Is Your IDaaS Too DIY?

A TACTICAL GUIDE TO FINDING THE RIGHT IDAAS PROVIDER

By Abhimanyu Yadav, Simeio VP of Product
CHAPTER 1:

Seven Questions To Help You Put The “Service” Back Into “Identity As A Service”

You wouldn’t think a simple word like “service” could have people scratching their heads. And yet there’s one use of that term which constantly creates confusion.

It’s the phrase “Identity as a Service.” (Or “IDaaS”)

When many people hear the term “identity as a Service,” they inevitably draw a parallel to “Software as a Service” — or “SaaS”. And rightly so. At their core, the two concepts are very similar.

They both free companies from the cost and burden of owning, maintaining and managing all the infrastructure required to deploy a specific capability. They do this by offering the exact same functionality on a subscription basis.

In the case of IDaaS, the capability we’re talking about is Identity and Access Management (IAM) — the combination of technologies and expertise that enables the right people (and only the right people) to access the right network resources for the right reasons.

With SaaS, there’s very little ambiguity over what “service” you get: the provider will host, manage and maintain the SaaS application, thus guaranteeing you a specific level of availability as prescribed in a service level agreement (SLA).

WHAT’S IN A WORD?

When it comes to “service,” it can be a lot. Actually - it can be everything.
It begs the question: can you really call it a “service” if the provider expects you to the job of managing it?

Many IDaaS firms adhere strictly to the SaaS model in that they are pure cloud-based solutions. Indeed, for most people “SaaS” and “cloud” are virtually synonymous. So when we tell people that Simeio is an IDaaS firm that provides managed identity services using any combination of your IAM infrastructure or ours, in the cloud or on-premise, they often get a strange look on their faces.

Isn’t it an oxymoron to say, “on-premise IDaaS”?

No. Not necessarily...

To continue the landscaping analogy, when you need your lawn mowed reliably and expertly....whether the gardener uses his mower or yours doesn’t really matter much.

The other thing that varies wildly is the breadth and depth of “services” that are actually offered by firms that call themselves IDaaS providers. In other words, there is no single definition of what “IDaaS services” are.

Many of these companies offer only a limited set of services — and by “services,” they really mean “capabilities” — such as Single Sign-On (SSO).

Many are also limited to integrating with cloud-based solutions only. They won’t work with legacy applications or offer any sort of customizable integrations or workflows! Gartner calls these “web-centric IDaaS providers.” This helps to distinguish them from what it calls “fullFeatured IDaaS providers”...such as Simeio.
To help you determine which provider is best for you, here are seven key questions to ask when choosing an IDaaS provider:

1. Do you offer a full, end-to-end set of enterprise-grade security and identity capabilities, including:
   - Access Governance
   - Identity Administration
   - Privileged Identity Management
   - Access Management & Federation
   - Core Directory Services
   - Security and Risk Intelligence
   - Data Security and Loss Prevention
   - Cloud Security

2. Do you provide these capabilities as a managed service, backed by stringent service level agreements (SLAs)?

3. Do you offer complete operational services including:
   - Provisioning and de-provisioning
   - Application onboarding
   - System maintenance
   - Incident/ticket resolution
   - Software installations
   - Enhancements and bug fixes?

4. Do you offer advanced monitoring, alerting and reporting capabilities such as user behavior analytics to detect and prevent aberrant or unauthorized access attempts?

5. Do you integrate with legacy systems as well as cloud-based services?

6. Can I use any combination of your IDaaS platform and my own infrastructure?

7. Are your solutions vendor and technology agnostic – that is, will you tailor the right set of solutions to meet my unique needs regardless of what company’s technologies are required?

BY THE WAY? AT SIMEIO, WE’RE PROUD TO ANSWER “YES” TO ALL OF THESE QUESTIONS.

While the IDaaS industry may be confused over what “service” means, we’re sure not. Simeio is the leading provider of Managed Identity Services. Put simply, it means that we don’t just host and maintain your IAM infrastructure, we operate it, too. It is an outsourcing model for security management, which is an essential component in secure business resilience and agility.
CHAPTER 2:

Five things you should demand from your IDaaS provider

Businesses have routinely relied upon independently operated Security Operations Centers (SOCs), which combine highly skilled professionals with industry-leading processes and technologies to detect, analyze and prevent network security incidents.

But this model is just starting to take hold for IAM.

We’ve reached a tipping point in the maturity of IDaaS, which has given rise to Managed Identity Services. This evolution is being fueled by organizations who now have greater expectations of their IDaaS providers and a growing list of demands.
2. Flexibility and Agility

Companies are no longer interested in a one-size-fits-all IDaaS model, especially where they are expecting IDaaS solutions to do more than simple tasks such as employee login and provisioning.

Where IAM is being used to fuel the Digital Business, improve customer engagement or manage threats, companies are looking for IDaaS vendors to provide them with the flexibility and agility they need to meet their business goals.

For a next generation IDaaS company, this means providing a single tenant or multi-tenant solution, hosted or on-premise, with fixed monthly pricing or transaction-based pricing.

Service flexibility goes a long way to reduce risk and to allow businesses to quickly seize fleeting opportunities. In an IDaaS or SaaS model, the vendor is responsible for governance, operations, security, compliance, etc. So IDaaS vendors must be flexible enough to provide custom-tailored security controls and SLAs that are negotiated into contracts, including service levels, privacy and compliance controls.

3. Single Sourcing

Any company with well-defined enterprise security risk management must view each SaaS provider as a supply chain security issue. This is especially true in the case of IDaaS.

Each provider has to be carefully examined – what are their incident management and disaster recovery processes? How do they backup data? Are they ISO 27001 compliant? Do they perform background checks? Who has access to the data, what are their access controls, etc.? It’s not surprising that companies often demand in-person site inspections of their IDaaS suppliers.

Introducing multiple IDaaS companies in the supplier chain exponentially increases business risk, and often reduces the economic benefit that could have been gained due to efficiencies derived from an IDaaS resource in the first place.

If a customer is expected to use one IDaaS company for single sign-on, another for privileged access management and another for access governance (and the list of diverse options goes on), then they are left at the center of a storm.

You shouldn’t have to choose between convenience and security!
4. Expertise

IAM is a complicated discipline that requires rare and deep expertise. Expertise that often lies outside the typical company’s core competency.

With the rapidly expanding array of network services from legacy systems to new SaaS offerings, combined with the mushrooming demand for access to these services from increasingly diverse stakeholders, you can scale up your IT organization and infrastructure and get into the IAM business, which is laborious and expensive. Or, you can simply turn to the experts.

Yet first-gen IDaaS companies seem oblivious to this reality. A well-known IDaaS company, for example, frequently hosts technical workshops on “How to Integrate Office 365 for Single Sign-On”. You may even have received these emails yourself.

But has anybody stopped to ask, in an as-a-Service arrangement, why is the business customer expected to learn how to do this? How are they expected to deal with complex scenarios or custom integrations? Is “IDaaS” in this situation just hosted software that the customer has to figure out how to operate? Is the customer expected to recruit and retain permanently trained experts on staff?

Managed Identity Services companies, on the other hand, will handle all this complexity for you. They will essentially get you out of the IAM business -- so you can focus on your own.

5. Portability

Something that is not spoken about enough when it comes to IAM is inter-operability and portability. This is becoming increasingly important as companies have had, for one reason or another, to change part of their underlying technology stack or switch IDaaS vendors entirely.

The issue with most IDaaS companies today is they are not built to integrate with each other (their competitors). When a business places all their security, compliance and reporting into the custody of such a provider that has proprietary standards (or lack of APIs), they are introducing risk, which will result in higher fees down the road.
CHAPTER 3:

Fixing the Problem:
The Simeio Difference

Now that we’ve covered the five growing expectations businesses have, here is specifically how Simeio is responding to these new demands.

What makes us truly, meaningfully different from the competition?

Unlike most other IDaaS providers, who primarily host and maintain your identity and access management (IAM) infrastructure but still expect you to operate it, we offer (Simeio offers) Managed Identity Services. We operate, monitor and defend your IAM infrastructure as a full-service solution.

Like I wrote earlier, the concept of Managed Services isn’t new. But there’s a fundamental difference between simply outsourcing the task of managing your IAM infrastructure and delivering on the promise of next-generation IDaaS. While it is inherently valuable to have experts handling the job, next-generation IDaaS requires more than just people. (Otherwise, it’s just a different group of people doing the same old things.)

Next-gen IDaaS requires a next-generation identity platform. That’s exactly what we’ve built at Simeio.

By definition, every IDaaS provider has a platform. Although the list is pretty extensive, what makes ours different – and an enabler of next-gen IDaaS – boils down to two key features: identity virtualization and identity analytics.
Identity Virtualization

Identity virtualization is a unique and critically important feature of our platform, abstracting the functions used to operate and manage your IAM infrastructure from the underlying technologies.

And yes – I’ll admit that “identity virtualization” sounds like just another IT buzzword. So as my marketing colleagues often remind me to do, let’s talk about the benefits.

First, it enables us to be vendor, technology and deployment agnostic. Put simply, this means it doesn’t matter what mix of IAM vendors or technologies you have, or where they’re deployed – on premise, in the cloud, or a combination of the two – in order to enjoy the benefits of next-generation IDaaS. No other IDaaS provider can make this claim.

We can use your existing IAM infrastructure – or we can augment it with advanced capabilities or replace it entirely with our IDaaS solutions.

You can choose from a wide-range of IAM and security solutions from leading vendors, including Oracle, CA Technologies, Dell, IBM, ForgeRock, Saviynt, Palerra, ObserveIT, Lieberman Software, CyberArk, BeyondTrust, RSA, Brinqa, Securonix and more.

I can’t overstate the importance of this. No one-size-fits-all IDaaS model can possibly meet the dynamic requirements of today’s digital enterprise – which is why we sell capabilities, not software.

In fact, in order to offer the broadest and deepest set of Managed Identity Services on the market today, we have to combine best-of-breed technologies from multiple vendors – no one vendor’s stack does it all. So rather than introduce complexity to achieve this goal by adding multiple technologies that have to be managed separately, our platform enables us to actually simplify operations.

There are important business benefits, too.
Regardless of the complexity of the underlying infrastructure, you still get “one throat to choke” with our Service Level Agreements (SLAs) guaranteeing uptime. It also significantly reduces risk by eliminating vendor or technology lock in.

You get unparalleled flexibility and agility with the freedom to combine best-in-class offerings to create a solution that’s customized to meet your specific requirements, and the freedom to add, switch or upgrade any component at any time to meet new or changing needs and seize fleeting business opportunities.

We can deploy individual IAM capabilities such as privileged account management and multi-factor authentication, or even entire IAM solutions in a fraction of the time – and a fraction of the cost – of building and developing your own. And so your IAM capabilities can actually become a business enabler instead of a bottleneck as your business needs evolve.

The business model is equally as flexible. You have the option of using a cost-effective multi-tenant solution or using a dedicated environment. You get a choice of “pay as you go” pricing options; services can be licensed per user, per transaction or subscribed through a fixed monthly fee.

Identity Analytics

As I discussed in the previous chapter, next-gen IDaaS solutions must provide organizations with a new and improved level of analytics that enables them to better understand risk and to address it up front – as well as to identify opportunities to add value.

In today’s connected enterprise, you can’t simply firewall off your sensitive data to keep it safe; too many people need access to it in order to do business. So what’s the key to keeping the bad guys out while letting the good guys in? Analytics.

Your IAM capabilities can actually become a business enabler instead of a bottleneck.
Simeio Identity Intelligence combines proprietary and best-in-class monitoring and alerting technologies, System Information and Event Management (SIEM) technologies, and User Behavior Analytics (UBA) to create a powerful solution that’s designed to provide real-time insights into how digital identities are being used – or misused.

It’s designed to detect both security vulnerabilities and malicious activity tied to identity, such as ghost accounts or undeleted default accounts, or atypical access patterns such as unusual times or locations.

It includes special features for monitoring and recording privileged user activities – those associated with accounts used by system administrators that provide nearly unfettered access to your entire IT infrastructure where, in the wrong hands, the damage can be catastrophic.

It then goes further to provide identity intelligence and behavioral analysis. It offers insights into patterns of usage among employee, partner, supplier or customer accounts, and analytics that can be exploited by sales or marketing to identify new business opportunities.

People still make the difference

While I’ve focused here on the Simeio Identity Platform, I don’t want to conclude without at least a nod to our people. IAM is a complicated discipline that requires rare and deep expertise that lies outside the typical company’s core competency.

At Simeio, we have the largest in-house team of consultants, engineers, analysts and advisory professionals compared to any other IDaaS provider. You get greater efficiencies through aggregation of knowledge, harnessing broad actionable intelligence, and having a full complement of security professionals on hand at all times.

Our people and our technology come together in the Simeio Identity Intelligence Center™ (IIC), our cutting-edge Center of Excellence for Identity and Access Management. Simeio IIC™ enables us to deliver Managed Identity Services far more efficiently and effectively than any other provider.

Get in touch and we’ll be happy to show you how our next-generation Identity Platform can transform the way you look at identity management.
Simeio is a complete Identity and Access Management (IAM) solution provider that engages securely with anyone, anywhere, anytime, with an unparalleled “service first” philosophy.

Contact us now to set up your free consultation.