Is Legacy Identity Infrastructure Holding Your Enterprise Back?

6 Common Myths About Cloud-Based Identity Management

okta

Index

Chapter 1

How legacy identity hinders digital transformation

While the term “digital transformation” has become a tired buzzword in recent years, that doesn’t make it any less important to a business’ success. In today’s technology-first world, every enterprise CIO is tasked with major digital projects that play a crucial role in helping their company stay competitive. In order to take advantage of these new opportunities while protecting applications and data, IT leaders must break through four frustrating barriers:

Security

Cyber attacks are growing in frequency and sophistication every day, and security concerns are slowing cloud adoption due to a perceived risk of losing control of sensitive data.

80%

of data breaches are caused by compromised credentials*

$3.86M

Average cost for organizations**

Operational complexity

With large companies’ intricate organizational structures, IT often lacks a single directory for all employees, contractors, partners, and customers. This hinders growth and creates friction, especially during mergers and acquisitions.

Cost

Legacy on-premises infrastructure is deeply entrenched in big organizations and expensive to maintain. For this reason, forward-looking IT teams are undertaking a phased approach to moving their workloads to the cloud, and eliminating CapEx cost models by transitioning to subscription-based licencing.

Time-to-market

Developers require more resources and freedom so they can adopt agile development and build competitive customer experiences quickly. Unfortunately, their efforts are frequently slowed by the need to develop non-core security and privacy features for each application they create. Organizations need a consistent identity plane to manage and secure their customers.

* Source: https://www.cso.com.au/mediareleases/29642/hacked-passwords-cause-81-of-data-breaches/

** Source: https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

Robust identity management with secure authentication, provisioning, server access, API management, and more can play a valuable role in overcoming each of these challenges. But this often feels easier said than done. Over the past few decades, most large enterprises have adopted a tangled web of on-prem identity and access management (IAM) systems from vendors such as CA, IBM, Microsoft, Oracle, and RSA. This presents a huge burden for IT departments, with some teams managing hundreds of cobbled-together identity stores or domains, along with customer identity that's fragmented across various websites, portals, mobile apps, and APIs.

These old identity systems create bottlenecks to digital transformation and make it difficult to securely support modern priorities and workplace realities, e.g., flexible workforces, best-of-breed stacks, and heterogeneous devices.

They require hardware and software that's difficult to connect with or maintain unless you have the budget for professional services or hard-to-find specialists. What's more, these platforms weren't built for the cloud and have thus far failed to offer viable cloud strategies.

> *If you stick with legacy identity, you're choosing to live with technical debt that borrows from future agility.*

Given all of this, CIOs are at a fork in the road. If you stick with legacy identity, you're choosing to live with technical debt that borrows from future agility. Alternatively, you can rethink security with a Zero Trust model, and put identity control points in place to address traditional network perimeters that are no longer effective. In this way, you'll improve workforce productivity and drive a digital agenda with frictionless user experiences — making the business more competitive. Once you have a handle on identities spanning all of your customers and workforce across multiple brands or subsidiaries, you can support faster onboarding or offboarding of users during major business events or new application rollouts. Lastly, given the current nature of our global, technology-driven marketplace, modern, cloud-based identity plays a critical role in protecting your APIs that support external technology services.

Chapter 2

Debunking myths about modern identity

In talking with many of the world's largest organizations, we've found that, despite these opportunities, some still feel held back from modernizing their identity stack due to misconceptions about cloud options. Here are six common myths that come up surrounding the replacement of legacy identity platforms with newer alternatives:

Myth #1

> *"Next-gen IAM platforms can't handle hybrid cloud or on-prem access needs."*

The first generation of identity and access management systems were built to secure homogeneous, on-prem resources within a corporate network. Under the hood, they contain significant technical gaps, so their "lift and shift" approach to the cloud actually requires IT to duct tape together multiple solutions if they want to address all use cases. That's why, a decade ago, modern identity options were tailor-made to address the rapid rise of cloud-based applications like Salesforce and the like. But you no longer need one IAM platform for your cloud apps, and another to secure on-prem systems.

You can extend your cloud IAM platform protection to on-prem applications thanks to solutions such as the Okta Access Gateway, which provides unified cloud-to-ground resource management for any type of hybrid IT environment. It lets you add cloud single sign-on (SSO) and multi-factor authentication (MFA) to on-prem apps without changing their source code. This brings added security to legacy systems and helps you centralize access policies and configuration to eliminate inefficient, inconsistent silos.

Myth #2

> *"Modern identity tools are just brokers for SaaS apps, they aren't yet mature enough to support enterprise access management requirements for infrastructure and APIs."*

Five years ago this might have been true. To be sure, cloud identity solutions started by specializing in SSO, but the industry has made massive strides over the past decade.

According to Gartner, Identity-as-a-Service (IDaaS) will be the chosen delivery model for more than 80% of access management deployments globally by 2022, and today's pure-play IDaaS leader is the Okta Identity Cloud. Okta now supports *any* access management or provisioning use case to secure all critical resources across apps, servers, and APIs – cloud or on-prem, public or private.

Okta's enterprise-grade, end-to-end solution features a Universal Directory, which acts as a business' central source of truth for all identity, and boasts a broad and deep integration network with thousands of pre-built app connectors. With our Advanced Server Access product, you can manage access to any multi-cloud or on-prem infrastructure to protect your critical development environment for customer applications. In addition, our API Access Management solution secures your API resources with fine-grained, configurable authentication and authorization policies.

Myth #3

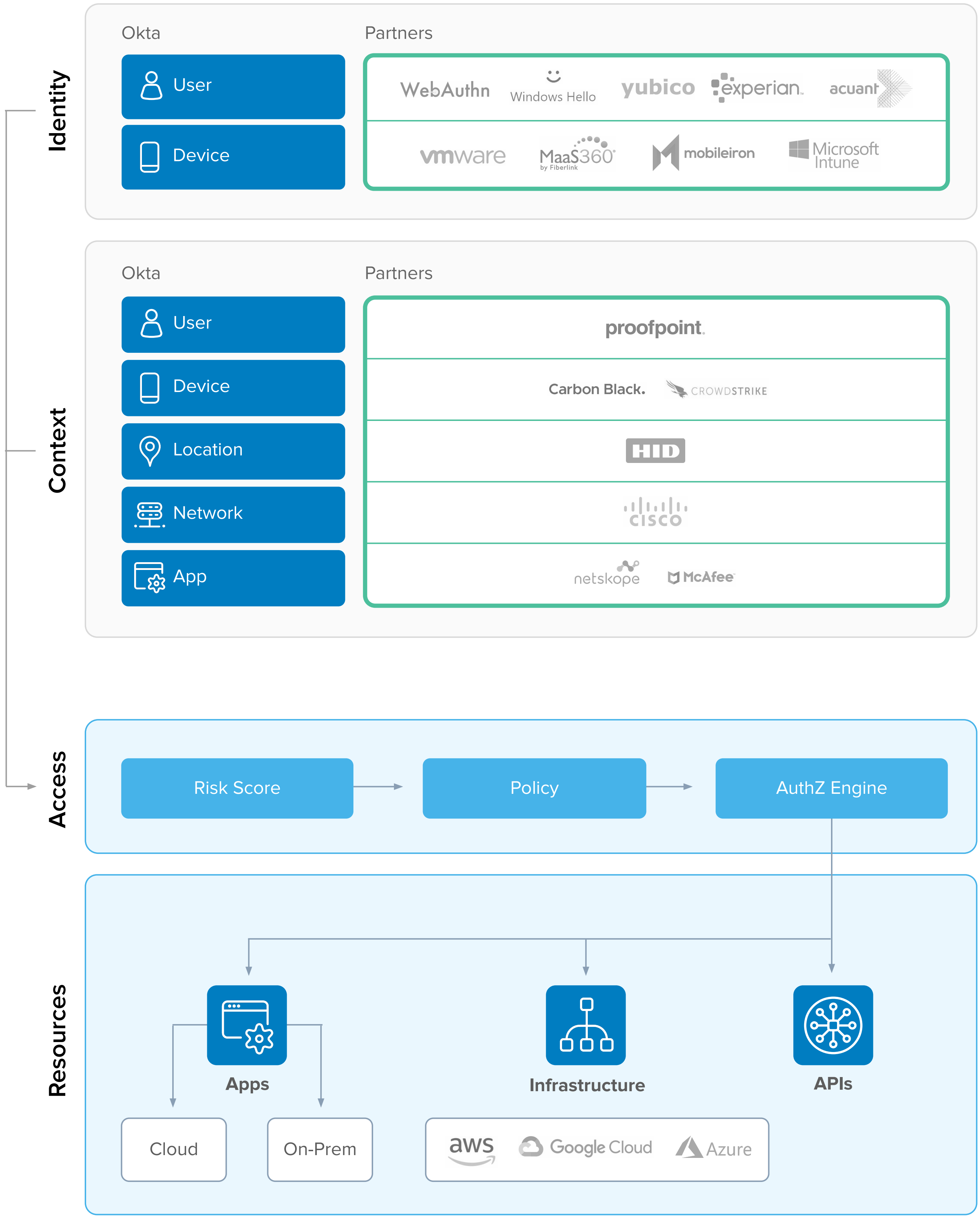
> *"Newer IAM solutions aren't as secure, scalable, performant, or configurable as more established infrastructure."*

Legacy identity platforms certainly bring decades of experience trying to meet yesterday's enterprise needs and security threats, but they struggle with the architectural anchor of an on-prem history that slows innovation.

On the other hand, Okta's cloud-native solution is 100% focused on meeting every IAM requirement of the modern enterprise. It is designed, built, maintained, monitored, and updated weekly with security in mind and no planned downtime. Our best practices range from live updates, advanced infrastructure security, and customer data encryption, to securing software development and conducting extensive security and penetration testing.

Okta maintains certifications such as ISO 27001:2013, SOC 2 Type II, Cloud Security Alliance, and FedRAMP Moderate ATO, and we help thousands of customers comply with HIPAA, PCI-DSS 3.2, Sarbanes Oxley, and GDPR. Our Zero Trust approach to managing enterprise risk protects against the latest security breaches by analyzing a variety of factors and context signals that help determine whether a user should get access to a certain service. Customers benefit from the proven scale, uptime, and reliability of our infrastructure, and since Okta is fully configurable, they enjoy self-service control and visibility over all identity processes, group rules, and more.

Zero Trust Reference Architecture



Identity

Okta

User

Device

Partners

WebAuthn · Windows Hello · yubico · experian · acuant

vmware · MaaS360 by Fiberlink · mobileiron · Microsoft Intune

Context

Okta

User

Device

Location

Network

App

Partners

proofpoint

Carbon Black. · CROWDSTRIKE

HID

cisco

netskope · McAfee

Access

Risk Score → Policy → AuthZ Engine

Resources

Apps

Cloud

On-Prem

Infrastructure

aws · Google Cloud · Azure

APIs

Myth #4

> *"These identity platforms only protect employees, not customers, supply chain partners, or contractors."*

Traditional IAM systems were built to support only one specific use case, whether that be employees, partners, contractors, or customers. This led to fragmented identity approaches over time, and presents increasing security risks as organizations struggle to both understand who has access to critical resources, and deploy unified access policies. Meanwhile, today's customer and partner-facing apps are usually built on APIs (often poorly secured and scoped), which leads to greater risk of breaches.

With the explosion of flexible workforces and new digital customer experiences that extend beyond the network perimeter, identity has become an enterprise's new security perimeter. Thankfully, it's no longer necessary to force these modern use cases into legacy infrastructure or maintain different identity stores for your workforce and customer users. Okta provides a complete modern access management platform that blocks security threats against all identity and resource types — for B2E (employee/contractor), B2B (partner), or B2C (customer) users — no matter where they are.

Myth #5

> *"It's more cost-effective to use my preferred IT vendor's identity platform and as many of their apps as possible because we have an enterprise licensing agreement."*

Despite the value of faster adoption and better productivity that comes with best-of-breed apps, some IT teams are scared off by the perceived cost of mixing and matching independent solutions versus adopting "free" options from someone like Microsoft or Oracle. But, have you ever heard the phrase "free like a puppy"? Beware of trade-offs when you rely on a single-vendor stack that requires a ton of resources to feed and care for it. Incumbent vendors aren't incentivized to facilitate a diverse ecosystem, so they typically offer only immature integrations outside their own products, and minimal or disjointed support for non-traditional identity types. If you have successfully deployed some independent security tools already, you know that they are almost always more effective and support deeper integrations than their Microsoft equivalents. And many companies don't realize they can save money by opting out of particular Microsoft SKUs that overlap with other systems in their environment.

Because identity is Okta's singular focus, we often do a better job of connecting multiple products from a single software provider than the vendor does themselves. Optimizing for choice is built into our business model, and this vendor neutrality facilitates any multi-cloud or best-of-breed strategy. The Okta Integration Network accelerates integrations and deployment across thousands of apps and services. It's important to compare these benefits against the hidden costs associated with the IAM tools in an enterprise suite, e.g., manually building and maintaining brittle integrations, security risks, servers, and outages, as well as vendor lock-in and rising prices.

Myth #6

> *"Ripping out decades-old legacy IAM systems is too big of an undertaking."*

For most large organizations, migrating entirely off your legacy IT infrastructure is not realistic or desirable today, so you'll likely be running a hybrid IT model for the foreseeable future. While breaking down entrenched complexity may feel like a pipe dream, it's very possible to start small and gradually modernize your identity infrastructure, consolidate internal and external user identity stores, improve your security posture, and deliver a better user experience over time.

Our IDaaS model delivers a platform architected for high scale and high availability, deploying updates automatically in the cloud without on-prem capital expenditures. And with any solution from the Okta Identity Cloud, you'll experience the fastest deployment and adoption ramp in the industry. In the following chapters, we'll describe several possible ways to take advantage of this opportunity, such as retiring non-critical legacy apps or tackling M&A-driven complexity. We'll also share real-world examples from companies like Experian, 21st Century Fox, and Hitachi that showcase the advantages a modern identity cloud can deliver.

Chapter 3

Five routes to modern identity

Every enterprise is unique, and paths towards identity modernization will vary. Even if you need to maintain some on-prem systems indefinitely, you can still achieve the benefits of moving your identity infrastructure to the cloud, while you phase out legacy IAM tools as quickly or as slowly as your organization requires. This journey could include any of the following five approaches.

	Strategy	**Ideal for:**	**Key benefits**
1	Add advanced authentication to SaaS apps	Companies adopting modern, cloud-based apps	● Low barriers to entry ● Reduced authentication risk
2	Retire non-critical legacy apps	Organizations with stagnant on-prem systems	● Increased adoption, productivity, and business agility ● Lower IT costs and maintenance
3	Tackle M&A-driven complexity	Businesses with inorganic growth and frequent org changes	● A single source of truth for cross-org users and duplicate identities ● Faster acquisition integrations with day-one access
4	Layer advanced security over legacy on-prem tools	IT environments with legacy on-prem WAM tools	● Strengthened security, while maintaining existing policy-based authentication ● Reduced reliance on legacy investments
5	Improve developer agility	Companies focused on digital transformation	● Frictionless customer experiences ● Improved data protection ● Accelerated innovation

1

Add advanced authentication to SaaS apps that already support modern protocols

In our recent Digital Enterprise Report, we found that 75% of IT decision makers in organizations with at least $1 billion in revenue are running apps in the cloud, with a broad spectrum of adoption ranging from under 10 apps to over 100. 67% of respondents said they expect to increase the number of cloud apps they use in the coming year. As forward-looking companies quickly move to the cloud, a simple first step in modernizing identity is to leverage the Okta Identity Cloud for all new applications you add. Even if you're not yet ready to retire all of your legacy IAM platforms, you'll be able to start proving the benefits of Okta's advanced sign-on policies, which use contextual signals (such as location or device management) to better align your authentication experience to the risk.

2

Retire non-critical legacy apps as new SaaS options come to market

At the same time, you can start proactively looking for opportunities to move stagnant on-prem systems over to best-of-breed apps with consumer-friendly interfaces. Giving employees access to proven tools they've already used at other companies will accelerate their adoption of modern tools designed for a mobile, cloud world. In addition, you'll simplify the change management associated with rolling out new technologies, and deliver competitive advantage through greater business agility. Finally, you'll be able to minimize your dependence on legacy identity infrastructure, enjoy deep pre-built integrations that don't require custom work, and cut expenses by decommissioning costly servers. By gradually replacing the least-supported, lower value-add areas of your software stack, you'll get your shadow IT under control and eliminate maintenance headaches that jam up resources.

3

Tackle M&A-driven complexity, sprawl, and disjointed IT

As large organizations evolve through mergers, acquisitions, divestitures, spin-offs, re-orgs, and other structural changes, one side effect is often a mish-mash of identity stores, overlapping profiles, and business rules that can increase security risk. A company-wide cloud identity layer like the Okta Universal Directory can provide a key control point and unified view of security as you integrate users across different organizations. Okta lets you pull in identities from disparate Microsoft Active Directories (AD), and contains logic that masks complexity and manages duplicate identities behind the scenes. With a single source of truth, you'll be able to provide newly acquired teams with day one access to multiple instances or domains across your subsidiaries while you evaluate consolidation options.

4

Layer advanced security over on-prem tools that use legacy protocols

Some IT teams are understandably reluctant to rip out existing web access management (WAM) tools that manage their complicated policy-based authentication. By simply adding Okta Multi-factor Authentication on top of existing identity systems with on-prem LDAP or RADIUS protocols, you can quickly strengthen their security. Many companies use Okta as a cloud gateway through our LDAP interface, bringing the benefits of leading-edge identity to older WAM tools, such as ADFS or Ping, which can continue to support regulatory compliance. In this way, you'll curb your legacy investments and start implementing more cloud-based controls, workflows, and automation to break down technical obstacles over time.

5

Improve developer agility by making it easier to launch secure customer apps

Real digital transformation goes way beyond your workforce to encompass all of the technology-driven experiences you deliver for customers and partners, as well. Organizations looking to compete, evolve, and empower innovation are faced with a critical mandate to "platformitize" their overall business. This requires you to update and connect all underlying architecture and microservices — especially anything that touches your customer-facing apps. With all of the demands placed on IT today, chances are you don't have enough developers to execute on everything you want to accomplish. In this pressure-cooker environment, apps aren't integrated, spaghetti code and security exposure is everywhere, and the burden of legacy decisions weighs heavy. It's no wonder developers are reluctant to mess with legacy identity systems.

The truth is, building identity is hard, but keeping users secure is mission-critical. And since customers hate friction, any difficulty with signups, logins, or password recovery causes them to bail and impacts revenues. To effectively balance security with usability, you'll also need a modern approach to customer identity. Modern platforms like Okta ensure flexible, seamless user login and registration from multiple sources, while leveraging contextual access management to better protect customer data. By unifying all your customer (and workforce) identities in one platform, you'll reduce costs while increasing efficiency.

Chapter 4

Modern identity in action

Let's bring these modernization strategies to life with four real-world examples of large companies that realized significant cost savings and greater business agility by adopting Okta's cloud-based identity management.

Enhancing security with a Zero Trust model for 50,000+ partners

21st Century Fox faces the challenge of securing industry-leading content that's produced by a massive, complex network of partners, contractors, and employees to delight 1.8 billion subscribers. The media organization wanted to increase its security posture to reduce the likelihood of a data breach, while providing a dynamic access model for secure collaboration.

- **Step 1**: The company's global CISO decided to evolve from perimeter-based security to a Zero Trust environment that would keep users and their credentials protected and secure, no matter where they're working.
- **Step 2**: 21st Century Fox reduced its identity sprawl and gained better visibility by adopting Okta SSO, Universal Directory, and Lifecycle Management.
- **Step 3**: The organization next adopted Okta API Access Management to support its large and complex creative network, and rolled out Adaptive MFA to bring consistency to the authentication process without causing unnecessary friction for users.
- **End state**: 21st Century Fox now benefits from a holistic, fine-grained security infrastructure with a clear view into all user activity; easy onboarding and offboarding of employees, contractors, and partners; and contextual access management that considers the user, app, device, location, and network of each request.

Replacing disparate on-prem identity products during M&A

Allergan is a growth pharma leader, with a high volume of mergers and acquisitions (we're talking 13 acquisitions in a single year) and very diverse business lines. Previously, its many different legacy IAM products created confusion and caused the IT help desk to be inundated with password reset requests.

The company took a measured approach to adopting modern identity before eventually connecting its entire extended ecosystem, including health management IoT devices.

- **Step 1:** Allergan first implemented Okta as a common authentication point for cloud applications, later adding Okta's Lifecycle Management and Universal Directory solutions.
- **Step 2**: Following a major merger, the organization standardized all of its IAM onto Okta, implementing robust governance around provisioning.
- **Step 3**: Next, senior leadership decided to weed out lower priority legacy systems and rebuild IT around best-of-breed partners, with Okta as the cornerstone of that process.
- **End state**: Today, 23,000 employees, 50,000 partners, and four million doctors and patients use Okta to connect to all of Allergan's cloud and on-prem apps and portals. Okta even powers secure identity for an app patients use to manage hand-held devices that help with dry eye disease.

Saving $1M+ by moving from 6 identity platforms to 1 for vital customer and workforce identity needs

Experian, the largest consumer credit reporting agency in the world, is transforming into a customer-driven, real-time data services company. To prepare for this, they decided to standardize on a single identity platform.

- **Step 1**: Experian's consumer services division started using Okta as the identity solution for its new Credit Tracker mobile app.
- **Step 2**: The company hired a new CIO, who decided to build on that success by moving from six separate identity systems to Okta. The organization gained one identity standard for its 16,000 employees, consumers, and partners.
- **Step 3**: To build out secure API services for customers, the team next turned to Okta API Access Management and Apigee in order to manage APIs in the same way they do devices, users, and applications.
- **End state**: Okta now enables a better user experience for Experian's digital services, as well as faster development cycles, better authentication, and a simplified IT environment. By shutting down an array of fragmented on-prem tools, the company avoids $1 million annually from the ongoing expense of managing those services.

Managing digital transformation on a timeline for 120,000 employees

ENGIE, an international purveyor of power, natural gas, and energy services, is leading the transition to a more sustainable, de-carbonized world. To support this effort, it recently transitioned to a decentralized business model distributed across 24 geographies. ENGIE's CIO immediately recognized the impact of this restructuring on identity management and took action.

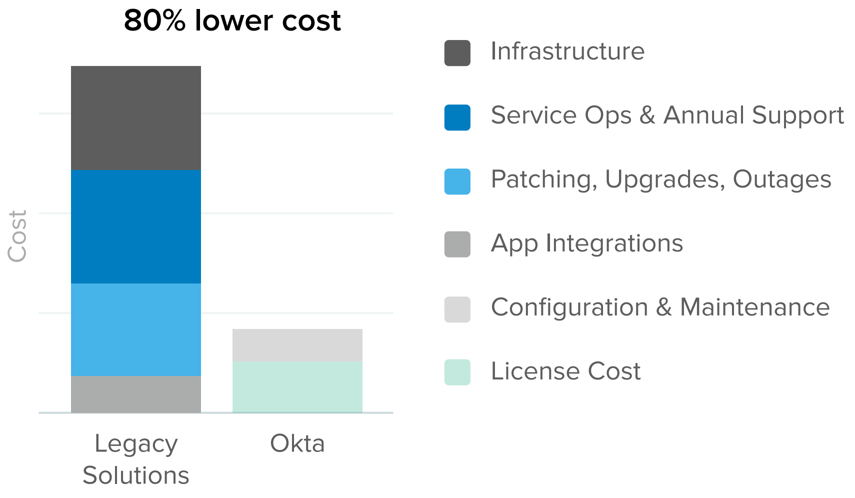
- **Step 1**: He chose the Okta Universal Directory to quickly connect 100+ AD domains and unify global business units, while facilitating innovation at the local level.
- **Step 2**: Okta's modern identity platform ensured agility during a rapid Office 365 deployment for 120,000+ employees in 60+ countries.
- **Step 3**: Later, the IT team quickly integrated 40+ additional apps with Okta SSO and brought 50,000 field workers online for the first time so they could benefit from easy access to applications from any device.
- **End state**: ENGIE also deployed Okta's MFA for another layer of protection, and the entire organization now enjoys simplified, future-ready security and access.

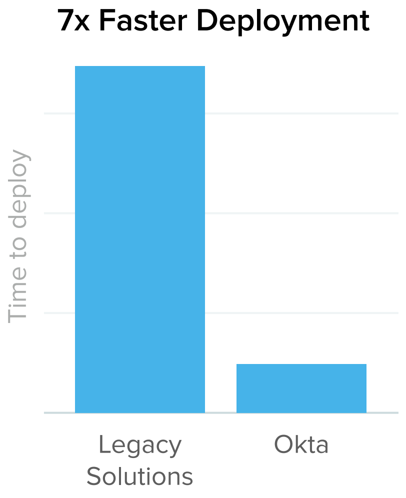
Chapter 5

Justifying the business case for identity modernization

Many IT leaders face organizational resistance and inertia when they advocate for infrastructure modernization projects. But according to Forrester, modern, cloud-based IAM delivers a 60-80% reduction in operations, ongoing maintenance, and development personnel costs compared with on-prem installations. To prove out these savings and navigate internal roadblocks, it's helpful to challenge the status quo by asking questions like:

- How much time and money do we spend on upgrades and maintenance for our current identity tools across the organization?
- Are the IAM vendors we're working with today really going to be long-term allies and partners for our business?
- Are they motivated to build deep integrations to all the apps we might need in the future, or are they incentivized to create vendor lock-in?
- Is security and identity their core business?
- Can they secure our new SaaS apps in a way that's simple for our users and doesn't require tons of custom development for IT?
- Are they cloud-native or do they still have an on-prem mindset? What's their track record when it comes to delivering consistent IAM innovation?
- Are their products as integrated as they claim, or just cobbled together to form the appearance of an end-to-end solution?





During these conversations, you can be a change agent by building a solid business case to get people thinking about the costs of delaying modernization. Rather than insist on a full rip and replace, show your stakeholders how next-gen identity can add value incrementally over time.

For example, Hitachi, a century-old conglomerate, has 900 divisions and its CIO faces daily pressure to both slash costs and accelerate the transition to the cloud. To meet these demands, he convinced the company to replace its legacy IAM infrastructure with Okta. As a result, his team streamlined application access for 300,000 employees and suppliers, and sped technology adoption cycles across business units, all while ensuring geographically specific regulatory compliance in APAC and the EU.

> *“To maintain our innovative culture, we recognized the importance and value of integrating new technologies and enabling our global workforce to access the tools they need from anywhere. The Okta Identity Cloud powers our truly modern identity system, flexible enough to adopt any technology and secure enough to protect our most valuable asset — our people.”*
>
> *— Ashish Sanghrajka, CIO Hitachi Americas*
>
> HITACHI
> Inspire the Next

Another case in point is Cardinal Health, a $120 billion company that revitalized its decade-old, highly customized CA-based identity layer for 60,000 employees and rapidly migrated 100+ applications to Okta in one weekend. This new paradigm significantly improved speed, resiliency, security, and the user experience, while minimizing the disruption of inevitable change.

> *“When we thought about ROI, there were three main drivers we considered: the expectations of our customers, which are a lot higher right now than they've been historically; the opportunity to improve agility and minimize the immense amount of time and money we were spending trying make our legacy platform work for us; and finally, cost.*

> *All our previous integrations and customizations were costing too much money, so we knew we needed to find a way to optimize our delivery for any new capabilities the business required.”*
>
> *— Bill Dubois, Manager, Identity and Access Management, Cardinal Health*
>
> CardinalHealth

Fortune 10 company McKesson is one of the largest healthcare organizations in the world with nearly 80,000 employees across 15 countries. The business has grown through acquisitions over the years, with many divisions operating separate data centers and technology stacks. Given this decentralized environment and the headwinds of the healthcare industry, delivering products with a seamless customer experience is almost impossible.

> *“We kicked off our transformation because we wanted IT to get out of the way of the business by offering a platform that is self service, always available, and secure. Identity is a differentiator for us and allows teams to get from concept to a minimum viable product in the shortest time window possible.”*
>
> *— Andy Zitney, Chief Technical Officer, McKesson*
>
> MCKESSON

Chapter 6

How the Okta Identity Cloud delivers business advantage

In the midst of intensifying pressure on IT as every business morphs into a technology company, be careful not to overlook identity's essential role in your infrastructure. Modern IAM can be a major differentiator because it enables a frictionless experience for all users, which in turn accelerates adoption and digital transformation. At the same time, you'll gain peace of mind by mitigating security breaches and meeting compliance requirements.

By investing for the long-term, you'll be ready for whatever comes next, while ensuring backward compatibility. To achieve these results, you need a partner you can trust to transcend the inherent complexity of your environment. Here's how Okta can help you overcome the four key IT challenges we discussed in chapter one:

1. **Security** – Okta helps reduce password management risk and protect against identity attacks. Its strong authentication for apps, APIs, and servers enables a Zero Trust security model.

2. **Cost** – With a modern identity platform in place, it's easier to start deprecating old legacy systems that are costly to maintain and reduce CapEx by adopting best-of-breed cloud applications. In addition, Okta helps centralize audit reports and license management, giving you the controls you need to easily grant or revoke access to any application.

3. **Operational complexity** – By making it effortless for your workforce to access apps from any device, network, or location, Okta helps accelerate growth and improve employee productivity. With automated onboarding and offboarding of users, as well as efficient domain consolidation, you'll expedite M&A integrations and gain a 360-degree view of all your identity types across multiple lines of business.

4. **Time-to-market** – With Okta's world-class identity solution protecting the IT environment, your development team can shift gears to focus on speeding digital transformation.

Okta offers security, agility, and neutrality with a seamless cloud deployment model and frequent releases of new capabilities and integrations. By leveraging open standards and pre-built connectors, we minimize the need for expensive consulting projects and help combat big software vendors' lock-in tactics. In addition, our scalable cloud architecture and AWS do the hard work of disaster recovery, virus protection, and more, so you don't have to worry about server maintenance or version control. This means you'll be able to roll out innovative technologies to your workforce and customers faster, while gaining the flexibility you need to handle constant changes to business operations.

If you let legacy identity impede your digital initiatives, disruptive competitors will surely rise up. In fact, 86% of the world's largest organizations are actively engaging in at least two of these forward-looking IT initiatives today:

- Adopting cloud apps with a hybrid mindset,
- Increasing Infrastructure-as-a-Service (IaaS) use,
- Pursuing digital transformation,
- Prioritizing customers' digital experiences,
- Embracing agile app development,
- Adopting a Zero Trust strategy, and
- Using strong multi-factor authentication types.

Thankfully, adopting a modern IAM platform to power these projects is easier than you might think. Don't get left behind – schedule a meeting with Okta, and we'll help tailor an identity modernization journey for your organization's unique 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 6,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 6,100 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.

www.okta.com