Not All Identity Clouds are Created Equal

Review the benefits of Okta's independent, future-proof identity

okta

Index

The evolution of identity and access management

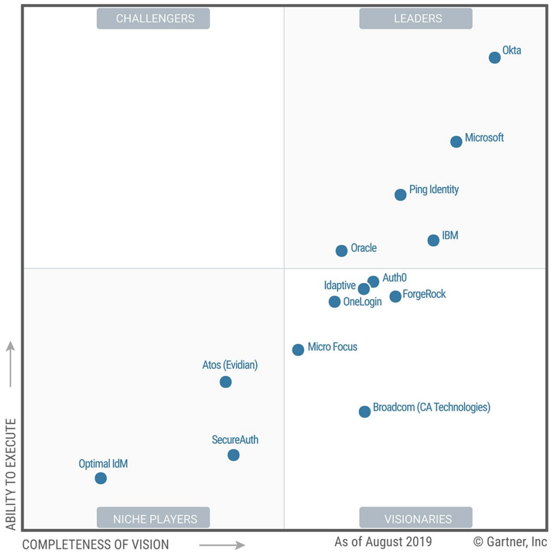
Microsoft's Active Directory (AD) was born back in 1999, initially providing companies a means to track and secure employees and IT resources in mostly homogenous, closed-network environments. As a result of legacy lock-in, AD is still used widely today, even though it fails to meet several needs of modern organizations, such as:

- Adopting best-of-breed cloud technology and bring-your-own-device (BYOD) policies
- Securing a remote workforce while increasing productivity
- Enabling trusted access for external users like partners, customers, and contractors

Over the past two decades, new cloud-first identity and access management platforms, also known as identity as a service or IDaaS, emerged specifically to meet these needs. In response, Microsoft began shifting its AD capabilities to the cloud with a product called Azure AD. However, Azure AD still has a long way to go before it can fully support the modern requirements mentioned above, especially when it comes to managing external users, non-Microsoft apps, or devices. That said, according to industry analysts like Gartner, Microsoft and Okta are now at the head of the pack as the two most prevalent providers in the identity space.

Given identity's cornerstone role in mitigating the current threat landscape, many enterprises looking to modernize and protect against data breaches find themselves deciding between these two options. Below, we'll sum up top considerations for CIOs across three important criteria: identity and access management capabilities, security, and resource drain.

Figure 1. Magic Quadrant for Access Management



Source: Gartner (August 2019)

Gartner
Magic Quadrant for Access Management

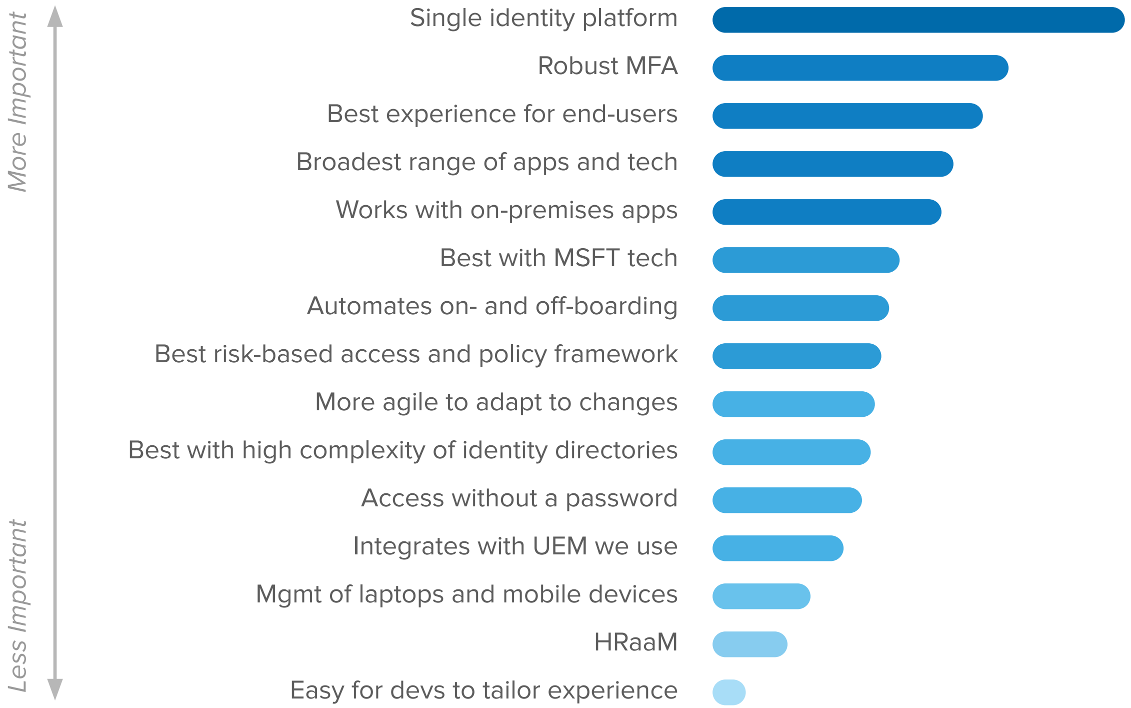
Gartner's 2019 "Magic Quadrant for Access Management" placed Okta and Microsoft as the top leaders based on both ability to execute and completeness of vision.

Gartner's most recent "Critical Capabilities for Access Management" report rated Okta's product scores the highest amongst workforce, partner, and customer use cases, while Microsoft's solutions came in 4th, 8th, and 8th, respectively.

Evaluating identity and access management (IAM) on core capabilities

In terms of core functionality, there are a few primary areas where the top two solutions differ. To identify these areas, Okta worked with a third-party research organization to survey 200 identity and access management leaders who had recently purchased and identity and access management (IAM) solution for an enterprise organization. First, Okta wanted to understand what capabilities mattered most in a purchasing decision. Not surprisingly, the IAM leaders ranked a single identity platform, robust MFA, and end user experience as the three most important capabilities for an identity solution.

Attributes rated most highly for importance in vendor selection (Indexed to top-ranked attribute)

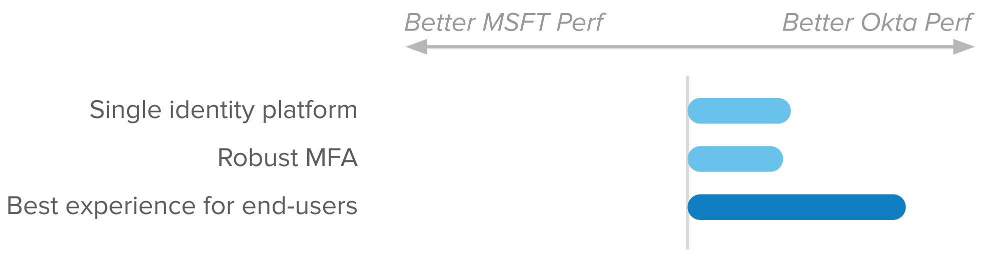


Okta, Enterprise IAM Buyer Survey, 2019

Next, Okta wanted to understand how well its own products compared for each of these important capabilities.

The results, outlined below, mirror Okta's ranking in the Gartner Magic Quadrant and Critical Capabilities research. As you can see, the IAM buyers who evaluated both Okta and Microsoft AAD ranked Okta's performance higher across each of these top three capabilities.

Relative performance of Okta vs. Microsoft performance on top three capabilities



Okta, Enterprise IAM Buyer Survey, 2019

In the following three subsections, we'll dig into each provider's strengths in these key areas.

Single, unified identity platform

According to our research, a single identity system of record for all user types—employees, customers, partners, and contractors—and all resource types—apps, APIs, and infrastructure—is the single most important capability of an IAM solution. That's because having one platform as a foundation for every identity scenario drives efficiencies to help you speed time to value, gain agility, and stay responsive to your users' needs. Specifically, security and IT teams benefit from a single pane of glass where they can easily apply, view, and manage settings, policies, security, and governance across the board, no matter which identity use case they start with. With visibility and control across all identities in one place, CIOs gain insights that can accelerate the adoption of evolving business models and new revenue channels.

Most identity providers have focused development efforts on employee use cases, and perhaps dabbled in a few limited use cases for partner scenarios, but neglected customer requirements.

When it comes to customer identity and access management (CIAM), which is increasingly crucial in the digital transformation age, consider whether your provider truly offers an integrated platform built with an identity-first philosophy, as opposed to an organization-centric or employee-centric approach. The reality is that Azure AD's B2C solution only supports single-app external use cases, does not integrate or federate with the Azure AD workforce solution, and offers only limited customization capabilities. Okta, on the other hand, provides a single identity platform and can accomodate increasingly complex use cases where the lines between user types blur. For example, employees that are also customers or partners that need access to external custom portals and internal applications.

On the other hand, when you need to provide partners and contractors with guest access to critical systems, like supply chain or customer relationship tools, other variables impact security and the user experience. It's better for partner users to connect via their own identity platform as opposed to creating new, difficult-to-remember credentials for your systems or logging in with their personal email addresses. This ensures the directory housing partners remains up to date, so your IT team can easily control provisioning and deprovisioning when employees leave a partner organization.

As the majority of organizations are now technology companies and are developing software in some capacity, it's also important for an identity system to secure all development resources equally, including infrastructure from cloud platforms other than Azure. That's why Okta's Advanced Server Access extends core Okta capabilities to Amazon Web Services, the Google Cloud Platform, Azure, or on-premises servers to easily maintain Zero Trust access policies.

Will your IDaaS support your future identity needs?

To determine if your vendor can support evolving, multi-dimensional identity needs, ask the following:

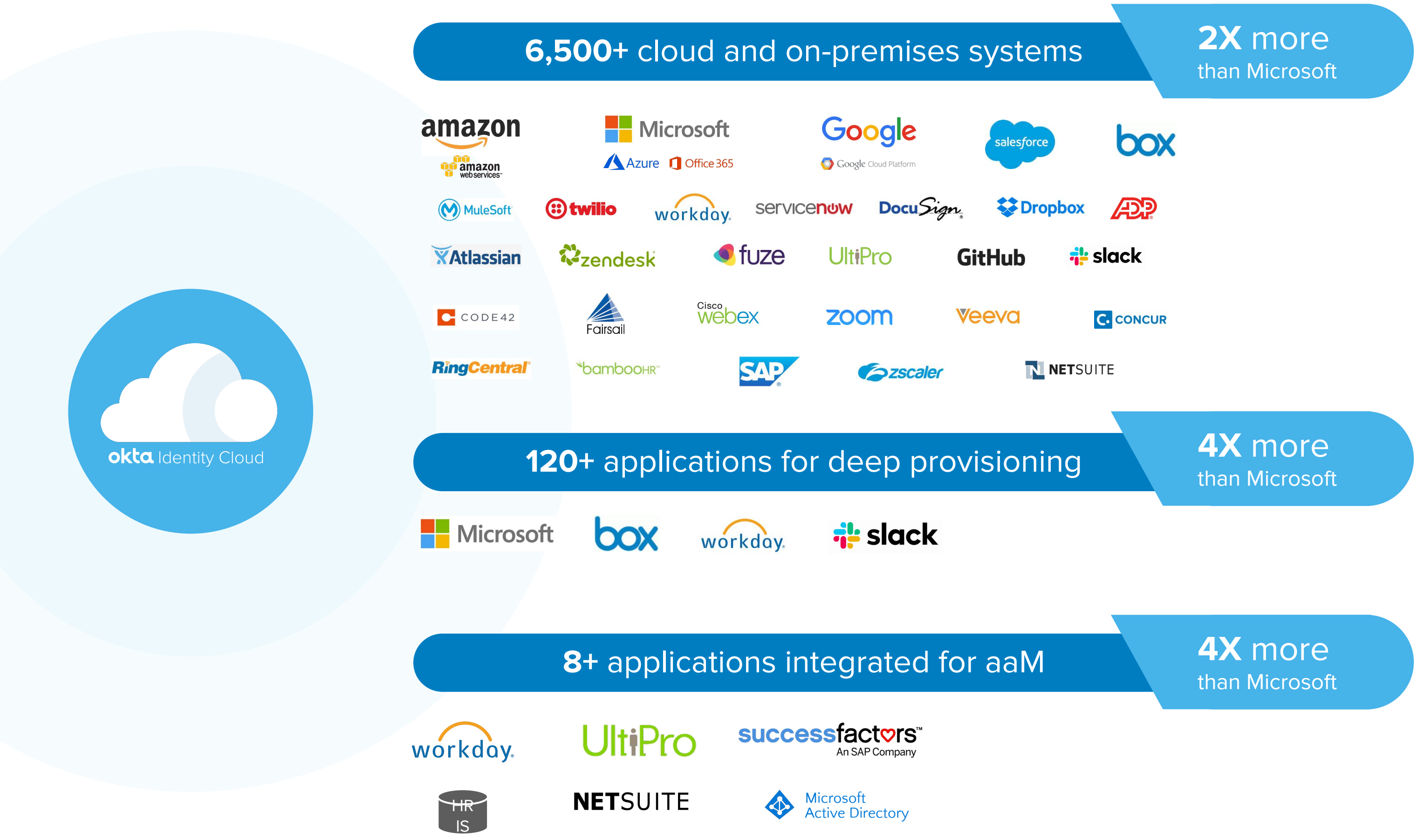
- Will you need separate identity solutions with different capabilities, architectures, policy management and identity directories to effectively support employees, customers, and partners?
- Do these multiple solutions result in identity duplication and a greater admin burden?
- How many validated customer references does the vendor have for each user type?
- Does the CIAM offering provide out-of-the-box integrations and developer tools to support customer identity use cases?
- Will your solution allow you to federate partner identity sources, or does it require your team to maintain partner identities?
- Does the solution have appropriate partner controls in place; like limiting the use of personal email address or limiting identities to approved partner domains?
- Can you easily provision or deprovision access for a partners' employees?
- Is the provider investing the same amount of R&D into partner and customer identity use cases as they are into workforce identity?

Frictionless user experience

As CIOs continuously push their teams to become business enablers, they want to provide end users with an experience that balances security with usability and workforce productivity—regardless of an employee's location, resource, or device. Since the average enterprise now uses hundreds of different business apps from a variety of vendors and platforms, this starts with providing extensibility to manage identity across a wide variety of applications and infrastructure.

The Okta Integration Network consistently tops the pace and depth at which SAML/SCIM integrations are developed. Today, Okta offers pre-built integrations with twice as many cloud and on-prem systems, four times as many applications for deep provisioning, and four times as many human resources platforms for employee master records.

Okta's integration network outperforms Microsoft AAD's


6,500+ cloud and on-premises systems — 2X more than Microsoft

120+ applications for deep provisioning — 4X more than Microsoft

8+ applications integrated for aaM — 4X more than Microsoft

Your identity platform should enable a broad range of technology choices, so users can work with whichever apps they prefer—all through a single dashboard that's as frictionless as possible. Make sure it will provide a seamless, simple end-user experience, even in heterogeneous device environments that might include Apple, Microsoft, and Google. Your platform should also support passwordless access with a wide variety of authentication factors to choose from.

In addition, look for a solution that minimizes administrator headaches during identity and access management platform deployment. Okta customers find relief from overly complex admin interfaces and limited prebuilt integrations. This leads to high-friction rollouts and slow adoption that can delay the valuable benefits of modern identity.

> *"Microsoft gives you the capability to do a lot of things—but not easily. We needed to get away from doing those same mundane tasks, and get our people educated in an application that they could pick up quickly and start doing more with."*
>
> — Willie Clemons, Director of Identity and Access Management, EBSCO Industries, Inc.

Does your platform support a best-of-breed strategy?

Many organizations opt for best-of-breed technologies over bundled solutions because they make their workforce more productive through a drastically better user experience. Even if you lean toward a single vendor today, consider the future of your IT environment, and ask yourself:

- Do we use best-of-breed solutions for productivity and business applications today?
- Which security vendors are we using outside the Microsoft stack? (e.g., Proofpoint, Mimecast, Symantec, Netskope, McAfee, Ciphercloud, Splunk, Crowdstrike, VMware, MobileIron)
- In the next 10 years, do we see our organization using non-Microsoft products?
- Does the identity platform we're evaluating offer a connector for our HR system of choice?
    - If so, how frequently and effortlessly does it sync the data between the two platforms?
    - Can it use the HRIS as a master and ensure day-one access for new employees, and immediate deprovisioning for terminated employees?

Robust multi-factor authentication

Beyond the underlying attributes of flexibility and ease of use, you'll need an identity platform that includes adaptive, robust multi-factor authentication (MFA) with intelligent policies based on login context. When evaluating MFA capabilities, it's helpful to review the various factors and sequencing configurations each vendor offers. Look at their track record of supporting emerging factor types as the security landscape has evolved, and ensure the solution's factor sequencing options are comprehensive enough to meet your organization's current and future needs.

Be sure to review the historical reliability of each MFA solution you evaluate, since a single MFA outage can impact access to all of your mission-critical business systems. Even "modernized" platforms like Azure AD often still rely on antiquated architectures susceptible to cascading outages like those Microsoft suffered in the past few years. It's helpful to look at the root cause analysis reports from a provider's recent incidents, and question whether their solution contains legacy components, such as domain controllers, that cause unnecessary vulnerabilities.

In order to maintain the best possible security posture in a BYOD (bring your own device) environment, your vendor should also work with a range of partners for device trust or any other advanced security requirements. For example, Okta integrates with industry-leading mobile device management (MDM) and enterprise mobility management (EMM) technologies (such as VMware AirWatch), any SAML or WS-Fed approach, as well as other best-of-breed security technologies (like Proofpoint, Netskope, Phantom, and SailPoint). This means Okta's adaptive MFA solution is able to collect valuable real-time risk signals from a wide variety of sources. Meanwhile, Microsoft's contextual access is optimized to work best with their proprietary InTune and Office 365 solutions, which limits customers who prefer other best-of-breed or productivity apps.

How comprehensive is your vendor's MFA?

- Do you check contextual risk factors pre-authentication or post-authentication?
- How many false positives does your system trigger?
- How do you prevent brute force attacks?
- Are risk factors analyzed in real-time to avoid latencies?
- Do geolocation policies work down to the state and region-level, or do they allow only country-level access management?
- How easy is it for admins to tailor and manage these adaptive MFA policies?

As noted above, enterprises tell us that having robust MFA is one of their top two identity priorities. Given this, you should find out whether your vendor's MFA policies are granular enough to set all the controls you'll need to block bad actors, without inadvertently locking actual users out of their accounts. Okta uses real-time intelligence to gain an instant, holistic view of the context behind each login across all of your best-in-breed applications. In particular, Okta's ThreatInsight solution analyzes risk pre-authentication to differentiate valid users based on more than just their IP address, which helps protect against account takeovers.

Never compromise on trust

Since identity is the lynchpin to protecting your business' data, there are other crucial considerations CIOs should think about as well. Any security breach or identity downtime can have a devastating effect on your business—including drops in workforce productivity, customer trust, and sales. Okta is solely focused on identity and committed to protecting customers no matter what technology stack they choose (e.g., AWS, Box, Proofpoint, Netskope, Slack, Zoom, Splunk, etc.).

Before you turn over the keys to your kingdom, it's also important to compare each vendor's overall transparency, security, reliability, and privacy to make sure you can trust them with this mission-critical part of your IT stack.

Pillars of trusted identity

Transparency

Trust starts with transparency. It's hard to know whether you can trust your provider if they don't offer public resources detailing their security, reliability, or scalability efforts.

Reliability

There's never a good time for your identity service to go down, so the solution should be built and operated with the expectation that it must always stay on no matter what occurs behind the scenes. Expect high resiliency and zero downtime.

Security

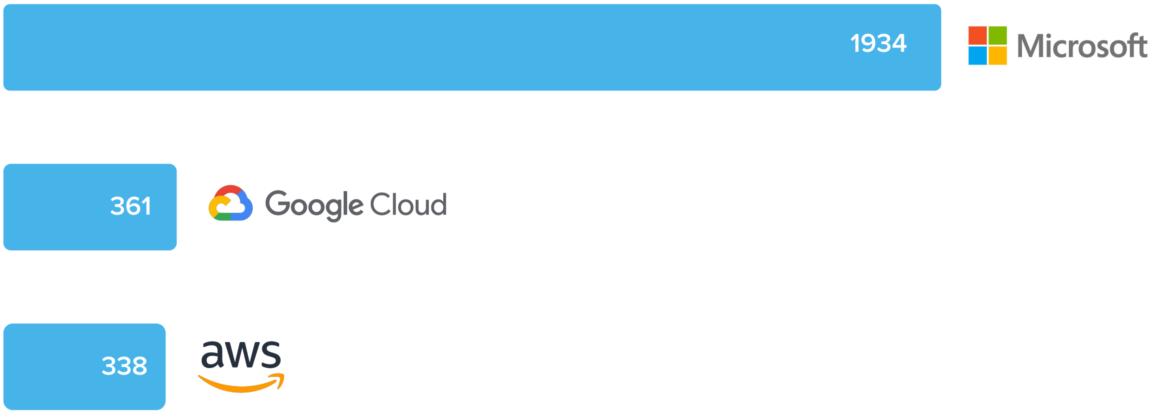
Your identity vendor's security measures should be far-reaching, but pay special attention to their data cryptography practices, credential hashing, Zero Trust guidance, and software development lifecycle practices. Demand mature integrations with best-of-breed security technologies vs. an internal stack of second-tier security tools.

Privacy and compliance

When evaluating an identity solution, check that it's routinely audited and has achieved certifications from trusted, independent firms. You want a platform designed to meet the rigorous requirements of even the most privacy-sensitive organizations and industries.

The infrastructure reliability of your identity service is arguably just as important as its security posture. Unfortunately, it's difficult to compare apples-to-apples, since each cloud vendor takes a slightly different approach to quantifying and reporting outage data. One third-party analyst found that, even after under-reporting outage time, Microsoft Azure (the platform that runs Azure AD) had 5X more self-reported downtime hours than Google or AWS over a recent 18-month period.

Total Reported Downtime (hours) 2018-2019



Source: ZK Research

Watch out for resource drain with “free” bundle add-ons

Azure AD is regularly included with Microsoft’s enterprise bundles, so at first glance it usually appears less expensive than best-of-breed identity alternatives. But it’s crucial for CIOs to think through all the hard and soft costs that come along with the drawbacks described above. Consider the impact of an unpredictable total cost of ownership (TCO) that includes extra spend on hybrid infrastructure, custom development, integration, deployment, service operations, manual administration, and consulting support—let alone the opportunity costs of spending your resources on these tasks.

Beware these common traps that many companies forget when opting for a bundled option:

1. You pay for things you don’t need.
2. You pay for things you’ll never use.
3. You sacrifice end user experience, productivity, and collaboration by opting for “good enough” rather than best-of-breed.
4. You end up having to upgrade to increasingly expensive tiers, because what once was free gets changed to premium pricing.
5. You lock your organization into the bundles’ ecosystem as these vendors are not incentivized to prioritize best-of-breed.

Hybrid IT requirements

In our survey, 90% of recent Azure AD buyers purchased it in conjunction with at least one or two other Microsoft identity products. Depending on your IT environment, if you choose Azure AD, you might need to maintain AD for on-prem access management, or supplement it with add-ons like Microsoft Identity Manager (MIM) for on-prem provisioning or the Azure App Proxy for access to legacy resources.

MIM requires significant hours of professional services work to get operational, delaying time-to-value. Microsoft’s App Proxy only works out-of-the-box with a small percentage of applications, while it requires source code changes to work with most apps (especially those that are more complex, yet very common like Peoplesoft or the Oracle e-Business Suite). It also lacks key capabilities such as URL authorization, app templates, and error handling.

Sinca Azure AD doesn't support header-based applications, you may need to deploy a partner solution, like Ping Identity, if that is a requirement for your ecosystem. Okta Identity Cloud includes our Access Gateway solution, which allows companies to secure their on-premises apps without any changes to how the apps work. CIOs should closely review all of their applications to confirm whether their identity platform can support them natively with future-proof, secure access management that covers all apps, regardless of where they're hosted. Otherwise, you may end up having to purchase a pricey web access management (WAM) solution on top of your primary identity system.

The customization burden

If securing customer identities and access is important for your organization (or may be in the future), look closely at each identity CIAM solution and make sure the solution you choose allows the level of customization you need. With Azure B2C, your developers will be faced with a demanding learning curve, and even Microsoft acknowledges that its "custom policy editing" is not for everyone".

> *"Custom policy editing is not for everyone. The learning curve is demanding, the startup time is longer, and future changes to custom policies will require similar expertise to maintain."*
>
> — Microsoft Documentation

This delays time to value, and means future changes to custom policies require expertise to maintain. While basic authentication and SMS two-factor authentication might be simple enough to configure with Azure B2C, other factors or authentication policies require custom code to be written, deployed, and managed without an admin-friendly interface.

Azure AD's B2C solution limits developer's control over certain customization components including the URL, federation options, and programming languages that can be used with it. By comparison, Okta provides out-of-the-box integrations and developer tools, strong documentation and SDKs supporting over a dozen development languages, centralized administration for all user types, and reusable components like our sign-in widget. In general, Microsoft's complex infrastructure often requires additional resources to manage, which leads to 3-5x higher TCO than companies experience with Okta.

Be sure you're aware of all the hardware components your implementation could potentially need, how much developer time and effort it will take to stand up the solutions, as well as the operations costs for ongoing maintenance.

How easily does your platform's CIAM solution support custom needs?

- Supports all the environments and frameworks your developers prefer, or boxes you into a few ridgid tools?
- Allows customization, such as custom domains or login experiences, user consent, or provisioning integrations?
- Enables custom authorization flows without requiring AD integration or client access licenses (CALs)?
- Separates the infrastructure and development environments for workforce and customer identity platforms, requiring even more customization work if you need more than their default flows?

Future-proof with the emerging identity standard

When thinking about how long they've already had AD in their organization, most CIOs recognize that careful consideration surrounding any changes to identity and access management is paramount. Moving to a modern identity-as-a-service (IDaaS) platform is a rare opportunity, and it's a choice that will likely last your company at least 10 years. That's why, rather than just "lifting-and-shifting" to the cloud, you'll want to be confident that the identity solution you select today will keep up with your technology needs into the future.

Identity is Okta's entire focus as a company, not just a means to support other revenue-generating platforms. On the other hand, Microsoft's resources are spread across a myriad of solutions, including their most recent addition—Microsoft Dynamics 365 HR. Which integration do you think they'll invest more deeply in: their Azure AD connector for Workday or the connector for their own HR system? Most teams want to adopt at least some non-Microsoft business and security apps, and many have even found that Okta works just as seamlessly with Microsoft solutions like O365 (it's actually the most popular app amongst our customer base). Okta has always been vendor-neutral, so you're free to use the best technology for your organization, whatever that may be.

Looking ahead, it's worth noting Okta is laser-focused on creating a robust identity-centric platform that's sophisticated and flexible enough to meet any real-world need. Even if you're a committed Microsoft shop, there are many reasons to avoid the lure of simply jumping over to Azure AD to maintain your status quo. Otherwise, why would only 22% of companies with access to "free" Azure AD Premium (via an existing Microsoft bundle) end up selecting Azure AD as their identity platform?

To learn more about how to replace Active Directory with the leading cloud identity platform, visit okta.com/rethinkad.