Modern Infrastructure and Development: Using Identity to Scale for Tomorrow's Technology

Okta Inc.
100 First Street
San Francisco, CA 94105

info@okta.com
1-888-722-7871

Table of Contents

As a result of groundbreaking technological advances over the past 20 years, we've witnessed a massive shift in the way businesses are operated. What began as a quest to supplement brick and mortar with a digital storefront is now a customer experience-driven crusade to be the most innovative, the most agile, and the most accessible. This new reality means that in order to be a leader in the twenty-first century, you must also be a *digital* leader.

Modernization is the answer

To insulate themselves against catastrophic data breaches, companies are moving toward modernizing their tech stacks through the refactoring and consolidation of legacy software components.

On top of bolstering data security, modernization also increases agility, shortens app development cycles, and reduces infrastructure costs. It's a no-brainer for any business that wants to survive rapid scaling. But how do you actually do it? And—more importantly—how do you do it while still retaining the ROI of your current infrastructure?

Okta surveyed 100 top IT and app development leaders from companies with over 1,000 employees to discover what's holding them back when it comes to application modernization. The results are both surprising and enlightening.

The pains of legacy infrastructure

With the rising use of cloud applications, most of today's new companies operate solely (or at least primarily) in the cloud. But more established businesses are often caught in limbo, wondering how to migrate from their decades-old legacy infrastructure to the cloud.

On top of how, they are also wondering if they should migrate. According to our survey data, 50% of respondents are worried about the security of their data as they migrate to the cloud among several other challenges.

Maintaining costly infrastructure

The servers, network equipment, and legacy middleware/virtualization software that once filled your capital expenditure are now liabilities. Lack of flexibility, constant maintenance and upgrades, and the very real threat of total loss due to disasters such as fire and flood translate to vast overspending.

Customer friction

An outstanding customer experience is and always has been at the crux of a business' success, and that experience starts with onboarding your users. In today's 'bring your own device' world, this means providing a fast and seamless sign-in and sign-up experience using the modern capabilities of the device they're using, such as authenticating users through built-in biometric readers like Apple FaceID. Unfortunately, achieving this can be nearly impossible to accomplish when your digital assets are powered by legacy identity, and customers are taking notice of those who aren't stacking up.

Lack of developer agility

While developing languages change and are updated alottin new functionality to a wide array of new use cases the truth is, current systems are not keeping up with todays development standards. Companies like Amazon, Facebook and Google roll out changes across vast systems in an instance while most homegrown legacy systems can take weeks, months and even years of change management for a single change to roll out. Additionally, 32% of those polled said they're struggling with security due to their aging, on-prem systems. Migrating those systems comes with a variety of challenges.

Security

Nowadays everyone is a target, including you and your customers' personally identifiable information (PII). Staying up to speed on the latest in data security practices is key to building and maintaining a healthy business. But most pre-modernization organizations can't say with certainty that their developers are doing so, nor can they be confident their legacy software is patched up-to-date to protect

against the latest security vulnerabilities. One common area of weakness is around API security; only a handful of app development teams are well versed in OIDC and OAuth 2.0, the modern authentication and authorization frameworks. A vendor dedicated entirely to identity and app security can help fill the gaps.

How modernizing drives scale

These days, technology is often synonymous with scale. The tools you have access to are built to amplify your efforts so that you can generate more impact with less effort. Without these tools at your disposal, it's unlikely your business will be able to keep up with your competitors—not to mention protect yourself from crippling security breaches.

However, a common misconception among many organizations is that they can't afford to modernize...and it's no wonder why. Currently, 38% of businesses are spending their IT budget on maintaining legacy infrastructure, and a whopping 43% see these costs as a barrier to innovation.

With their budget tied up in the past, it's difficult for these organizations to see into the future. But the numbers are clear: as the infrastructure ecosystem continues to evolve, and software development cycles speed up, it's critical to move away from on-prem infrastructure and monolithic methods of development. Modernization empowers teams to shift existing budget allotments to software expenses, reduce the cost of infrastructure that reoccurs with hardware updates, and allows the ability to take advantage of new software immediately.

Scale securely with an identity-as-a-service API provider

For those with extensive legacy systems, migrating to the cloud entirely might not be possible or even ideal. In these cases, a hybrid-cloud model utilizing identity as a service is the best option. Identity as a service allows you to adapt and integrate legacy assets with modern solutions such as SAML and OpenID Connect. As a result, you have the flexibility to maintain your legacy systems while protecting them behind the cloud identity which ultimately will allow you to architect for scale as your cloud presence grows and your on premise dependencies diminish.

However, 74% of survey respondents reported having concerns about creating new vulnerabilities from misaligned security policies, and they're absolutely right: it's important to limit the number of redundant technologies you employ. Choosing the right software, one that consolidates identity and security, integrates with your existing applications and creates flexibility to still use legacy applications in conjunction with your modern applications, will ultimately prevent security mismanagement and reduce administrative overhead.

Five steps to modernize your tech stack

Identity is critical to every application in your tech stack. It not only ensures your users can sign in securely but also gives them the right level of access. Leveraging modern identity standards such as OAuth 2.0 enables app development teams to transition to a microservice-based architecture.

To begin modernizing your tech stack with identity at its core, start with these simple steps:

1 Migrate to the cloud

Cloud-based infrastructure will promote agility and simplicity within your organization, whether it's best-suited for full cloud migration or a hybrid-cloud solution.

With Okta Customer Identity products, migration is simplified thanks to direct integrations with legacy directories such as Active Directory (AD), Lightweight Directory Access Protocol (LDAP) and an on-prem provisioning connector, as well as a robust integration network of over 6,000 industry-leading apps to centralize

and automate access management. The result is an environment that is secure, easy to maintain, and capable of deploying new services quickly.

2 Leverage the API economy

To mitigate the risks associated with using APIs without negatively impacting the benefits, organizations should consider implementing API Access Management. Built on Okta's Universal Directory, Okta's API Access Management allows the ability to easily grant (and revoke) API access based on predefined policies. The result is a sharp reduction in security risks associated with exposed APIs.

3 Refactor for cloud-native

User tech stacks are multiplying by (what seems like) the day, and users—including customers, partners, contractors, and vendors—are cycling technologies at an increasing rate. Refactoring—the process of restructuring existing code—can help by transforming an application to become cloud-native. This process, while not for the faint at heart, empowers businesses to scale securely at a pace that would otherwise be unattainable using a solely on-prem environment.

4 Retire legacy infrastructure that can't be modernized

If your organization is still using legacy homegrown applications, it becomes increasingly difficult to incorporate multi-factor authentication—a must-have when optimizing for security. These apps are a priority for retirement.

Beyond that, you'll want to determine which systems and data you keep on-prem and which you migrate to the cloud. A good rule of thumb is to keep the most vital systems and data on-premises while migrating less sensitive data and more frequently accessed systems to the cloud. For London-based finance firm TP ICAP, this meant using Okta to move its customer-facing Fusion platform to AWS to make it more flexible, scalable, and easy to use. After their huge success with Fusion, TP ICAP implemented Okta across the entire organization.

5 Shift from monolith to microservices architectures

Traditional on-prem applications are monolithic, meaning they operate as a single, giant web of code. They're simple to develop and deploy at the outset, but become increasingly difficult to update and scale down the line. By transitioning to microservices—loosely coupled services that make up a larger application—app dev teams can deploy updates on specific components quickly and with ease.

For the Motorists Insurance Group, Okta's microservices approach allowed them to choose the apps that best suited their needs—like F5 to give agents access to their on-prem systems and applications, MuleSoft to ensure each agent accesses the right backend services, and Guidewire to manage policies, billing, and claims. Armed with these improvements, they were better able to serve their nearly 700,000 policy holders.

Okta's Customer Identity products

Your development team should be focused on your core product—not maintaining overloaded and underperforming on-prem systems. With the Okta Customer Identity products, this becomes a completely achievable goal.

Use Okta's best-in-class Customer Identity products, and take advantage of everything Okta has to offer, including a scalable service that grows as you grow; a secure user store; easy-to-roll-out MFA; password policy engine; out-of-the-box account recovery flows; a catalog of products for integration with your existing systems; SDKs for the most common programming languages; a fully customizable sign-in widget, and support for the next wave of identity technology.

Contact us to learn more, and visit our Customer Identity products page to see how Okta can help you get started with modernizing your infrastructure.