Whitepaper

September 2021

The CIO’s Guide to Identity-Driven Innovation

Modern Identity’s Role in the Future of IT

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871

Contents

The End of "Business as Usual" IT

Even before the pandemic came along, several technology and human behavior shifts led smart businesses to rethink their approach to IT. As the world became more digital, mobile, and cloud based, user expectations soared. At the same time, the proliferation of devices and applications increased the attack surface for bad actors, causing security debt to pile up.

Forward-thinking IT organizations know that providing secure, frictionless, and relevant experiences is no longer a nice-to-have, or even a competitive advantage for that matter. Top-notch digital experiences for customers, partners, and employees are now table stakes for any business. Of course, COVID-19 catalyzed this evolution overnight, speeding the digitization of customer interactions by 3-4 years on average[1] and increasing the long-term adoption of remote work by 4-5x[2].

Now, it's time for technology leaders to double-down on the numerous short-term IT wins they achieved during the pandemic, and focus on further modernizing IT for the long haul.

> "After pulling off what most considered the impossible, IT is now turning its eyes from the triage and stabilization of the disrupted enterprise towards recovery and enabling a new reality. In what promises to be a much more economically challenged, but digitally connected world, the CIO is facing a dilemma of how to deliver digitally native capabilities, while containing costs, skilling up and running lean."
>
> Steve Bates
> Global Lead, KPMG CIO Center of Excellence

[1] "**How COVID-19 has pushed companies over the technology tipping point**," McKinsey, Oct. 5, 2020

[2] "**The future of work after COVID-19**," McKinsey, February 18, 2021

As we put a tumultuous year in the rear-view mirror, many CIOs are looking for innovative ways to help their companies jump-start growth. They've quickly enabled product, marketing, and digital teams to implement new capabilities for telehealth, e-commerce, online citizen portals, and more—prompting end users to expect even more secure and seamless experiences. In fact, 17% of customers abandon transactions due to concerns about security[3] and 80% say they'd stop engaging with a company altogether if it experienced a breach[4].

Against this backdrop, IT organizations play a key role in building customer trust. They are increasingly accountable for more than just keeping the back-office lights on. They're now strategic enablers of the front office, tasked with finding new ways to empower the people they serve and generate business value.

Identity: A Hidden Differentiator

With every crisis comes opportunity, and today's technology leaders are perfectly poised to elevate IT's impact. In fact, 61% say their influence has increased as a result of the pandemic[5]. Yet identity and access management (IAM) is often overlooked when it comes to preparing IT for the future. This paper will explore how a modern identity infrastructure can support IT transformation that aligns with your company's growth goals.

But first, let's define what we mean when we talk about "identity." Historically, many used this term to refer to basic IT services—such as access controls and password resets, single sign-on (SSO), or user directories and authentication. But today, identity is much more than that. It has truly become the connective tissue for the digital economy.

Modern IAM enables all users to interact with businesses, technology, things, and other people in the most personalized and efficient way possible. By powering flexible access and protection across APIs, new sensors and devices (IoT), intelligent machines, and whatever comes next, identity is also a key lever for emerging revenue streams.

Four Ways Identity Can Fortify Your Business

Without a robust approach to identity management, it's impossible to secure anytime, anywhere access across your organization's infrastructure, applications, and people. In order to protect this wide variety of resources, you'll need more than just short-term band-aids. As you consider your long-term strategy, it's important to understand the role extensible, scalable identity plays in future-proofing IT.

[3] "**How Users Perceive Security During the Checkout Flow**," Baymard Institute, 2021
[4] "**Mind The Trust Gap**," Forbes, December 8, 2017
[5] "**Harvey Nash / KPMG CIO Survey 2020**," KPMG, September 22, 2020

Balancing Security & Usability

Enabling the massive jump in **remote, distributed work** has been top of mind for most CIOs over the past year. Companies made it easier and safer to work from anywhere, and remote collaboration grew 43X faster than expected[6]. Solutions like Okta protected many of these interactions, and we saw use of stronger forms of authentications—such as push notifications rather than security questions—jump 184%[7].

More companies are recognizing that the rise of remote work and cloud computing makes a traditional network perimeter-centric view of security obsolete. By implementing a robust "**zero trust**" strategy with identity at the core, you can ensure the right people have the right level of access to the right resources, in the right context. What's more, you can assess access levels continuously to deliver the holy grail of productivity and protection with the least friction possible.

However, many still assume that this security comes at the expense of usability, and vice versa. This myth can be especially problematic as IT teams look to build on their workforce success by enabling similar digital experiences for contractors, customers, citizens, and partners—who want every login and interaction to be as instantaneous as their favorite consumer app.

The good news is that during the pandemic, we saw the cream rise to the top. Businesses with great user experiences underpinned by modern identity solutions delivered highly secure, yet still frictionless, services for all types of virtual communications and transactions.

Smart CIOs are bridging the virtual and physical by building the right digital support structures to boost flexibility for all their audiences. This includes:

- Establishing a **single source of truth** for identity across the workforce and offering self-service support. This brings several benefits, such as making it easier for your HR team to hire and onboard people from all over the globe, and giving employees the freedom to safely work in the ways they want.
- Offering an **intuitive, customizable dashboard** that brings all the tools employees need together in one spot—increasing collaboration and productivity.
- Carefully triggering customer login and registration flows that bypass disruptive security techniques and instead **apply the right security at the right times** for a more **optimal customer experience**.

Identity management, when used in these ways, is not just a commoditized IT service for access grants and password resets. It's a critical Zero Trust control that will only rise in importance as everything gets more complex.

[6] "**How COVID-19 has pushed companies over the technology tipping point**," McKinsey, Oct. 5, 2020
[7] "**Businesses at Work report**," Okta, 2021

FedEx rolls out zero trust strategy in record time

As **FedEx** moved to enable remote work for office workers and adapt quickly to the growth in customer demand due to COVID-19, its IT team sped up their planned deployment of the Okta Identity Cloud. This allowed them to retire a “spaghetti” IAM infrastructure made up of several different legacy point solutions, which was adding friction for end users, as well as software developers who were supposed to be focusing on cloud-native IT renewal.

More than 85,000 team members were able to securely access the company’s VPN on the first day of work-from-home. Within 36 hours, FedEx also rolled out SSO and multi-factor authentication (MFA) so employees could access the over 250 cloud technologies they needed to be successful, such as Microsoft Office 365, ServiceNow, Zoom, and Salesforce. With this approach, the organization rapidly laid a solid foundation for Zero Trust in preparation for the future of dynamic work.

Trey Ray, cybersecurity manager at FedEx shared, “Zero Trust security at FedEx is really about doing user validation and marrying that up with device validation. Instead of using a username and password, we take that a step further and validate the user with push notification and device context. And then we use that to make a decision on how to tailor the sign-in experience when they log in to FedEx applications and resources.”

Establishing a Universal Control Plane

In most companies, the former model of centralized IT departments who purchase and maintain pricey software packages has been replaced by a decentralized approach. The average large organization now uses 175 apps[8], and that number is only growing with the consumerization of the enterprise. In many cases, CIOs still have to maintain critical legacy systems, while keeping up with the demands of this modern workforce, pressure to innovate, and reductions in budget and headcount. Thankfully, holistic identity management can provide an invaluable control plane to help you manage all of this.

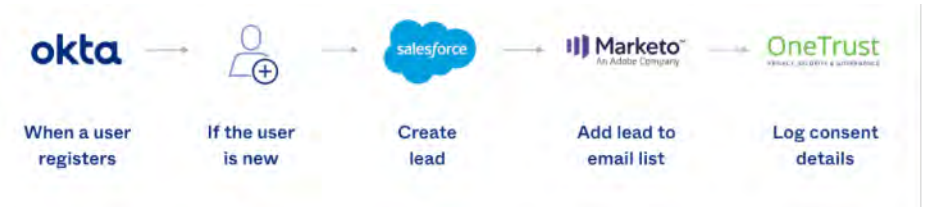
Streamline IT operations

Identity provides a common thread that ties the people, resources, and things in your organization together in a single view. If you’re looking to scale and adopt new cloud solutions, you can leverage an identity platform as part of that strategy and streamline previously manual IT tasks, like app provisioning and deprovisioning, syncing users between different systems in an organization, or managing end-to-end user and resource lifecycles.

[8] “**Businesses at Work report**,” Okta, 2021

If your identity platform offers self-service, no-code, or low-code customization options, your team can easily automate IT processes that span employees, customers, and partners, as well as applications, infrastructure, and IoT. As a result, they'll boost productivity, achieve operational efficiency and faster time-to-value, and mitigate common security risks associated with manual, error-prone processes.

Pro Tip: Using tools like Okta Workflows, teams can easily automate identity processes at scale—without writing code.



Extend cloud identity to on-prem resources

Identity's impact is greatest when it encompasses your cloud, on-premises, and hybrid environments. A modern identity approach ensures consistent access management across all of these resources—no matter where you are on your cloud migration journey. For the 89% of organizations[9] that still rely on at least some hybrid and on-premises infrastructure, cloud-based identity can help bring together these critical assets and protect your entire technology ecosystem more effectively and efficiently.

Consolidate IT systems where possible

Prior to the pandemic, CIOs noted that their expected timeline to migrate to the cloud was around 1.5 years, but the realities of a global pandemic shortened these cycles to just 23 days on average[10]. As you think about what will drive IT success (or slow you down) over the next ten years, it's a great time to capitalize on this progress and plan for future growth as opposed to current needs. Audit your tech stack and determine which assets you want to **retain, retire, or rethink** (see sidebar for popular strategies).

Since cloud-based identity increases the agility and flexibility of your infrastructure, it can be a valuable catalyst for your IT consolidation and modernization efforts. Establishing a unified identity layer across all your technology resources will help you maintain secure, simple access as the mix evolves.

[9] "**State of the Cloud Report**," Flexera, 2021

[10] "**How COVID-19 has pushed companies over the technology tipping point**," McKinsey, October 5, 2020

Pitfall of DIY AD/LDAP integrations

Take an inventory of all your most important systems. Determine how you'll enable and secure what will stay, rethink any systems that are holding you back, and retire what has lost value. Your identity approach can facilitate each of the following common cloud migration strategies:

Rehost. Often, technology teams employ a "lift-and-shift" to speed legacy migration. In this scenario, you're simply moving an application's workloads to run in the cloud without optimization.

Revise. For some apps, you might want to update certain components (i.e. load balancers, databases, certification management, or Zero Trust network access tools) by leveraging managed services while retaining the app's core source code.

How identity can help:

Protect against potential new vulnerabilities that can occur during the rehost/revise process by replacing on-prem identity components with cloud-native IT access management.

Re-architect. In this case, teams materially redesign an on-prem app's underlying architecture to fully embrace cloud-optimized techniques for scale, business continuity, performance, and time-to-market improvements.

Rebuild. This means starting over from scratch to re-code your highest priority business-critical systems. This allows you to write off technical debt and convert outdated tools into cloud-native applications.

How identity can help:

When breaking monolithic applications into APIs and microservices, a robust identity platform secures access to resources like APIs and cloud infrastructure. This enables seamless collaboration across operations, security, data science, and engineering.

Replace. For many older apps (whether commercial off-the-shelf or homegrown), your best bet is to replace them with cloud-first SaaS services.

Retain. There may be some on-prem applications in your digital portfolio that you need to leave as is—either for the short term until later phases of an overall app retirement strategy, or for the long term because it's a sensitive asset.

How identity can help:

- Modern identity can protect on-prem ERP, HRM systems, or middleware that you plan to retain, alongside new best-of-breed SaaS.
- By establishing a single source of IAM truth across the organization, you can easily replace, extend, and build on top of your tech stack as needed (this is especially helpful during M&A).
- If you swap out legacy or homegrown customer identity services with a cloud-based solution, you'll be able to link the user directory to your CRM for a 360-degree view.

Building Digital Trust

The pandemic proved that accelerating digitization was not only feasible, but essential. 69% of companies accelerated online business initiatives in the wake of COVID-19[11], and digital solutions for employees and customers alike now top the CIO agenda. As the speed of app development increases, IT can deliver core underlying capabilities that help digital teams scale their portfolio.

That’s key, since 86% of companies say the customer experience (CX) will be their main competitive differentiator by 2021[12]. Earning and maintaining trust during people’s interactions with your brand is especially critical following a year when more than 40% of organizations experienced increased spear phishing and malware attacks[13]. In order to preserve customer loyalty, your digital experiences must be not only secure, but frictionless, personalized, and relevant.

Here are some specific best practices CIOs can employ to foster trust amongst their employees, contractors, customers, citizens, and partners:

- Establish an **enterprise-wide identity foundation** that spans all user types. This helps digital teams build and roll out new solutions faster, while keeping security and compliance a priority in the early stages of development.
- Prioritize a **“buy over build” approach** to new software, to take advantage of accelerating innovation in cyber security and identity spaces, and iIncrease internal innovation while reducing tech debt.
- Put c**ustomer-facing identity and access management (CIAM)** at the center of all external digital offerings. This supports effortless registration, login, and credential management, while governing identity profiles with a proactive approach to privacy, compliance, and customer consent.
- Make use of unified identity profiles for a **360-degree view.** This helps the entire organization better understand what customers and employees want, so they can deliver more consistent, cohesive, compelling experiences.

[11] “**2021 Gartner Board of Directors Survey**,” Gartner, September 30, 2020
[12] “**CIOs: Make Your Mark on the Customer Experience Initiative**,” Gartner, November 7, 2019
[13] “**Harvey Nash / KPMG CIO Survey 2020**,” KPMG, September 22, 2020

How Takeda built a trusted healthcare experience

As a top ten global pharmaceutical company, Takeda's brand is heavily based on trust. During the COVID-19 pandemic, the company knew it had to maintain this reputation, while finding new ways to engage with the public and expand its reach. To capitalize on digital as a path for growth, Takeda's IT team built a single customer identity that could support interactions with patients, payers, healthcare providers, IoT wearables, and product R&D.

"Identity is the crux of how people interact with our organization," said Bob Durfee, Head of DevSecOps for Takeda, "for us, the best way to establish a digital relationship with our customers was to consolidate customer identity across all platforms."

The company's global identity journey followed three primary stages:

- **Step 1: Expand on workforce identity.** The team learned from their workforce identity implementation, which included centralizing identity management, account governance, authentication, user provisioning, requests, and reporting for all employees and contingent workers in the cloud.
- **Step 2: Apply Zero Trust principles to customer identity.** Takeda next optimized its CIAM strategy for millions of patients and physicians with a focus on security, scale, and efficiency. By centralizing customer identity with a Zero Trust approach that makes no assumptions about a customer until their identity has been confirmed and their access privileges verified, the company was able to mitigate risk. This also reduced customer friction, helped users feel safe and protected when they interact with Takeda's brands, and made it easier for digital teams to analyze interaction data and create more personalized experiences.
- **Step 3: Accelerate productivity.** With a single global identity profile across all users, the business can now develop secure internal apps faster for global teams, bring legal and compliance teams into digital projects from the beginning, and help each brand build to its potential versus getting sidetracked by identity plumbing.

Cultivating an Empowerment Mindset

Identity helps CIOs break down barriers to digital transformation by enabling frictionless, trusted experiences and reconciling legacy systems, manual processes, and siloed management of users, apps, and resources. But once you have a solid identity strategy in place, what's next?

Many IT organizations are taking a hard look at their team culture. The typical IT mindset is all about trying to control technology, which only adds to shadow IT. Today, teams need to focus on more than just enabling and protecting employees. Future-ready leaders are cementing IT's essential role in the business by shifting it towards bringing people together and truly empowering them to do great work. To foster this mindset, CIOs have to constantly look for ways to make their technology solutions more secure, intuitive, scalable, and useful for everyone. With this in mind

Guide your team towards embracing the consumerization of the enterprise and the broader mandate that comes with it. For instance:

- Find ways for IT to **be the end user's BFF**. Consider offering rewards for reporting attacks, leveraging programs that create a flywheel for experimentation, and proactively soliciting (and then acting on) user feedback. Ask your business partners if your current IT priorities are best aligned to the overall strategic goals of the business.
- As mentioned above, bringing together disparate identity stores in a single unified control plane allows you to **extract more insight about your employees and consumers**. Take action on what you learn and evolve how you talk about technology through an empowerment lens.
- **Identify new IT career opportunities** that will attract top talent in competitive markets. For example, with cyber-security expertise now the most in-demand IT skill set, many teams are upskilling existing staff and simplifying key processes so more work can be done by IT generalists.

Looking Ahead: How Modern Identity Will Propel Innovation & Growth

After a year that defied all IT expectations, it is crucial to step back and reassess the trickle-down impacts of your rapid evolution during COVID-19. Going forward, CIOs must be even more proactive and not only respond to, but predict, changing market needs. As we've explored, your identity layer can help with this by not only modernizing existing technology resources and securing new digital assets, but future-proofing your business for decades to come.

Modern platforms like the Okta Identity Cloud elevate IT's value by mitigating risk while driving innovation across your cloud, on-premises, or hybrid enterprise IT landscape. In particular, by powering a holistic end-to-end identity strategy, Okta improves digital time-to-value and operational efficiency to accelerate growth.

The platform helps organizations:

- Seamlessly manage all people, resources, and things in one place, while balancing usability with security
- Extend the power and protection of cloud identity to critical on-premises systems
- Deliver frictionless, trusted experiences for employees, contractors, customers, citizens, or partners

As a result, IT can focus on higher-value work instead of simply closing ticket after ticket. And your entire business can take advantage of the market's latest security capabilities without having to worry about manually patching vulnerabilities for each application or access point. This kind of growth accelerator is key, since organizations that invested more in experimenting with new digital technologies during the crisis in 2020 were twice as likely to report outsize revenue growth[14].

To learn more about the power of identity in advancing your organization's goals, visit Okta.com.

[14] "**How COVID-19 has pushed companies over the technology tipping point**," McKinsey, October 5, 2020

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. For more information, visit **okta.com**.