MAKING THE CASE FOR IDENTITY-AS-A-SERVICE

ABSTRACT

This white paper covers the different evaluation criteria in approaching cloud-based Identity and Access Management (IAM). It maps key considerations in the evaluation process, as well as perceived barriers to achieving Identity-as-a-Service (IDaaS).
INTRODUCTION

Identity-as-a-service (IDaaS) is a topic that has picked up considerable momentum recently as the IT landscape has continued the shift toward SaaS applications, to the point where today many organizations are seriously considering running security applications from the cloud. Many organizations today are considering IDaaS, but as with many new concepts, the unknown presents both exciting and daunting aspects. As organizations consider IDaaS, it is natural to have questions and concerns that need to be addressed before proceeding down that path.

First, not all paths are created equal. It may be tempting to think that there is step-wise, one-size-fits-all approach to IDaaS, but the truth is that there are multiple variables that influence this decision. It is critical that organizations understand what these variables are, which questions to ask, and the context in which their organization sits in order to understand whether a cloud-based IAM system is the right approach.

Second, again, as with any new concept, there are always doubts and perceived barriers to tackle. The goal organizations should reach for is to dig deeper into these barriers and understand what the reality, drivers, and constraints are for their particular organization. The ultimate goal should be to address any doubts and confidently proceed down the right path for you at the moment. First, let’s explore the topic of whether a cloud-based IAM solution makes sense for you.

IS CLOUD-BASED IAM RIGHT FOR YOU?

Cloud-based Identity and Access Management (IAM) solutions have come a long way. Now that these solutions have achieved a reasonable level of maturity and market acceptance, it’s a good time to evaluate whether it is the right solution for you and your organization. The more an organization can ask the right questions and understand what the key criteria are, the more confident can the organization be in their decisions.

The first consideration is to create, validate, and gain a deep understanding of your organization’s business and technical goals as they relate to IAM. These goals serve as the most critical guideposts that set the direction in the decision path. Common goals include reducing operational costs, creating a simpler user experience, or even building a more secure system. Dig deep into what the primary problems and challenges your organization is facing, from both a business and technical perspective. Once you have this as the foundation, you can take the next step in evaluating whether a cloud-based IAM solution will work for your organization.

The next consideration is to look at the volume and types of Software-as-a-Service (SaaS) applications that your organization uses. This will provide a good indication of what your organization’s level of acceptance is for SaaS applications. Beyond your organization’s appetite for SaaS applications, you will also need to understand the level of trust being placed in the cloud. In other words, assess how “business-critical” the SaaS apps are – for example, are only basic HR systems being stored in the cloud, or are critical files being stored in the cloud as well?

As organizations move to the cloud, the hybrid approach is inevitable – consider how your organization is choosing to take their next step to the cloud. Some organizations choose to deploy only new business applications in the cloud as a first step. Other organizations choose to deploy certain aspects such as development and test in the cloud and deploy production systems inside the firewall. It all depends on the business and technical strategy behind your organization’s approach.

Finally, bring it up a level higher and question what value a cloud-based IAM solution will bring to your organization. Various drivers organizations consider include a reduced operational effort, a smaller on-premise deployment footprint, and a financial shift from capital expenses to operational expenses. At the end of this evaluation, the end-game is to be sure that, in the right context, a cloud-based IAM solution fits with your organization. Now that you’ve asked all the right questions and made the assessment that IDaaS is the right choice for your organization, it is natural that doubts will surface and make way for a few more questions. We’ll explore this in more depth next.

OVERCOMING BARRIERS TO IDAAS

Common (or at least, commonly perceived) barriers to IDaaS that we often see include questions around stability, security, cost, and interoperability with existing systems. We believe the best approach for each of these is to tackle them head-on, so we can understand whether each obstacle is truly an obstacle.

Stability
Contrary to popular belief, cloud-based solutions do not necessarily offer less stability than an equivalent system deployed on-premise. By design, many enterprises do have a single point of failure in parts of their IT infrastructure. In fact, organizations
can rarely justify fully redundant infrastructure for 100% of their applications and are faced with selecting just a few key systems. In comparison to a cloud-based solution, it runs on commercial-grade cloud infrastructure, which is more robust than an organizations’ standard infrastructure. This, in turn, provides a higher level of uptime.

**Security**

Now that your data is stored in the cloud, a common fear is the loss of control, given it sits outside your organization’s traditional boundaries. Again, contrary to popular belief, on-premise deployments are not automatically more secure than cloud-based deployments. The notion of a traditional security perimeter has been shattered, and in place of that, organizations are responding to the demands of business agility and have opened up internal applications to partners, customers, and suppliers. By doing so, they have of course also opened up their vulnerability to an evolving generation of hackers. IDaaS solutions are deployed with a very limited set of entry points, which reduces the potential in an attack. IDaaS vendors also typically go through rigorous and ongoing penetration tests to ensure that the systems are secure and up-to-date, and in many cases, surpass the level of testing that on-premise solutions undergo.

**Cost**

SaaS solutions have shifted the cost and consumption model for enterprise applications. The models have shifted from the on-premise license associated with an upfront capital expense and annual maintenance costs. This has shifted to a subscription-based approach, which usually can be classified as operational expenses. Given this, it’s important to understand how your organization treats capital expenses vs. operational expenses. In some scenarios, it’s easier to secure funding and execute for operating expenses, which would help make the case for IDaaS.

Then, it is important to understand the total cost of ownership behind on-premise vs. SaaS solutions. At first glance, the sticker prices will naturally vary, but also think about hidden costs associated with implementation, customization, time-to-deployment, and maintenance. If your organization requires complex use cases, often times custom-coding is far more involved and costly than a simpler configuration-based deployment. Most organizations find that cloud-based solutions are easier to deploy and faster to derive immediate value from, which translates to a lower cost of ownership.

**Interoperability with On-Premise Applications**

As valuable as it is to access external SaaS applications, it is just as critical to access on-premise applications as well. Many IDaaS vendors claim to provide “enterprise identity management,” but if you take a closer look, they often times only connect to on-premise directory systems and not with on-premise applications. Take a close look at what vendors claim they do when it comes to application access and understand what it really means. After all, the ability to access only external SaaS applications provides only half of the equation when it comes to business impact!

**Fit with Existing Processes**

When it comes to IAM systems, especially IDaaS solutions, this is an ideal time to engage with the line-of-business (LOB). Take this as an opportunity to analyze and improve your current business and technical processes. During time of change, it is always a good chance to re-evaluate current processes and determine whether changes are required. The key in choosing an IDaaS vendor in this process is to find one that is flexible and can adapt to your current (or proposed) processes.

**CONCLUSION**

There is no quick answer when it comes to understanding whether IDaaS is right for your organization. The best thing you can do for your organization is ask the right questions, assess your organization’s business and technical goals, and of course, apply it all in the context of your business. With the right level of thought, planning, and reflection, IT can successfully leverage cloud-based IAM across the organization for maximum impact.