrid enterprise—on-premises and in-the-cloud data and applications, accessed from anywhere, via any device—it represents a world of constant change, where workloads are shifting to the cloud and applications are adopted and abandoned with ease.

“Enterprises need to focus on managing and leveraging the hybrid combination of on-premises, off-premises, cloud and noncloud architectures.”

—Gartner

According to Gartner, “Unless very small, most enterprises will continue to have an on-premises (or hosted) data center capability. But with most compute power moving to IaaS providers, enterprises and vendors need to focus on managing and leveraging the hybrid combination of on-premises, off-premises, cloud and noncloud architectures, with a focus on managing cloud-delivered capacity efficiently and effectively.”

Complementing on-premises applications with SaaS-based applications is quickly becoming the norm, and the trend is accelerating. However, adopting SaaS significantly increases the threat surface for a potential security breach. One issue is identity sprawl: User identities and credentials are created and stored in each cloud application, rather than being consolidated on the existing identity and authentication systems used for internal applications. This leads to multiple passwords (and poor password practices) for employees, provisioning and deprovisioning difficulties and a lack of full identity lifecycle management. Organizations look to identity and access management (IAM) solutions to control unauthorized use of approved SaaS apps and gain visibility over those not approved. There is rising interest in SaaS-based IAM solutions (IDaaS) to cover security needs for on-premises and SaaS applications.
“By 2020, 40 percent of IAM purchases will use the IDaaS delivery model.”

—Gartner

According to Gartner, by 2020, 40 percent of IAM purchases will use the IDaaS delivery model. But not all IDaaS solutions are created equal, and not all of them adequately handle the hybrid enterprise with its complex interplay of on-premises and SaaS applications. Forrester explains “The interplay of on-premises and cloud SaaS applications is where enterprises can lose data the easiest, thus fueling the need for hybrid IAM solutions.”

The hybrid enterprise enables the workforce to access important apps from anywhere, via multiple access methods. For the enterprise, it’s an opportunity to enable greatly increased productivity and agility, but is built on constant change, with little visibility and control. In this new world, employees and other members of the workforce have come to expect streamlined, native application experiences, intuitive interfaces and constant data availability, as well as on-the-go access. Business is increasingly looking to IDaaS to provide a streamlined, consistent user experience that meets more sophisticated user expectations.

IDaaS for the Hybrid Enterprise

IDaaS solutions have been around for some time, but until recently, primarily focused on federated single sign-on (SSO) to SaaS applications. While federation for SaaS applications is a good first step for improving the user experience, large enterprises demand more mature solutions that can meet their requirements around security and compliance, and handle the complexity challenges of hybrid environments that encompass both legacy on-premises applications as well as new SaaS applications.

IDaaS can play a key role in helping organizations reap the benefits of the hybrid enterprise environment. The right IDaaS solution can lead to the right balance among security, agility and user experience across the hybrid environment. And can provide the workforce with a consumer-grade user experience across on-premises and cloud-based applications: frictionless yet integrated. At the same time, an optimal IDaaS solution empowers the actual owners of the applications (often LOB owners) to move quickly and adopt the applications they need—without waiting for IT. Plus, app owners can easily and securely provide the necessary authentication, access and entitlements.

This can lead to higher organizational effectiveness, accelerated cloud adoption and cost minimization. Security, manageability and control are assured without impeding productivity or incurring additional risk: Service desk work is reduced due to fewer user password reset requests, cloud identity sprawl is controlled and managed, and common security issues such as the reuse of passwords don’t jeopardize the strong security measures already in place.
Top Five Requirements for an Optimal IDaaS Solution

There are some common threads that lead to the optimal balance of security, agility and user experience, while unlocking cost savings and avoiding risk. Look for an IDaaS solution that is:

1. **Hybrid** Provides a true hybrid solution with efficiency and control across on-premises and SaaS-based applications
2. **Agile** Makes your business more agile, speeding up application onboarding, user provisioning and delegating ownership
3. **Secure** Strengthens your overall organizational security, managing accounts throughout their lifecycle
4. **Cost Effective** Reduces your IT costs while delivering quick time-to-value
5. **Consumer-grade** Gives your users a consumer-like experience with SSO to cloud, on-premises and legacy applications from a single launch pad

Let’s look at each of these in depth, show why they’re important and how they can help you achieve your business optimization goals for the hybrid enterprise.

**IDaaS that provides a true hybrid solution**

For years, many large enterprises have been leveraging on-premises IAM systems—with enterprise-grade provisioning capabilities and SSO—and the systems are deeply embedded in the environment. However, when moving rapidly to cloud-based apps, a disconnect occurs. Cloud-based IDaaS systems can sometimes integrate with on-premises systems, but it’s usually at the expense of security or time-to-value. Because many enterprises are not willing or able to rip and replace their on-premises IAM systems with IDaaS, they adopt IDaaS to run alongside their existing on-premises systems. Then the enterprise must deal with two separate systems, one for on-premises apps and another for cloud-based apps. It’s a struggle to deal with user access and administration in two different worlds; admins and users alike are forced to compromise.

**1. IAM for On-Premises and SaaS Applications**

While IDaaS solutions have come a long way in the past three to four years, they generally still lack the broad and deep functionality of an on-premises IAM solution. Many cloud-based IAM solutions offer federated SSO to a broad set of cloud apps and basic provisioning capabilities to only a small subset of the apps. Many on-premises IAM capabilities are not supported with IDaaS, especially for legacy on-premises application integrations. Integration with any on-premises applications, if even possible, often requires difficult customization.
Administrators are left with a dilemma: Do they embrace cloud-based IDaaS, and force users and administrators to deal with on-premises apps separately? Do they engage professional services to integrate IDaaS with on-premises applications? Or do they try to blend together disparate products from different vendors to provide frictionless access to both on-premises and cloud-based apps? In all these cases, TCO and time-to-value dramatically increase and user experience suffers, offsetting the benefits that the organization expects from implementing an IDaaS solution in the first place.

How IDaaS helps

The right IDaaS solution can provide a seamless, consumer-grade interface for users to access all apps, both on-premises and in the cloud. Look carefully at the proposed IDaaS solution to make sure that it doesn’t put all its emphasis on SaaS applications or positions password vaulting as an alternative to more-secure integrations with on-premises applications. Instead, the IDaaS solution should offer the ability to integrate with your on-premises IAM solution to leverage your existing investments and provide rapid time-to-value, without compromising security. The ideal solution provides a true, built-in hybrid approach, with SSO to target SaaS and on-premises applications from a single launch pad. Regardless whether the application is protected by IDaaS or the on-premises IAM systems, the user experience is seamless. This reduces the administrative burden and avoids duplication of effort in managing application access policies. The ideal IDaaS solution lets admins leverage existing on-premises IAM policies and dynamically evaluates policies, no matter where the applications live, to determine who should get access.

For the end user, the right IDaaS solution has an intuitive and dynamic user interface that provides one-click access to all apps that users have access to. As they move around, join groups or leave, the launch pad automatically reflects users’ updated applications and access. This eliminates additional manual steps for administrators to manually update the launch pad, assign entitlements or deal with ad hoc requests once a user is provisioned or changes roles.

2. IDaaS That Increases Business Agility

It’s rare to find an organization whose employees don’t need access to some basic, cloud-based apps, such as Box and Office 365. Other business-specific apps, such as Marketo or Salesforce, have their own requirements for user access that are understood by the department or LOB head but perhaps unknown to the IT team. Some apps must remain on premises and won’t be moved to the cloud anytime soon, if at all. Employee onboarding and access needs to address all these apps—in an ideal world, without extensive technical involvement on the part of IT.

What impedes business agility?

IT is already dealing with limited resources and tight budgets, leading to bottlenecks in application rollout. Meanwhile, the LOBs need to move quickly and often bring up their own applications without the knowledge of IT (Shadow IT). This results in pockets of application knowledge—in effect, silos of information—leaving IT with incomplete knowledge about and control over applications in their environment. The cost of administration grows exponentially, as does the risk of human error.
The time it takes an IT team today to onboard a new employee is measured in hours or days, and is only exacerbated by incomplete information. The burden is no less great for the employee who struggles with a growing number of passwords and login instructions. Many LOB-owned cloud applications are unknown to IT and often not integrated in on-premises IAM systems. Since each cloud application likely maintains its own copy of user identities and credentials, the user is faced with numerous, different methods for accessing needed cloud applications, in addition to their on-premises applications. The more complex the login process, the greater the likelihood that users will resort to unsafe methods such as writing down passwords or using the same credentials for multiple apps.

How IDaaS can increase business agility

Look for an IDaaS solution that enables your team to quickly provision new users with a streamlined approach to setting up and managing accounts as well as the entitlements assigned to those accounts in target systems. This will eliminate tedious, additional manual steps to do initial assignments and handle ad hoc requests once a user is provisioned or changes roles. The IDaaS solution should incorporate business-friendly rules to automate deep provisioning and deprovisioning. Be wary of systems that make provisioning cumbersome, both in onboarding SaaS applications and user provisioning: This will present problems with all deployments, especially large ones.

A further boost to agility comes from the IDaaS solution with an administrative authorization model that enables efficient and safe delegation of application ownership to LOB owners. If the solution is easy to use and doesn’t require in-depth security or IT expertise, LOB owners can onboard their applications and assign access and entitlements based on their deep knowledge of their applications and user needs. This is far superior to the common practice of restricting app owners to granting access by IT-centric group membership, which severely limits owners’ ability to use the IDaaS solution adequately. With the right IDaaS solution, they can establish or edit rules through a business-friendly interface. Avoid solutions that require complex configuration, programming or API understanding: Delegation is difficult, if not impossible.

3. IDaaS That Strengthens Overall Organizational Security

The software attack surface is expanding rapidly as security perimeters dissolve and adoption of cloud-based applications accelerates. IDaaS is an essential tool to protect access and prevent incursions when the environment includes both on-premises and cloud-based applications. Based on a survey conducted by Forrester Consulting, security professionals are concerned about breaches for three primary reasons: financial loss, exposure of sensitive customer or employee information and decreased customer confidence and trust.4

What IAM-related security issues does the enterprise face?

IT and security teams are responsible for knowing that the right users have access to the right apps, and for validating that the access is authorized. This includes assigning the appropriate entitlements within applications based on user roles and attributes. Initial provisioning isn’t the end of the story: When users
move or change roles, their access and entitlements need to change. And when an employee leaves or is terminated, she or he must be deprovisioned in a timely manner.

Many factors can contribute to provisioning and deprovisioning issues: lack of visibility of user accounts, departmental silos and business process inadequacies that leave orphan accounts (allowing former employees to access SaaS apps and confidential data) and notification delays when an employee is terminated. Without a way to automate discovery of all accounts in all apps, the teams won’t even know what they don’t know. Even when orphan accounts are finally discovered, the task of remediation is huge.

Rogue accounts, those imported from the target system but not associated with a person, cause similar security issues. Whether due to a simple mismatch, a duplicate email address or an account created outside the standard IAM process, it’s usually a manual process to try to reconcile such accounts.

How IDaaS can help

An IDaaS solution should allow you to manage user accounts throughout the entire identity lifecycle, not just initial account creation. It shouldn’t depend on manual assignment of group membership but rather automatic assignment of accurate account entitlements based on rules. The solution will incorporate bidirectional integration capabilities, allowing you to find and quickly reconcile and remediate orphan and rogue accounts. Make sure to choose an IDaaS solution that incorporates account reconciliation capabilities, versus one that subjects the security or IT team to tedious, time-consuming and error-prone manual identification and reconciliation based on internal audits and guesswork.

Effective use of IDaaS to reconcile accounts to known identities can result in faster rollout of cloud apps, better control over cloud identity sprawl and a reduced attack surface.

4. A Cost-Effective IDaaS Solution That Delivers Quick Time-To-Value

Businesses have made significant investments in IAM solutions to handle authentication, authorization and access to on-premises applications. But today, with the explosive growth in accessible, easy-to-use SaaS applications, on-premises applications are being outpaced by cloud applications as business users rush to adopt the applications they need. This puts pressure on IT to provide quick access, while controlling and managing cloud identity sprawl. The costs to the organization to maintain control and visibility over all aspects of IAM, and provide quick yet secure access to all applications, quickly escalate.
What contributes to increased IAM costs and slow time-to-value?

With cloud identities and access being managed in silos across the organization, the lack of centralized administration of identity and access management functions can easily escalate administrative costs. In addition, developers may need to build IDaaS integrations with existing on-premises IAM systems. There is a very real chance of increasing the administrative burden in managing application access policies, especially when the solution does not leverage policies already in place. And there are administrative costs when user accounts are not fully provisioned. Some IDaaS solutions create a “shell” account without completing the assignment of account entitlements, which will require additional administrative effort. Once implemented, some solutions require IT involvement or costly programming each time a new app is added to the environment. Not only is this costly but it impedes business agility and delays time-to-value.

Rogue and orphan accounts in SaaS applications can contribute to escalating costs, since money is wasted on unused or unneeded subscriptions. One of the biggest cost factors is increased help desk costs for password resets. With a multitude of apps, employees find it difficult to remember all the passwords and login procedures, leading to an increasing number of requests for password resets. And the sheer cost of provisioning and deprovisioning users can quickly add up. For the business as a whole, failing to control the hybrid environment early on can result in increased administrative burden and escalating hidden costs.

The right IDaaS solution reduces costs and brings value quickly.

Look for an IDaaS architecture that can easily integrate with your existing identity management infrastructure. By leveraging existing products, practices and policies, the organization minimizes administrative effort and sees quick time-to-value without extensive engineering and integration requirements. This is especially important for organizations that have well-established SSO solutions in place for on-premises applications. Ideally, IDaaS will integrate quickly and smoothly with those solutions, leveraging them to provide a single, unified interface to users.

The right solution will also make it easy and quick to provision and deprovision users across multiple applications, and keep access rights synchronized when employees move from one department or role to another. The best IDaaS solution will enable automated provisioning with entitlement assignment, further reducing the administrative burden. As noted above, this will also contribute to greater business agility because IT is freed up to innovate and accelerate the business, rather than being burdened with tedious provisioning work.

Make sure the IDaaS solution provides user self-service for password resets and changes, to dramatically reduce the cost and burden of involving IT help desk in password resets. This can lead to stronger user adoption, fewer bypassed controls and reduced risk. In many cases, the ROI offered by self-service password resets can be a driving factor in justifying the cost of the IDaaS solution. IDaaS solutions should minimize the number of passwords users need to remember and enable self-service password reset.

Another area where the right IDaaS solution can contribute to cost savings is by reducing the overall cost of SaaS subscriptions. Many SaaS providers charge based on the number of accounts. If your IDaaS solution can detect and remediate orphan accounts, you can reduce SaaS subscription costs, which can represent significant savings.
5. IDaaS That Provides a Consumer-Grade User Experience for All Applications, Not Just SaaS Apps

You need to provide secure access to apps for your employees, but they struggle with a growing number of passwords and login instructions. As the number of apps grows, it’s increasingly harder for employees to access cloud-based systems and apps, as well as the legacy and on-premises apps they need to do their work. When there are separate ways for them to log into and access on-premises and legacy systems, it takes more time to log in, there’s more to remember and the chance of writing down passwords and creating other security issues increases. Each application access experience, from new-hire enablement to role transitions to simple, everyday application sign-on, should be as frictionless and intuitive as possible. And users’ expectations will rise as they become more accustomed to easy-to-use, consumer-style applications with highly intuitive interfaces.

For the IT or security team, the experience can be equally frustrating, as cloud-based launch pads do not incorporate on-premises apps, must be cobbled together with limited functionality or require developers to build, manage and update. Often, the requirement to use different vendors increases cost, complexity and time-to-value.

How IDaaS helps

The optimal IDaaS solution provides a true, hybrid launch pad that incorporates both on-premises and SaaS-based applications in one, single interface, regardless of where the application lives. The solution leverages the policies and entitlements already in place through integration with on-premises IAM, and provides a consumer-grade workforce experience for SSO across cloud and on-premises apps. The launch pad dynamically populates apps based on identities, policies and rich attributes, eliminating the need for developers to manually build and manage an integrated, hybrid user launch pad.

In addition, two-factor authentication in the IDaaS solution can supplement strong password login to the launch pad, increasing overall security. The ideal solution, of course, incorporates self-service password management and forgotten password recovery. In short, IDaaS can provide a personalized service, a consistent experience, on-demand access and rapid time-to-value.
The Right IDaaS Solution Nets Big Benefits

These common threads—agility, security, hybrid solution, cost reduction and consumer-like experience—lead to the optimal balance of security, agility and user experience, while saving costs and reducing risk.

- The business-related benefits of selecting the right IDaaS include a boost to organizational effectiveness, accelerated cloud adoption, maximum cost reduction, empowering the LOBs and reducing the IT burden, all of which can accelerate innovation and allow the team to focus on areas where their skills are really needed.

- The security-related benefits include reduced risk, accelerated employee adoption (with less incentive to bypass security systems), stronger provisioning and deprovisioning, reduced attack surface when rogue and orphan accounts are remediated, and less entitlement creep.

- The workforce also experiences benefits, such as improved employee efficiency, an enhanced, consumer-grade experience and the proper entitlements for immediate access to all needed apps.

It’s definitely worthwhile to spend some time to find the best IDaaS solution. And when that solution incorporates all five threads, you’ll be well on your way to achieving your business optimization goals for the hybrid enterprise.

Learn more about Identity-as-a-Service: [http://ca.com/identity-service](http://ca.com/identity-service)

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.