Checklist:

3 Reasons for Choosing Cloud-first Identity for Hybrid Environments

okta

Index

Not all hybrid identity solutions are the same

In order to stay competitive and reduce costs, smart enterprises are constantly on the hunt for disruptive ways to leverage technology. They're moving towards hybrid IT environments because they recognize the benefits of faster implementations and high cost savings that come with moving from on-premises to cloud-based applications and infrastructure. Although many businesses are in the process of moving as much as they can to the cloud, IDC estimates that 70% of large enterprise workloads still run in on-premises data centers. The popularity of best-of-breed apps (such as Office 365, Salesforce, Slack, and so on), paired with the reality of on-prem systems that aren't going away any time soon, contribute to complex hybrid IT environments that are challenging to secure.

Thankfully, there are powerful identity and access management (IAM) solutions that can help IT and security teams protect both Software-as-a-Service (SaaS) and on-prem resources. That said, choosing such a crucial platform for your business can be difficult, since there are many requirements, considerations, and variations to evaluate. One key way to differentiate hybrid access providers is to understand their origins—did they start out building a cloud-born platform and then extend its modern innovations to the on-prem world, or did they first focus on on-prem needs and later attempt to adapt that platform in light of growing demand for cloud IAM? As we'll explore below, this is no minor distinction, which is why cloud-led approaches win out time and time again in almost every technology category.

Just because your top leadership says they want to embrace this cloud journey, that doesn't mean you can rip out critical on-prem systems, like Oracle e-Business Suite or SAP, right away. It's more important to avoid adopting any new solutions that add to server sprawl, and instead look to mature cloud technologies as opportunities arise. One element of the IT stack that's prime for replacement is legacy web access management (WAM) systems, which are costly to maintain and offer only limited, commoditized capabilities. Consider whether the time might be right to adopt identity-as-a-service (IDaaS) and start protecting your hybrid IT environment *from* the cloud.

Key considerations for hybrid IAM

To aid in the IAM evaluation process, let's review the three primary areas where cloud-led solutions differ from on-prem-first systems: how long it takes to extract value from your initial investment, the ongoing resources required to support hybrid access needs, and the platform's ability to future-proof your enterprise's security posture. We'll start with a look at the long-term impact of hybrid IAM solutions.

Gaining future-proof identity

The most important advantage of cloud-born providers is that they are not constrained by existing on-prem baggage, so they bring features and security improvements to market faster. In thinking about your hybrid access needs, be sure to consider how they are likely to evolve over the long term as your company moves more and more towards a cloud-centric IT posture. Question whether your strategic partner is continuously investing in and innovating around the cloud, keeping in mind that the majority of today's most critical IAM functions—like authentication, federation, and coarse-grained authorization—are delivered more securely and cost-effectively as on-demand cloud services.

Below are some ways to determine how future-proof an IAM solution is:

Cloud innovation:

- How long has the cloud IAM offering been generally available?
- How well does the provider's cloud feature set match up against either their own original on-prem products, or other cloud-first solutions?
- How much is the vendor investing in true cloud innovations, vs. basic APIs that just lift-and-shift on-prem identities to the cloud?

Advanced capabilities:

- Which cloud-specific features do they offer, if any? For example, adaptive multi-factor authentication, dynamic scaling, or identity lifecycle management?
- Is the provider able to analyze the evolving threat landscape and emerging attack vectors across thousands of customers to uncover real-time insights that will protect you before attacks occur?

Scalability:

- Is the solution built to automatically handle growing volumes of both users and authentications, so it won't restrict your company's growth?
- What type of scale has the platform already been proven to support (while meeting all performance and compliance expectations), e.g., can it manage billions of identities, millions of daily authentications, and traffic bursts of up to 500,000 authentications per minute?

R&D spend:

- According to the provider's financial statements, how much do they spend on research and development overall?
- Considering their product portfolio, how much of this spend likely goes to cloud solutions vs. maintaining older versions of revenue-generating on-prem solutions?
- What is the total headcount of the vendor's development team?
- How many of those developers are focused on addressing technical debt and supporting legacy products, as opposed to building and enhancing IDaaS solutions?

Independent validation:

- Has the provider's position in Gartner and Forrester's industry reports improved consistently over time?
- Does the vendor emphasize *enabling* you to comply with various regulations, but still leave most of the burden on the customer?
- What is the scope of their own third-party attestations, like SOC 2 Type II compliance?
- Do they offer dedicated HIPAA and / or FedRAMP environments with enhanced security and audit controls?

Beware of "smoke-and-mirrors" tactics that some vendors use to mask deep on-premises technical debt while they build out unproven cloud offerings. Meeting current requirements (such as authentication or single sign-on) is good, but it's not enough. Instead, find a partner that will bring the latest identity innovations to your on-prem workloads, so you can rest assured they will have your back in the years to come.

Security insights

One value of IDaaS solutions that's sometimes overlooked is the rich security insights they uncover by supporting billions of identities in the cloud. Through machine learning and advanced analytics, companies like Okta are aggregating important real-time data about threats and risk signals to protect their customers in ways that on-prem-first vendors simply cannot, due to siloed customer deployments. The more data that's gathered, the more accurate and insightful it becomes, and the more valuable a resource this is to customers. Okta's ThreatInsight solution uses the network effects of Okta's large customer base to rapidly detect and proactively block malicious IP addresses that attempt credential-based attacks.

Increasing agility

When selecting a new solution, it's also important to understand the total cost and agility impact of managing and maintaining that system over time. Switching from a legacy WAM system to on-prem-centric IAM can *initially* provide incremental value, but it will still consume too many resources for administration and maintenance. If you fully modernize with a cloud-first IDaaS solution, you will minimize on-prem sprawl, increase your team's productivity and responsiveness, and eliminate the risk exposure of delayed upgrades.

For a comprehensive comparison of the ongoing resources you'll need to support hybrid access, ask the following questions about each solution:

Operational requirements:

- How much IT effort and headcount will the solution require from your business for patching, upgrades, monitoring, and overall maintenance?
- Does the vendor deliver service improvements directly to a cloud tenant? Or when updates are needed, do they just provide patch files with instructions?
- Will you need multiple nodes to support a large IAM deployment? If so, how much work will it take to stay current with the latest versions and manage complicated rollbacks if you encounter an upgrade issue?
- How many environments (development, test, production) will you need to maintain for expensive on-prem servers?

Customizations:

- How many pre-built integrations to SaaS and on-prem apps are included in the provider's catalog?
- Does the platform have proprietary customization requirements that promote vendor lock-in and make the upgrade process even more brittle, or does it follow standards to help you efficiently support unique use cases?

Reliability:

- What is the vendor's reputation around reliability? What is their history of maintenance windows, unplanned outages, or data breaches?
- Is the architecture built with enough redundancy to stay online even when the underlying infrastructure has an outage (i.e., is the solution replicated across redundant availability zones, with constant controls and health checks)?
- Does the platform include a local database, application server, or other dedicated servers that are prone to failure?
- How does the SLA account for planned downtime (if at all), and what is the cost of this on your business in terms of productivity and reputation?

Security:

- Does the vendor have processes, tools, and policies in place to prevent, detect, and respond to threats in real time?
- Do they make smart investments and release regular security innovations that will help you stay ahead of the curve and fight the threats of the future?

Remember, just because a hybrid identity platform might promise lower costs than expensive legacy WAM solutions from the 1990s, that doesn't mean it's your best option today. Make sure to look beyond "good enough" on-prem-centric IAM, and consider the full advantages you'd gain with a modern IDaaS' efficiency, reliability, and availability. Cloud-first IDaaS solutions outpace all other identity platforms because they offer predictable subscription pricing, reduce ongoing customer maintenance costs by 3X-10X, and minimize your enterprise's on-prem dependency.

Ensuring consistent end-user experience at Alliance Data

Alliance Data, a Fortune 500 provider of loyalty and marketing services, fuels its growth through M&A, completing multiple acquisitions over the past few years. With this rapid growth, its complex, distributed, on-prem infrastructure caused significant friction for both end-users and IT admins, and became difficult and expensive to maintain. Alliance Data turned to Okta, adopting Okta Access Gateway (in addition to Universal Directory, Single Sign-On, and Adaptive Multi-Factor Authentication) to centralize access management across its 100 apps, 16 of which are on-prem, for its 20,000 users.

> *"With Alliance Data's rapid growth over the last decade, we needed a way to secure company data while streamlining the onboarding process, without disrupting our user's experience. With Okta Access Gateway, we were able to reduce the complexity for both our IT staff and our end-users, providing a seamless acquisition experience while improving our security posture and ensuring our customers' privacy"*
>
> *— Darren Linden, Head of Corporate IT Services, Alliance Data*

With Okta Access Gateway, Alliance Data saw a reduction in help desk calls for password resets, ultimately making its employees more productive and improving their overall experience at work.

Accelerating value

Many businesses are moving their IT resources to the cloud for the faster return and greater agility that best-of-breed apps like Workday for HR or Salesforce for CRM deliver. Even though you probably need to keep some legacy systems on-prem (such as your ERP, which might not support modern SAML and OAuth standards), that should no longer hold you back from moving identity management to the cloud.

In addition to the ongoing agility considerations we discussed above, here are some things to think about when comparing the time-to-value of cloud-led IDaaS versus on-prem-first IAM:

Cloud-to-ground product configuration:

- What percentage of the solution's IAM logic runs in the cloud vs. in customers' data centers? Does the platform's heavy lifting happen on-prem or in the cloud?
- How much legacy on-prem software are customers required to deploy in order to meet hybrid access needs?
- Is the vendor's cloud solution a native, born-in-the-cloud service, or simply their on-premises software running in a virtual machine on cloud infrastructure?
- How long will the provider's full migration to the cloud take, and how might this hinder your own cloud journey?

Unified vs. disjointed capabilities:

- Is the solution a truly unified identity cloud that will keep all of your configuration, administrative, and policy management tools in a single place from day one?
- Will the platform require you to duplicate user identities from on-prem in the cloud, or will it provide a single directory for all your hybrid access management needs?
- Will you need to navigate any fragmented workflows (e.g., for login, multi-factor authentication, or integrations) that might slow adoption?

Deployment time:

- How long does the solution take to deploy — days, weeks, or several months?
- Can it support all of your use cases out-of-the-box, or will you need non-standards-based customization that adds complexity to your environment?

Infrastructure and personnel costs:

- If the solution heavily relies on on-prem components, what types of dedicated servers, load balancers, etc. will you have to procure, deploy, and manage to support replication and high availability?
- What additional costs should you plan for infrastructure, administration, and support?

As you are reviewing these criteria, keep in mind this key advantage of modern IDaaS solutions: they only require a very small on-prem footprint, which is simple to install and maintain. Because 95% of the product's capabilities are delivered via the cloud with simple bridges connecting the identity solution into your data center, cloud-led hybrid IAM avoids the infrastructure headaches common with all other IAM platforms.

Elevate your hybrid identity strategy

With the latest IDaaS advancements, there's no longer a question of whether cloud-born identity platforms can handle on-prem use cases. Choosing to implement (or continue to leverage) an on-prem-first IAM solution will only slow down your company's migration to the cloud. Instead, a cloud-first IDaaS solution like Okta, with the vast majority of its platform running the cloud, is well-positioned to solve the hybrid realities of today's large enterprises, while saving money and time down the road as you migrate the rest of your business into the cloud.

Not only can Okta's market-leading solution meet the full spectrum of identity and access requirements—for applications and resources residing in either customer data centers or cloud infrastructure—in one centralized solution, it increases IT agility, improves your security posture, and lowers total cost of ownership up to 80%.

> *Okta Access Gateway brings all of Okta's proven capabilities from the cloud to the task of securing legacy on-prem workloads that can't be quickly rearchitected for modern standards like SAML or OAuth. Unlike traditional IAM vendors that grew up on-prem, Okta's no middleware, no database architecture reduces identity infrastructure up to 90% by running most of the identity platform in its cloud and simply providing a lightweight gateway with on-prem agents. Okta also offers zero downtime, regular patching, weekly product releases, dynamic scaling, a highly redundant cell-based architecture, and comprehensive industry certifications.*

For more details on how Okta Access Gateway enables enterprise organizations with hybrid IT environments to achieve simple and secure resource management across their legacy and cloud systems, visit https://www.okta.com/products/access-gateway/.

About Okta

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 6,000 apps, the Okta Identity Cloud enables simple and secure access from any device. Thousands of customers, including NASDAQ, Experian, CNA Financial, Allergan, Albertsons, Nordstrom, and 20th Century Fox trust Okta to work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work. For more information, visit us at www.okta.com or follow us on www.okta.com/blog.