okta

5 Ways to Distinguish Best-of-Breed Identity

All IT and security teams want to help their businesses grow, but you can only do that when you're able to truly focus on innovation and differentiation. While it's frustrating to be unexpectedly sidelined by complex identity challenges, the identity and access management (IAM) layer of your environment can't be ignored. That's because identity is a critical gateway to everyone and everything in your organization. Managing IAM is especially difficult if you're working within the stifling limitations of identity software that contains decades of technical debt. Many popular platforms still rely on legacy architecture that creates a massive attack surface, limits high availability, and hinders your application choices and future growth in general.

5 critical questions to ask your identity provider

As the go-to modern identity partner, Okta is committed to helping customers navigate their most complex and difficult use cases. Based on our exclusive focus on identity and our extensive experience supporting global enterprises, we've noted key questions that forward-looking technology teams ask to evaluate whether their IAM provider can effectively meet the organization's evolving needs.

Do you put customer trust and security first?

First of all, you'll want to consider how much research and development your vendor invests in critical platform capabilities that build customer trust. And since one of the most critical aspects of IAM security is multi-factor authentication (MFA), it's jaw-dropping that the global percentage of admins who actually use MFA today is just 9%. Given this, it's crucial to find out how robust your provider's MFA offering is.

Important questions to ask

- Do you prioritize integrations to your own internal stack of security tools or offer mature integrations with advanced tools (Proofpoint, Netskope, and Crowdstrike)?
- How many security exposures or vulnerabilities has your environment experienced in the past 12-24 months?
- How many "9s" of availability do you offer? How much on-prem legacy does your solution rely upon?
- What scalability measures do you have in place? Do you use automation to dynamically add, heal, or remove servers on demand?
- Does your solution officially support the full spectrum of MFA factor choices today? Or are many of the factors still in preview?
- How do you manage MFA across scenarios like LDAP, Radius, or APIs?
- Beyond risk and context-based protection, does your MFA solution offer pre-auth protection against account takeovers?

Part of the beauty of Okta is the balance it provides in terms of when to trigger MFA and when not to. It allows us to target the riskiest subset of access requests, rather than blanketing everybody.

–Kris Wilson
Senior Director, Product and Technology, T-Mobile

Was your IAM platform built from the ground up with a **modern architecture?**

Ideally, no one wants to swap out their identity infrastructure more than once in a decade, so it's important to be sure that your foundation is solid and future-proof.

Important questions to ask

- Is the platform cloud-native, or does it still rely on legacy components (such as Active Directory) that increase complexity and expose our cloud resources to Pass-the-Hash attacks?
- Does it lock us into brittle, outdated, on-prem directory or identity services?
- Can the IAM solution protect both hybrid cloud and on-prem resources without requiring us to change how our apps work today?

We've retired our custom MFA code and we've enabled both MFA for Office 365 and MFA for all of our on-prem solutions and all of our cloud solutions. We simply leverage the Okta APIs and MFA experiences that are provided natively out-of-the-box. We're also improving our availability and our scaling flexibility.

–Ben Hutchins
Identity Program Manager, The Church of Jesus Christ of Latter-Day Saints

Do you provide one unified platform to manage all of our identity needs?

Universal Directory

User Identities live in a lot of different places. With Okta's Universal Directory, you can create a centralized view of all your users, wherever they're mastered. It'll make access management more straightforward and secure and give users a consistent experience across your products.

Single Sign-On

If your product connects several apps together but requires people to authenticate every time they jump into a new section, you're losing major UX points. With Okta, users can click once to sign in to everything.

Provisioning

With Okta, you can automatically create user accounts for on-prem and cloud services, and then revoke access when an account is canceled. Implement Okta's connectors or write your own to build cross-application experiences that are more secure, more intuitive, and more delightful.

Watch out for providers that primarily view identity as an internal workforce requirement. Even if you don't have major external user requirements today, you'll eventually need to juggle diverse identity use cases if you want to keep up with the pace of digital transformation today. Think about how much time it would save to have one pane of glass where IT admins could manage identity and access needs across all of your customers, partners, supply chain firms, apps, and resources.

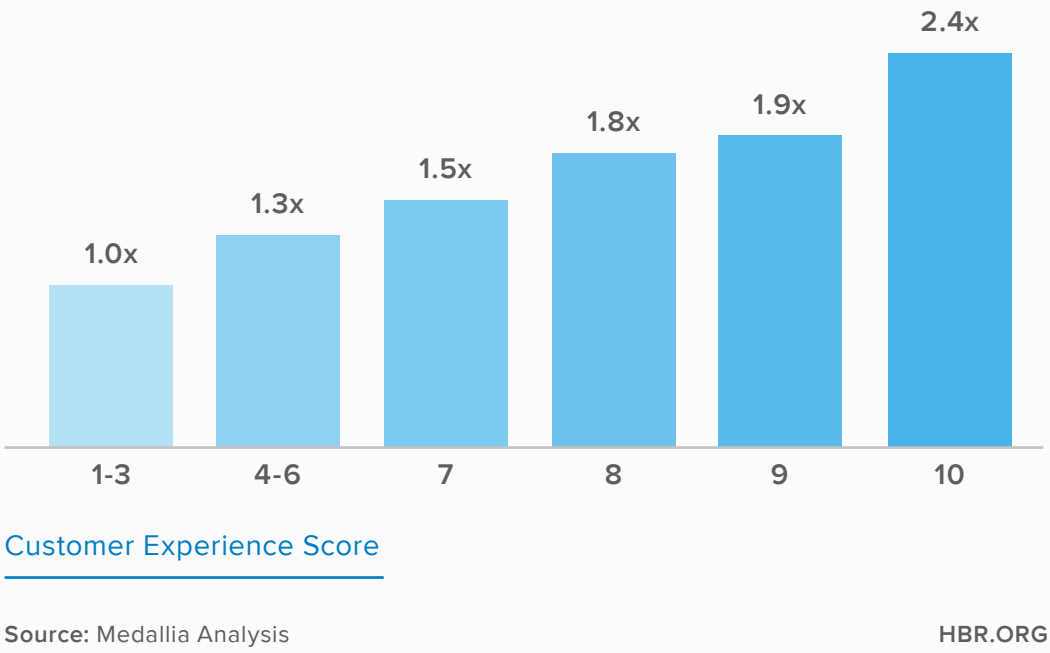
Important questions to ask

- With your platform, can we easily apply identity and access settings, policies, security, and governance across multiple groups in a unified interface?
- What is the extent of your support for external users or non-users?
- Will different user types require separate platforms, resources, dev pipelines, skills, policies, governance, or control resources?

Does the IAM solution give both developers and end users a truly **frictionless experience?**

Customer Experience Drives Sales

In a transaction-based business, sales are driven by good customer experience.



Source: Medallia Analysis

HBR.ORG

Unfortunately, the user experience surrounding identity is often overlooked. Many IT and security teams uncover frustrating UX shortcomings once their IAM solution is deployed in the real world.

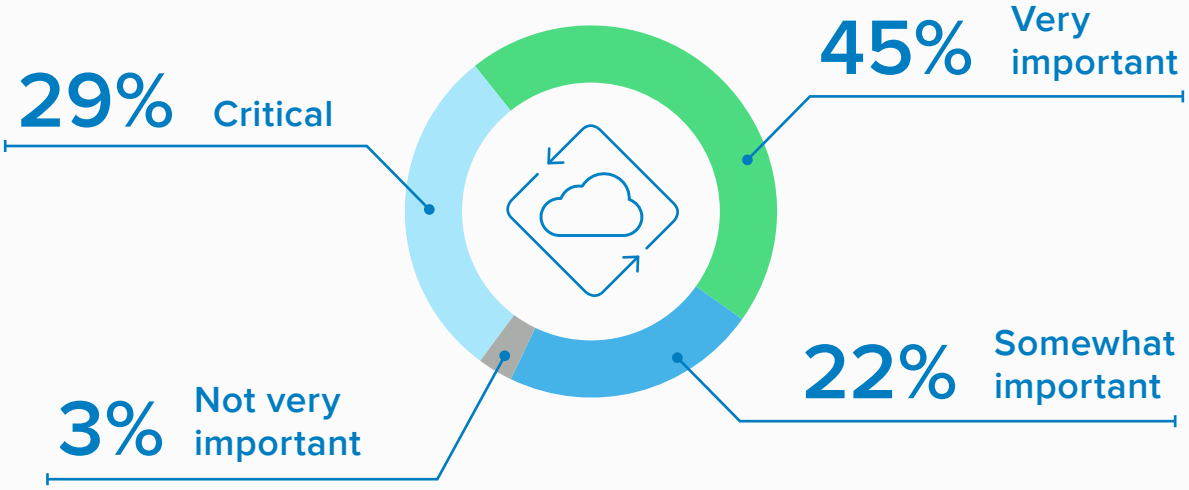
Important questions to ask

- Does the IAM platform minimize friction through streamlined workflows for developers and administrators who have to deploy it and manage policies, etc.?
- Does it make MFA intuitive for end users, or add frustration and extra steps with a disjointed experience across different device types?
- Does it provide a neutral platform that works seamlessly with all best-of-breed apps (not just the vendor's own software) to ease our journey to the cloud, no matter where it takes us?

Does the platform free up resources to accelerate business initiatives?

3/4 of organizations consider IAM highly important to enabling digital business initiatives

Importance of IAM in Relation to Digital Business Initiatives



Without visibility and control across business-to-employee, business-to-business, and business-to-consumer user profiles or access points, it can be challenging for the business to identify opportunities for workforce productivity improvements, new revenue models, or potential service offerings. Evaluate whether your IAM platform offers the agility you need to speed up your journey to the cloud, differentiate your customer experience, and ensure efficient merger and acquisition transitions.

Does the platform free up resources to accelerate business initiatives?

Important questions to ask

- Will your platform require added resources to manage complexity in the form of multiple ADs, domains, HR systems, deployments across regions, or other tricky scenarios?
- Can the solution help us unify multiple identity providers to streamline our environment and move to the cloud?
- Does the IAM platform offer capabilities that accelerate time-to-value, such as no code (or low code) workflows, deep provisioning and HR-as-a-Master integrations, or customization tools for customer portals and mobile apps?
- How quickly will your CIAM offering enable us to deliver our next digital initiative?
- Does it enable custom login URLs and support adaptive MFA to give our customers a tailored, secure experience?
- How does your CIAM approach free up developers from granular identity tasks?

That ability for our developers not to think about identity management databases, rules, permissions, and all those things that come with legacy identity management platforms—that, from a developer perspective, has been a major unlock for getting applications out the door faster.

–Cody Sanford
CIO, T-Mobile

Why Companies Trust the Okta Identity Cloud

Here at Okta, identity is our sole focus. We think about complex identity challenges in a modern way because we know how critical it is to your work. Smart IT and security teams leverage our cloud-first identity platform to support all of their identity needs—from core MFA deployments to API gateway integrations, custom scopes, dynamic client registration, spec-compliant OIDC, auth server discovery, and token introspect.

In addition to a unified directory with seamless single sign-on and MFA experiences, the Okta Identity Cloud's powerful capabilities include:

Okta Workflows

Automate complex identity-centric processes without code, using our graphical interface and library of connectors to make processes, like deprovisioning a user and transferring their files, simple.

Okta Advanced Server Access

Extend secure privileged access to your cloud-native infrastructure for elegant zero trust support. Automate the lifecycle of server accounts and policies across a dynamic fleet of infrastructure at any scale.

Okta Access Gateway

Secure access to on-prem apps and protect your hybrid cloud—without changing how your apps work today.

Our entire organization is built to help meet customers' identity needs, so you can navigate your most complex and difficult use cases with rapid, expert support. Don't rely on a vendor that makes your work harder, not easier. Visit www.okta.com to learn more about the Okta Identity Cloud.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 8,400 organizations, including JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.

Learn more at: www.okta.com