5 Ways Smart Executives Capture Value with Modern Identity

As a strategic and critical control point, identity is the gateway to everyone and everything in your organization. A modern approach to identity and access management (IAM) can help grow your business by redirecting IT and development effort towards innovation, new business models, and competitive differentiation. However, there are a variety of IAM platforms on the market. How do you know you have the right one to future-proof your business?
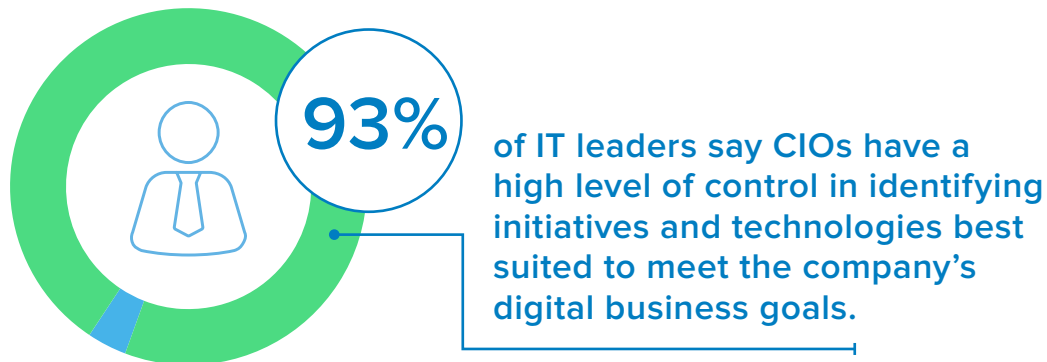
5 key reasons to embrace modern IAM

While sticking with the status quo or adopting a "free" solution from your enterprise IT bundle might feel like the path of least resistance, there are many trade-offs that today's technology leaders must consider. In most cases, the hidden costs of doing nothing are much greater than you think. These come in the form of lost productivity, increased security risk, and a diminished customer or employee experience.

It increases agility to accelerate business initiatives

IAM is a crucial enabler for core business events, such as mergers and acquisitions, entering new markets, and disrupting your competition. The platform you use is either a barrier that slows down these important initiatives, or it can act as an accelerant. Don't be held back by tedious domain consolidation projects or inflexible customer authentication and authorization.

93%

of IT leaders say CIOs have a high level of control in identifying initiatives and technologies best suited to meet the company's digital business goals.

You need an IAM solution your team can deploy in weeks, not months, so they can transform employee and customer experiences in months, not years. To do so, choose an identity platform that enables your IT administrators and app developers to manage all related tasks with peak efficiency and security. IAM should help your team:

| Roll out new apps fast | Protect server access | Quickly implement MFA in front of your most critical resources |

For example, T-Mobile embraced Okta's cloud-native approach as part of a technology transformation so it could move at the speed of customer expectations and improve security.

"

That ability for our developers to be able to hand off identity management to the experts would be a major unlock for getting applications out the door faster," said Cody Sanford, CIO at T-Mobile. "Time-to-market was a security risk. The longer it took for us to onboard applications, the more people looked for alternate solutions. They created their own siloed credential stores, so we couldn't monitor things or apply policies holistically," added Kris Wilson, senior director, product and technology at T-Mobile.

It manages all identities in one platform

Enterprises today must manage identities for a variety of user types—their employees, partners, and customers—across multiple internal and external apps and resources. This creates unprecedented complexity, since trying to wrangle access management across multiple different platforms, resources, dev pipelines, skillsets, policies, governance, and control resources can quickly become unwieldy for your team.

Your platform should provide a single, simplified management console that:

- Automates the administration of partner and customer identities
- Offers a centralized view of all users and resources in one pane
- Unifies security policies and management across the entire organization

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.

At The Church of Jesus Christ of Latter-Day Saints (LDS), the Okta Identity Cloud easily solved this challenge, as noted by Ben Hutchins, identity program manager. He shared, "We have many different types of audiences, but from an identity standpoint, we don't separate B2B, B2C, or B2E. We simply have one registration process where people can create an account and then based on their role (whether they're a student, staff, volunteer, or missionary), their access rights change. We have very robust, dynamic role-based access management."

It relieves IT headaches with a modern architecture

It's critical to avoid IAM platforms that still carry significant technical debt and force you to rely on brittle legacy and on-prem components even as they claim they've shifted to the cloud. Consider your provider's track record around vulnerability issues, outages, and downtime, and ensure your platform is architected for the cloud from the ground up. What methods do they have in place to guarantee superior availability, scalability, burstability, performance, and uptime? For instance, does the IAM solution maintain 99.999% availability?

If you're managing a hybrid IT environment like most companies, it's also a good idea to review your vendor's approach to on-prem access management. Make sure they can truly protect your hybrid cloud, servers, and header-based applications without requiring you to change how your apps work today.

"

Our previous infrastructure was very hard to maintain. We've deprecated or eliminated a lot of systems with Okta in place. Namely, we've been able to remove Azure AD, our integration with ADFS, and our internal LDAP solution. Now we have one platform to support instead of many."
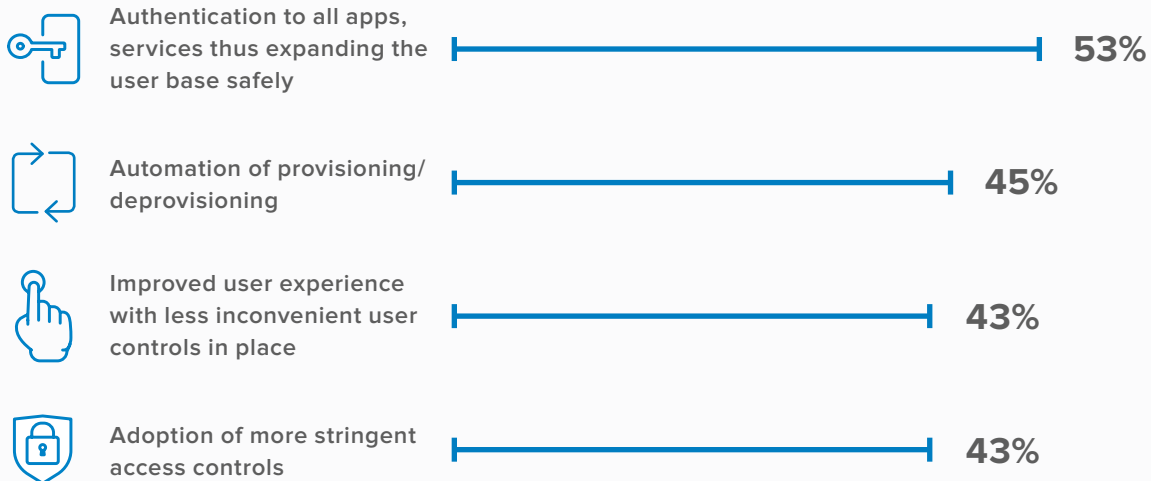
–Brad Burton
Director of IT, Cypress

It is built with an unconflicted, security-first mindset

Watch out for providers that don't prioritize security because they're distracted by thousands of other use cases across their product portfolio. Consider whether the IAM platform limits choice by locking you into one vendor's internal security stack, as opposed to helping you integrate with best-of-breed security vendors like Proofpoint, Netskope, and Crowdstrike to ensure the strongest security posture.

Addressing Security Concerns: Most Important Potential Benefits of IAM Solutions

Authentication to all apps, services thus expanding the user base safely — **53%**

Automation of provisioning/ deprovisioning — **45%**

Improved user experience with less inconvenient user controls in place — **43%**

Adoption of more stringent access controls — **43%**

*Research from IDG

In particular, don't forget that multi-factor authentication (MFA) shortcomings can lead to phishing attacks, insider data breaches, account compromises, and other threats. Of course, lack of advanced, adaptive MFA also delays your zero trust efforts, so it's useful to specifically evaluate the platform's MFA capabilities and adoption rates.

"

At energy technology company Baker Hughes, this became a particular concern. "When our infrastructure team was doing some experiments with Office 365, they were using the native tools for MFA, and they actually were compromised—so it was really clear that we needed to move to Okta as quickly as possible," remembers Keith Herdon, Baker Hughes' CISO.

Finally, be sure your IAM platform minimizes friction for all users—from your employees and customers, to your IT admins, developers, and security—through intuitive, modern design and a centralized admin experience. Rather than make end users and admins jump through hurdles to utilize MFA factors or customize policies, the software should be easy to use and support codeless workflows that automate as many identity tasks as possible.

Customer Experience Drives Sales

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

Annual Revenue Increase per Customer

Customer Experience Score	Revenue Increase
1-3	1.0x
4-6	1.3x
7	1.5x
8	1.8x
9	1.9x
10	2.4x
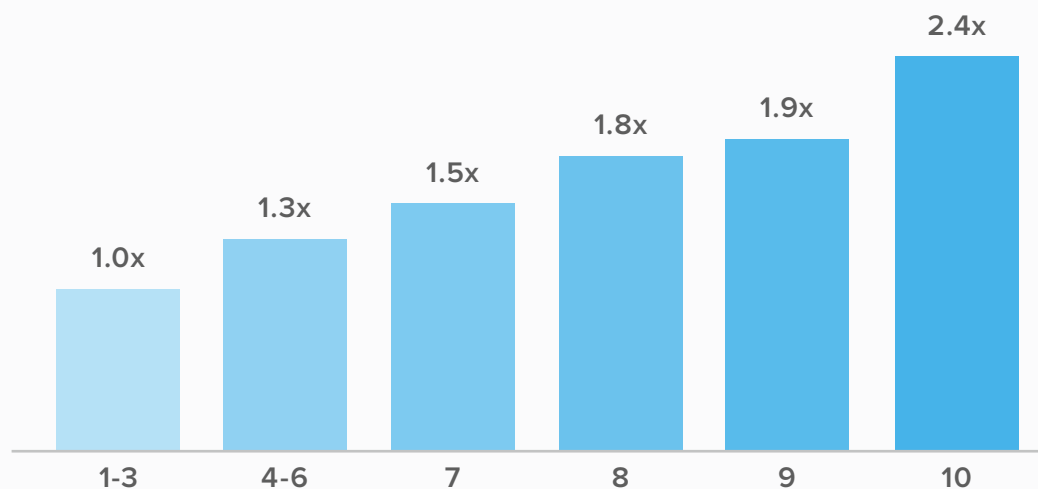
Source: Medallia Analysis

HBR.ORG

It should help your business:

- Drive adoption for best-of-breed apps and advanced technologies
- Retain current on-prem technology as long as you need to
- Future-proof for whatever your stakeholders need down the line

The LDS Church chose Okta as its IAM solution primarily on these grounds. Hutchins noted, "The predominant reasons we went down the path of Okta were that they just provided a better user experience...and less custom work on our side to make the full integration work."

3 IAM use cases that maximize value

With Okta's robust, modern identity cloud, forward-thinking organizations like T-Mobile, Baker Hughes, the LDS Church, and many others minimize their IT costs and speed time-to-value. Okta helps them simplify their existing infrastructure, reduce their reliance on legacy systems, and avoid unnecessary overhead.

High-value use cases include:

- Lower M&A Costs: Okta customers avoid AD consolidations by an average of 25-75%.

- Faster O365 Deployments: Okta shortens large-scale deployments of Office 365 from over 6 months to under 4 weeks.

- 360° View of All Users: Okta's centralized admin console can save 4-16 months of delayed deployments for all users (employees, partners, customers).

"

We had about 17,000 of our staff on Office 365, and over a weekend, we moved it to Okta. On Monday morning, we literally had only 12 phone calls from our help desk asking questions around authorization and authentication, so it was amazing."

–Keith Herdon
CISO, Baker Hughes

Trust Okta with Your Identity Requirements

Since our founding, Okta has been 100% focused on solving complex identity challenges with a modern cloud-first philosophy. Over the past decade, we've addressed many of the greatest complexities of IAM, such as securing access to dynamic infrastructure, delivering a consistent access experience for all applications from cloud to ground, and enabling M&A agility.

Our entire organization is built to help meet customers' identity needs, and to navigate your most complex and difficult use cases with rapid, expert support. We support a variety of critical requirements, such as:

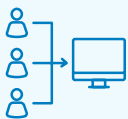A universal identity platform for employees, partners, and customers

Contextual authorization policies using device information from best-of-breed MDM

Multi-domain Active Directory environments

Secure access to ynamic infrastructure

Multi-tenant Office 365 collaboration

M&A time-to-value, agility, and collaboration

Don't fall into the trap of working with a vendor whose incentives aren't aligned with your IT strategies. Visit www.okta.com to learn more about how the Okta Identity Cloud can meet your needs.

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