ZIFF DAVIS

How to Avoid Purchasing a Throw-Away IDaaS

Introduction – The Evolution of IAM

Just as everything about IT security has evolved rapidly in recent years, so it is with Identity and Access Management (IAM). Greater IT mobility, hybrid infrastructures, and more agile line-of-business operations are all major drivers behind this evolution. These changes not only place new demands on IAM, they also offer new models for delivering and consuming IAM services.

IT infrastructure has grown well beyond the physical walls of the enterprise. It is now a complex hybrid environment made up of legacy systems, many different kinds of mobile devices, mobile apps, and cloud-based software (SaaS), as well as internet enabled products. This complexity has placed new demands on identity management. In addition to authenticating many different kinds of users, it must also manage authorization and provide accountability, which are essential functions of today's IAM solutions. As more business operations move into the cloud, IAM has become the core of security and touches every part of an organization. Lines-of-business (LOB) often have demanding projects requiring back-end IAM capabilities. Whether it's marketing requesting an easy, seamless single sign-on (SSO) experience, or development teams needing to rapidly roll out new mobile apps by leveraging authentication and self-service framework accessible through a REST API, IAM is now an essential part of revenue driven projects and innovation.

However, it's not just these new demands on identity management that are driving the evolution of IAM. Another factor is the emergence of IAM as a cloud based service. Known as Identity and Access Management as a Service, or IDaaS, this new incarnation of IAM provides IAM functionality as a monthly subscription service delivered from the cloud. IDaaS has quickly become the fastest growing segment of the IAM market. Gartner estimates that by 2020, 40% of all IAM purchases will be delivered as IDaaS.[i]

There are several reasons why IDaaS is coming to dominate the IAM market. First of all, new demands being place on traditional on-premises IAM infrastructure are overloading these legacy systems. Traditional IAM tends not to be agile enough to keep up with development or quick enough to respond to LOB needs, such as employees wanting immediate access to new cloud apps, or consumers expecting a seamless SSO experience with their social identities. With IDaaS, organizations can adopt modernized IAM capabilities and be more responsive to business needs without hiring new staff. This is a major advantage for enterprises with complex IT environments. IDaaS has other advantages too. For instance, most security experts today agree that cloud based systems are more secure because IDaaS service providers are totally focused on providing a secure identity management service for their customers. They offer more best-of-breed security expertise than most businesses are able to acquire on their own.[ii] Also, by eliminating on-premises infrastructure and making implementations faster, IDaaS lowers the cost of ownership.

With many businesses operating under a "cloud first" mandate from upper management, IDaaS would seem to be the perfect answer for moving increasingly challenging IAM functions to the cloud in a way that improves security, enables greater business agility, and saves money. But, there's a catch.

IDaaS is Evolving Too

IDaaS provides such a compelling value proposition that thousands of companies and early adopters have jumped on the bandwagon with first generation IDaaS products. Although many of these products offer effective federation to SaaS applications, and some also support access management for a limited set of standard on-premises systems, these capabilities only represent the easy parts of what a full IAM stack needs to do. In fact most of today's IDaaS solutions, even some of the best known and highly rated brands, have not evolved into fully baked IAM solutions.

Many users of today's first generation IDaaS products still need on-premises infrastructure to complete their IAM picture. That means most "Gen 1" products serve as only one part of a hybrid IAM environment. Making these cloud IAM products work with existing systems can actually increase an organization's costs and integration burdens. Although organizations that adopt these one-off products may now have a very good federated SSO product from the cloud, their original goals of reducing costs, increasing agility, and eliminating infrastructure challenges have not been met.

Some "Gen 1" IDaaS solution providers have no intention of delivering a full, cloud-based IAM product with the same breadth and depth as an on-premises IAM. Others, however, are still working to expand their product's capabilities. Meanwhile, large security companies with full function on-premises IAM offerings are investing heavily in their full-stack cloud IAM products. As some of these next generation IDaaS solutions are now becoming available, many early IDaaS adopters are throwing out there "Gen 1" IDaaS in favor of a full-stack solution.

Implementing an IDaaS only to throw it away and start over on a more complete cloud-based solution is a costly approach to IDaaS. It's also unnecessary. With the right kind of planning and product evaluation, you can avoid purchasing a throw-away IDaaS.

A Smarter Approach That Avoids Throw-away IDaaS Solutions

As the market stands today, there is considerable variation in the capabilities offered by IDaaS providers. This is especially true among cloud-only solutions. Many of those began by offering the easiest parts of the IAM puzzle – access management – and their strength in this area continues even as they lag behind in identity management capabilities. Adopting the wrong solution based on meeting short term access management or SSO objectives can result in more work than you anticipated, work that must be undone and redone if you ultimately decide you need a complete cloud IAM solution. Although buying a low cost IDaaS may seem like an easy, low risk decision, it can turn into a big, expensive headache. Unless you know exactly which capabilities your organization will ever need, or unless you expect your organization will never grow or change, there are several capabilities you must have in an IDaaS if you want to avoid a throwaway cloud IAM purchase.

Here are essential features, capabilities, and considerations you should include in your IDaaS evaluation:

✓ **To future-proof your IDaaS investment, a full-stack cloud IAM is essential.** First and foremost, invest in an IDaaS solution that offers a full stack of on-demand IAM features from the cloud, covering all elements of IAM: identity governance and administration (IGA), access management, federation, self-service, and powerful audit and reporting capabilities.

✓ **Don't overlook IGA capabilities.** Choosing an IDaaS that lacks IGA capabilities means an organization will not be able to complete its vision for cloud-based IAM without further integration of multiple products. Choose an IDaaS that offers both identity and access management, including multi-level provisioning, approval workflows, access request and certification, segregation of duties policy enforcement, and role lifecycle management.

✓ **Be sure the capabilities are available on-demand.** Even though your organization may not be ready for a "rip and replace" implementation, eventually moving your total IAM environment to the cloud will result in considerable cost savings and boost your organization's agility. Therefore, look for an IDaaS with premium on-demand cloud-based features that can be turned on when you need them, without having to integrate with an additional cloud product. The most cost-effective approach to infrastructure-free IAM is with one single cloud IAM service, not many.

✓ **Support your legacy systems.** Be wary of an IDaaS that cannot support your legacy applications or can only support a few basic ones. An enterprise grade IDaaS – one capable of serving as the core of your IAM environment – should be capable of supporting all your on-premises and cloud systems.

✓ **Look for powerful reporting from one single screen.** Choose an IDaaS that offers identity governance, federation, and access management reports from one single screen. This will greatly reduce costs, not to mention your team's headaches during audit time.

✓ **Cost-saving self-service tools are essential.** An enterprise grade IDaaS will offer cloud-based self-service tools supporting multiple languages and user populations, including user registration, password resets, username recovery, profile management, access requests and approvals, as well as recertification approvals.

✓ **Be able to support and scale rapidly for all user populations**. Look for an IDaaS that has proven scalability with all user populations: B2E, B2B, B2C, and B2IoT from a single platform. The IDaaS must be able to scale rapidly, especially for business scenarios that have dramatic changes in user demand, such as retail. A truly enterprise grade IDaaS will be able to handle tens of millions of B2C users and should become more affordable as the number of users increases.

✓ **Choose a vendor with global reach.** The IDaaS solution you choose should come from a vendor with proven geographic penetration. This vendor should have sales across all major regional markets, be able to provide service and support regardless of geographical location, and can scale globally without relying on third party vendors.

An IDaaS solution with these capabilities will provide a solid foundation for successfully fulfilling your IAM needs through a sustainable cloud strategy. When considering your IDaaS options, however, there are certain practices you should avoid:

✗ Do not think about an IDaaS investment as a short term solution to an immediate problem. Investing in IDaaS needs to be strategic.

✗ Do not invest in a solution that requires multiple cloud and on-premises partners to complete your IAM picture. This increases your integration headaches, expenses, and risk.

✗ Do not invest in an IDaaS solution based on promises of future functionality, because you could be benefitting from those cloud-based IAM features today. And, if the IDaaS fails to deliver on promised features, there is a good chance you will have to eventually discard your initial IDaaS purchase and start again.

Conclusion – Making the Right Decision

IAM has already moved to the cloud, and there are a lot of compelling reasons why. Actual use cases have shown that IDaaS can reduce deployment time by 75 percent, enable integrating new applications up to 100x faster, and reduce total cost of ownership by 60 percent.[iii]

However, the key to success is selecting the right IDaaS solution. Investing in an IDaaS should be a strategic business decision, because the solution will touch every corner of your organization. Many companies who unwisely purchase low cost, throw-away IDaaS later face tough decisions. Jason Meece, a Managing Partner at IBM Security, shared, "Some companies, who were quick to purchase a cloud IAM product simply for federated SSO during the last two years, are already trading up for IBM Cloud Identity Service, because it offers on-demand IAM capabilities spanning federation, web access management, and IGA all from one simple service." Meece explained these organizations don't want a cloud band-aide. Rather, they want an IDaaS to serve as the very core of their long-term IAM strategy.[iV]

Here are several steps you can follow that will help you make the right IDaaS decision for your business:

1. Begin by evaluating all your organization's IAM needs. What are your access management and identity management requirements? Does your organization plan to adopt a cloud-first initiative? What SaaS applications and legacy systems do your employees, customers, business partners, etc. need to access? What are your cloud and mobile requirements? What are your audit and compliance needs? How granular do your controls need to be?

2. Look ahead to where you expect your requirements will be in three to five years. Consider not only the identity and access management functions you will need, but also how you will support that for the level and types of business activity and growth you expect.

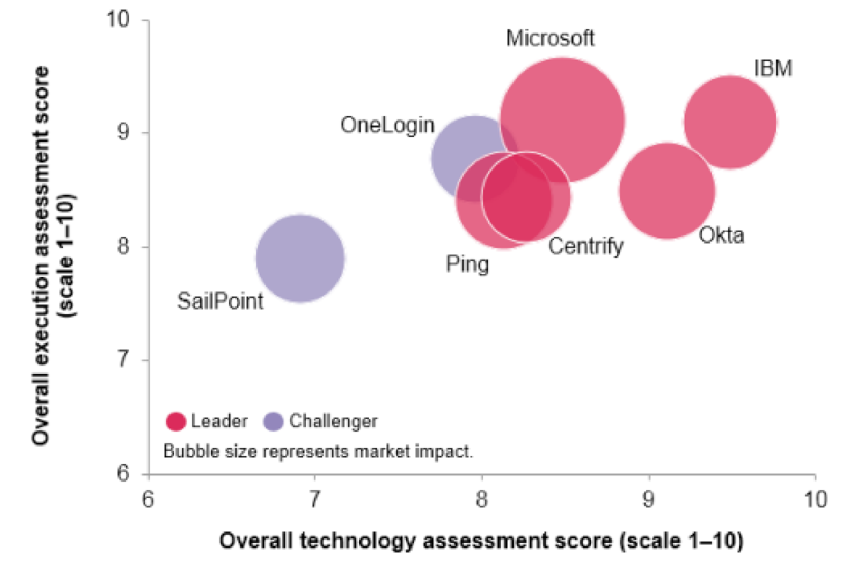
3. Evaluate vendors based on:

   - Their current ability (not future promises) to deliver a complete cloud-based IAM solution
   - The staying power of the parent organization
   - Their ability to reduce the TCO of your entire IAM environment, not just one aspect
   - The global security reputation and expertise of the parent organization
   - Their ability to scale globally without integrating third party vendors
   - Their proven success in supporting all user groups (B2E, B2C, B2B, B2IoT) without integrating another product
   - Their market leading position in the most recent IDaaS report

The ultimate goal of any IAM solution is to simplify and accelerate identity protection in multi-perimeter environments, but not in a way that limits your security or ability to reach your goals. Choosing the right IDaaS solution will not only increase your security but free you of the unpredictable costs and management challenges of on-premises IAM.

To learn more about how to evaluate IDaaS solutions, see Ovum's 2017 IDaaS Decision Matrix Report

Figure 2: Expanded view of Ovum Decision Matrix: IDaaS 2016–17



Source: Ovum

[i] Neil Wynne and Gregg Kreizman, "Critical Capabilities for Identity and Access Management as a Service, Worldwide," Gartner, September 29, 2016

[ii] Anna Seacat, "IDaaS: Life Before and After Cloud IAM," SecurityIntelligence, July, 2016

[iii] IBM internal research

[iv] IBM