

The Identity Accelerator

How Identity and Access Management Expedites Popular
Cloud Modernization Strategies (Okta's 6Rs)



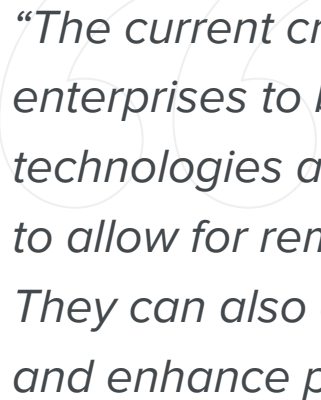
okta

Table of Contents

Evolving drivers of cloud adoption	3
Popular strategies for cloud migration	4
Key considerations throughout your cloud journey	6
Your modernization playbook	8
1. Rehost	8
Cypress secures and simplifies its complex hybrid environment with Okta	8
2. Revise	9
Okta brings cloud-agnostic identity to Alliance Data	9
3. Rearchitect	10
T-Mobile gains game-changing agility with Okta	10
4. Rebuild	11
Okta supports zero trust infrastructure access at Personal Capital	12
5. Replace	12
Dentsu Aegis securely moves to the cloud with Okta	13
6. Retain	14
Okta helps Hitachi secure legacy systems	14
Modern identity's role on the road to the cloud	15

Evolving drivers of cloud adoption

In the decades since “cloud computing” first achieved buzzword status, its benefits have been widely proven. And now that the shift to both dynamic work environments and digitized customer experiences have rapidly accelerated, migrating these applications to the cloud is more important than ever.



“The current crisis has amplified the need for enterprises to become more digitally adept... Digital technologies and approaches are designed not just to allow for remote engagement and operations. They can also change revenue and cost structures and enhance products and services.”

— [Gartner](#). “Identifying Digital Opportunities During and After the Pandemic,” June 2, 2020

The new normal requires flexible workforces that can work from anywhere and help organizations quickly scale up or down as supply and demand fluctuate. Additionally, external customer-facing applications must provide frictionless experiences across channels that enrich—rather than hinder—the customer journey. In this way, businesses can encourage customer engagement and create new revenue opportunities, as well as secure the employee experience and build trust.

Popular strategies for cloud migration

In many cases, digital transformation starts with migrating on-premises applications to the cloud. As technology leaders review their app portfolios, determine how to address myriad demands, and work to reduce capital expenses (CapEx) along the way, there is no one-size-fits-all approach. The best cloud strategy for each app depends on your business' IT budget, timing, and the individual app's criticality. For workforce apps, this is driven by how well they support remote, dynamic, and mobile work requirements with security that works everywhere (and not only in the office network perimeter). With customer applications, most cloud migrations are motivated by the need to deploy and scale personalized, relevant, cohesive omni-channel experiences that help grow and retain revenue.

No matter which of these many pressures are pushing your organization to modernize its on-prem ecosystem, there are several methodologies that can help you make the right choices. Experts at [Gartner](#) and [Amazon Web Services](#) recommend that technology leaders consider some, or all, of the following approaches.



Rehost



Revise



Rearchitect



Rebuild



Replace



Retain

1

Rehost

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

2

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. This is also known as “lift-tinker-and-shift,” since it employs a more cloud-aware approach.

3

Rearchitect

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. However, the effort involves in-depth changes to your application before you can rehost it in the cloud.

According to Gartner, 75% of organizations today plan to rearchitect their custom-built applications for the cloud.

4

Rebuild

A rebuild strategy 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.

5

Replace

For many older apps (whether commercial off-the-shelf or homegrown), your best bet is to replace them with cloud-first SaaS services. These usually include best-of-breed solutions like Salesforce for CRM, Workday for HR, or perhaps Okta for identity and access management (IAM).

6

Retain

Of course, 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.

Once in a while, you might find that as your business model evolves, certain legacy apps no longer add the value they once did. You can simply retire those tools completely to decrease overhead and increase security with minimal cost. However, across all of the strategies above, one essential requirement remains constant: **the ability to effectively secure your users and resources**. This is why identity plays such a foundational role in your journey to the cloud.

Key considerations throughout your cloud journey

In order to effectively evaluate each of the approaches above on an app-by-app basis across your technology portfolio, it's helpful to use a consistent framework for application rationalization. Experts recommend creating a detailed technical, operational, and business profile of each application before selecting your migration strategy. Across Okta's customer base, we've seen leaders zero in on four top factors when deciding what and how to move to the cloud:



Security

- How well does this approach improve our security posture?
- Can we now adopt modern techniques, standards, and protocols—like multi-factor authentication (MFA), OAuth, and OpenID Connect?
- Can these be easily managed and updated without having to rely on developers?
- Can I log and gain visibility across all of the layers of my cloud application?



Efficiency

- With this approach, can we more rapidly add to and maintain this application to improve developer productivity?
- What about support for continuous integration and deployment (CI/CD) practices?
- Does this improve agility and adaptability across development and infrastructure teams?
- Can we work across multiple IaaS providers for the benefits of a cloud-agnostic environment?



User Experience (UX)

- How much does this improve user experience?
- Can we provide easier, frictionless access with a modern interface?
- Does it support a cohesive customer experience across channels?
- Can we implement seamless integrations?



Cost and Return on Investment

- How much effort, risk, and cost does this strategy introduce as compared to its benefits?
- How critical is this particular application to our business?
- How widespread is our usage?
- What type of data does the application store (such as personally identifiable information or sensitive customer data)?

Below is a high-level summary of how each approach tends to stack up:

	Security	UX	Efficiency	Cost	Effort	ROI
Rehost	neutral	neutral	+	neutral	++	+
Revise	+	neutral	neutral	-	+	+
Rearchitect	++	neutral	+++	-	+	++
Rebuild	+++	+++	+++	--	++	+++
Replace	+++	+++	+++	-	+++	+++
Retain	neutral	neutral	-	neutral	neutral	-

Above all, be sure to look beyond the immediate tasks related to your migration, and focus on the broader cloud benefits you’re trying to achieve. The strategies you choose should align with that long-term vision. Most often, you’ll find that putting in a bit of incremental work (i.e., opting for a revise approach rather than a more basic rehost) will reap big rewards through more complete, future-proof outcomes.

Your modernization playbook

To help companies avoid common pitfalls and accelerate their cloud migration at any stage, we've gleaned best practices and recommendations from the thousands of Okta customers who've leveraged identity as a key enabler to support six primary modernization strategies.



Rehost

A pure “lift-and-shift” from on-prem to cloud will help you gain several cloud benefits, for example, quickly reducing data center costs and adopting an operating expense (OpEx) model for your infrastructure. Although cost reduction is often the main driver of data center consolidations, closures, or optimization strategies, keep in mind that both your cost and efficiency gains will be limited by your technology team’s existing application stack and development processes.

With a rehost, your security improvement will be neutral at best. In some cases, moving an application could even open up new vulnerabilities, so make sure to do a security analysis on each app and reconsider this approach based on the results. A modern identity platform like Okta can increase your impact in a rehost scenario by replacing on-prem identity components with cloud-native hybrid IT access management. It also enables secure server access while allowing you to remove intermediary directory or access management systems such as LDAP.

Cypress secures and simplifies its complex hybrid environment with Okta



[Cypress](#), a technology company that develops solutions for the Internet of Things, has millions of customers and multiple locations around the world. It also had a complex IT environment, a mixture of cloud and on-premises systems, and third-party and custom applications that required each user to have multiple accounts and passwords. Cypress turned to Okta to modernize its identity management system, implement new security standards, and offer an integrated, friction-free IT experience.

“Before Okta, we had a lot of limitations. We couldn't easily integrate our cloud applications or grow our cloud experience. Okta has facilitated our transition to the cloud quickly and easily,”

— Brad Burton, Director of IT, Cypress

“We've been able to remove our integration with ADFS and our internal LDAP solution. Now we have one platform to support instead of many platforms.” Cypress CIO Steven Nott added, “From an administrative standpoint, one platform is much easier to manage, and it brings savings, so it paid for itself. That's where the ROI was.”

As the company grew through M&A, new employees and new workplaces also added to Cypress's already complex hybrid environment—including Microsoft Office365, Salesforce, Zoom, SuccessFactors, and home-grown systems. With Okta, the organization's long-standing challenge of integrating cloud infrastructure and on-prem infrastructure has been almost completely erased. “We're doing it two different ways,” says Nott. “We're either phasing out the older systems as we migrate them to newer platforms, which is part of our system-consolidation strategy, or we're working with Okta to figure out ways to bring them in house.”

Revise

A revise strategy involves updating specific components of an application so you can expedite innovation and achieve total cost of ownership gains with just small changes to your application. By updating DevOps processes and further leveraging infrastructure-as-a-service (IaaS) platforms, you'll increase innovation surrounding your primary application, as well as overall developer productivity. Once you've modified some of your app components, you can significantly improve your security posture without touching the application code, perhaps by connecting it to an external identity service for single sign-on (SSO) and MFA protection.

The right identity platform will instantly support your cloud-enabled apps on multi-cloud deployments for greater flexibility. During this process, forward-looking technology teams often choose to replace their outdated web access management (WAM) systems or hardware tokens to further decrease their on-prem footprint. If you are revising a customer-facing app, it's usually worth swapping out any legacy or custom identity services with a proven customer identity and access management (CIAM) solution. You can then link the user directory to your CRM or customer data platform to establish a 360-degree view of your customers, which is critical to delivering cohesive omni-channel experiences.

Okta brings cloud-agnostic identity to Alliance Data



[Alliance Data](#) is the engine behind loyalty and marketing campaigns for consumer-facing companies worldwide. The Fortune 500 organization's 20,000 international employees rely on hundreds of cloud and on-premise apps to get their jobs done, but were previously burdened by an IT infrastructure that consisted of a traditional data center with a lot of hardware, heavy-duty on-prem applications, and a few SaaS solutions.

The company's IT team decided to revise some of these apps and move towards a cloud-first, hybrid infrastructure.

By layering Okta's Universal Directory, SSO, MFA and Access Gateway on top of its apps, Alliance Data was able to centralize its access management solution and infrastructure, and avoid changing source code for on-prem apps.

“Okta really is the face of our applications to our employee end users. It's great because it's cloud-agnostic which gives us the freedom to deploy systems where it makes sense.”

— Darren Linden, Head of Corporate IT Services, Alliance Data

Alliance Data now provides employees with access to 93 production apps, including 19 major on-premise apps, through Okta. “This initiative impacted our business by really enabling us to have a cloud posture with these large, mature, on-prem apps,” added Linden. “We essentially have no on-prem data center at this point, thanks to the power of Okta.”

Rearchitect

When it comes to your core business systems and external revenue-driving apps, it'll likely be worth the significant one-time project costs to open up the code and refactor at least some of their key subsystems to make these apps cloud-native. By embracing modern practices like 12-factor methodology and breaking the application up into APIs and microservices, your team can reduce technical debt for the underlying tech stack, and take advantage of elastic IaaS and platform-as-a-service (PaaS) services for cost optimization and growth. This effort delivers positive ROI through accelerated digital transformation and massive gains in agility and adaptability.

What's more, with minor code changes, you can also adopt modern identity protocols, like OpenID Connect (OIDC) and OAuth, for enhanced security. As part of this strategy, another best practice is to utilize API access management capabilities, software development kits from your identity provider, and additional zero trust layers like web gateways to protect mobile apps and single-page web applications (SPAs). With a robust CIAM platform, you can also support deeper integration with your CRM, call center, and customer data hub systems.

T-Mobile gains game-changing agility with Okta

T-Mobile

[T-Mobile](#)'s IT journey over the past five years has involved overhauling the entire technology stack, moving to cloud-native applications, embracing a DevOps working model, adopting product-centric design, and building a development team that can create experiences and products at speed. It's a model that every modern company aspires to. Initially, the team was using several different systems for IAM.

Different T-Mobile applications used different systems to validate users, and that lack of consistency led to frustration for customers and care agents alike.

T-Mobile replaced their entire Oracle identity stack with Okta, eliminating a vast on-prem infrastructure as well as licensing and support costs.

“We had upwards of 80 application servers and multiple data centers that we had to maintain. That’s now down to about six virtual machines, for a massive cost savings to our operational budget.”

— Kris Wilson, Senior Director, Product and Technology, T-Mobile

The team then deployed an API strategy that would expose functionality to product and technology teams, get them more reuse out of their work, and reduce their technology footprint and security surface area. “When you think about how identity plays into security with APIs, if you’re building identity multiple times into multiple systems, you’re multiplying the number of exposure points,” said Warren McNeel, senior vice president of IT. “We wanted to limit that by going to a single identity solution.”

Okta API Access Management also helps keep partner API calls secure. For API lifecycle development and implementation, the company uses an Okta partner, Apigee (now part of Google Cloud). The Okta-Google Cloud solution creates an ideal state for T-Mobile’s API ecosystem, providing a streamlined system for third-party integration and layering security policies over it.

“Okta was a game-changer for us,” says McNeel. “We’re no longer customizing APIs individually for all the different data access points we want to protect, all the roles that get different treatment.” Wilson added, “Having that all consolidated on the Okta platform is huge. Having an authentication platform that you can easily integrate with greatly accelerates the underlying system you’re trying to build.”

Rebuild

You’ll likely reserve a full rebuild for only your most important apps, because it’s typically a multi-year investment with a more comprehensive scope across the entire application. A comprehensive rebuild like this brings major UX improvements. For instance, it enables your developers to support a multi-channel, multi-device CX that better attracts, engages and retains your end-users. At the same time, they’ll gain the ability to leverage an end-to-end DevSecOps toolchain for maximum efficiency and reduced time-to-market.

Since these rebuilt workforce or customer apps will be cloud-optimized, your company also benefits from the full extent of cost optimizations possible with multi-cloud models, rather than being locked into a single IaaS provider. Finally, cloud-native apps make it easier to exploit advanced identity capabilities in order to gain world-class, zero trust security.

Okta supports zero trust infrastructure access at Personal Capital

PERSONAL CAPITAL

[Personal Capital](#), a digital-first wealth management company, managed more than US \$12 billion in assets as of May 2020, with over 2.5 million users. To support the growth and scale of the business while keeping financial data secure, the organization operates a robust cloud architecture, running both customer-facing applications and backend services on Amazon Web Services (AWS). After successfully deploying Okta's workforce identity solutions to secure user access for apps such as G Suite and Slack, the technology team implemented an elegant, scalable solution for accessing its cloud infrastructure securely.

"It was a challenge to dynamically provision the right identities, roles, groups, and associated public Secure Shell (SSH) keys while spinning immutable infrastructure up and down at scale"

— Maxime Rousseau, Chief Information Security Officer, Personal Capital

Without a unified layer for access control, the team had to either build their own connective tissue or add bolt-on access technologies, which would present adoption, compatibility, and scaling issues.

Okta Advanced Server Access (ASA) streamlines core Okta authentication workflows to Linux and Windows servers and gives Personal Capital's operations, security, data science, and engineering teams a seamless, secure way to access their critical AWS infrastructure. Rousseau's team relies on the Okta API for automating identity operations, including creating new projects, enrolling servers, and adding or removing users from groups. "Okta's API allows us to maintain control of a highly elastic cloud environment without a lot of management upkeep," said Rousseau.

"Okta Advanced Server Access was the right choice for Personal Capital because it simplifies secure server access while eliminating the need for additional technologies, manual integration, and static keys," said Rousseau. By solving for all policy requirements with one technology, Personal Capital avoids brittle manual integrations and much of the traditional operational burden that comes with infrastructure. "We have no account synchronization to worry about, no static credentials that can be stolen and/or misused," said Rousseau. "We can see who accessed what, from which machine, and when."

Replace

The fifth strategy is valuable if your business is looking to shift towards a cloud-first, best-of-breed SaaS ecosystem to better meet its workforce's needs. Because cloud-based providers make software their sole focus, these apps tend to be highly intuitive, with consumerized features that are hard to replicate via in-house development.

Specialized SaaS apps also eliminate common app management burdens, such as manually building integrations or brittle customizations, conducting software upgrades, adopting the latest security innovations, and other maintenance.

All of these cloud benefits free up your team to put their time towards tools and features that deliver the most critical functionality for employees, customers, or other users. Finally, since all clients share the operational costs of multi-tenant SaaS tools, they are more affordable than homegrown apps.

By leveraging an independent identity platform with thousands of pre-built SaaS integrations, you can establish a single source of truth for all identity types and automate account provisioning and deprovisioning—further improving your business' security posture. For customer apps, in particular, consider taking advantage of Okta's out-of-the-box sign-on widget, or go deep with our CIAM APIs that offer full branding customization (either of which will create a frictionless authentication experience for your users).



[Dentsu Aegis Network](#) is a multinational creative services firm that recognized how cloud-based apps could improve security while increasing the organization's agility and flexibility. With this philosophy in mind, the company developed its Digital 2020 initiative—a strategy for migrating the company's entire IT infrastructure by 2020—while also moving towards zero trust security.

“We're transitioning completely away from global data centers, while also making sure our new tools are all cloud-based or cloud-friendly from the start”

— Paul Timmins, CIO of Global Operations, Dentsu Aegis

With their rapidly growing ecosystem and shift to the cloud, the traditional network perimeter-based approach to security was no longer sufficient. Phase 1 for Dentsu Aegis involved choosing a core set of apps to secure with SSO. The company selected a few best-of-breed solutions, including Office 365, Workday, Tableau, ServiceNow, and Zoom. They deployed 15 applications to 45,000 users across 130+ countries over a single weekend. “Our roll-out was a testament to Okta. Changing a user's log-on experience is quite a critical action, especially when you're working with 45,000 identities over the course of a weekend,” said Timmins. “With Okta, we managed to do it seamlessly.”

The company rolled out Adaptive MFA with Okta Verify at the same time, making it easier for employees to access their work tools from anywhere, and on any device, whether they were logging in via Android, iOS, or even Apple Watch. In Phase 2, Dentsu Aegis set up automated onboarding and offboarding by rolling out Okta Lifecycle Management and establishing Workday—its HR system of record—as the single source of truth.

Now, when HR adds, removes, or changes a user identity in Workday, the action feeds down through the company's entire workflow, provisioning the user with all the apps they need to do their jobs on Day 1 and reducing provisioning-related security vulnerabilities.

"Okta, with its consumer experience and its very easy-to-use framework, has helped us empower staff without adding security overhead," says Timmins. With Okta at the core of Dentsu Aegis' cloud strategy, employees are staying productive with convenient access to their favorite apps, and the IT team can rest easy in knowing that all endpoints are secure, no matter who is requesting access, where they're working, or what device they're using.

Retain

Some applications aren't worth moving to the cloud, either because they're already targeted for future retirement, are simply a lower priority for migration, or contain very strategic intellectual property that your CIO wants to keep on-prem. While there's very little advantage to leaving older apps as-is without any cloud optimization, if that decision is made, it's still important to think about how you might improve security and the access experience.

There are several perks to protecting these apps with a cloud-native identity platform that makes it easy to secure your users and resources. For instance, you can add an identity layer to legacy apps with SSO and MFA, and give employees a simple access point for all of their cloud-to-ground resources in one portal.

Okta helps Hitachi secure legacy systems

HITACHI

As [Hitachi](#) has evolved its business model, its IT organization also changed their own processes—selecting cloud solutions over legacy options that created friction for employees and IT. Hitachi selected Okta Access Gateway to support its new hybrid environment. As a result, IT streamlined the user experience across the partner ecosystem and global employees, and deprecated their on-prem identity solution, realizing significant cost savings for the company.

In addition, as the company has continued to grow through M&A, Okta was instrumental in streamlining the process of migrating applications, improving the overall user experience, increasing security, and saving significant development costs.

"Our recent focus has been on transforming from a product-based company to a solutions and services-based company"

— Ashish Sanghrajka, CIO of Hitachi Americas and EMEA

"In order to enable our workforce to be productive and agile throughout this transition, we needed an IT infrastructure that was more scalable and cost-efficient, while keeping security a top priority. Okta Access Gateway was the right technology for transforming our legacy authentication infrastructure without disrupting the legacy systems."

Modern identity's role on the road to the cloud

A SaaS platform itself, the Okta Identity Cloud supports your organization's cloud journey by allowing you to shift various IAM workloads from on-prem legacy systems and components and reap the benefits of Okta's cloud-based [Universal Directory](#). Once you have this robust foundation in place, you can manage all of your organization's users and resources across a multi-cloud environment, and deploy several valuable capabilities that enable various IT modernization exercises, such as:

Single Sign-On, Multi-Factor Authentication, and the Okta Integration Network

Today, Okta is the de facto standard for agile, cloud-based SSO, and offers the largest, most reliable network of over 6,500 pre-integrated apps. With these powerful identity features in your toolkit, you can easily move off of intermediary directory and access management systems like LDAP or Active Directory Federation Services, gradually replace older apps with newer alternatives, and retire RSA and hardware tokens as you implement adaptive, intelligent MFA with Okta Verify.

Access Gateway (OAG)

With OAG, you can bring modern SSO and adaptive MFA to on-premises applications without changing code. This allows you to reduce identity infrastructure up to 90% by replacing deprecated on-prem web access management (WAM) systems like CA Siteminder, IBM Tivoli Access, and Oracle Access Manager. As a result, you'll diminish the operational burden surrounding identity, while adding SSO, adaptive MFA, and intelligent security from the cloud for legacy apps that you want to retain indefinitely.

Advanced Server Access (ASA)

Designed to power security for elastic cloud infrastructure, ASA extends the Okta Identity Cloud to servers, treating them as downstream applications. In doing so, it brings unified identity and centralized access controls to any hybrid or multi-cloud environment. ASA manages access to both Linux and Windows servers across Amazon Web Services, Google Cloud Platform, Microsoft Azure, or on-prem infrastructure, abstracting the complexities of IAM at scale.

You'll achieve rapid time-to-value as you rehost more and more applications in your portfolio and need to quickly spin up and secure new servers. And since Okta lets you automate the lifecycle of privileged server accounts and policies across your dynamic fleet of infrastructure, you'll be able to consistently maintain your security posture as developers come and go.

API Access Management

Most new custom apps are built with an API backend, and moving to the cloud introduces other APIs and API gateways (Mulesoft, Apigee, and others) into your ecosystem—each of which must be secured. Okta's API Management solution provides one place for API administration with an identity-driven policy engine and complete standard-compliant support for OAuth 2.0.

This allows your developers to centrally create, maintain, and audit all API access policies across both workforce and customer apps. By also taking advantage of Okta's mobile SDKs to leverage reusable business logic surrounding identity, they can focus on rearchitecting or rebuilding core app features as opposed to worrying about underlying identity components or login pages.

For more information about how Okta can support your cloud migration strategy for both workforce and customer applications, visit <https://www.okta.com/initiatives/customer-identity/modernize-infrastructure/>.

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