E-book

Accelerate Your Cloud Migration (at Any Scale) with Okta and AWS

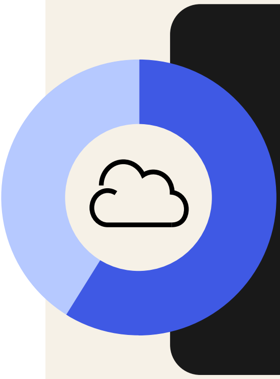
Use strong Identity and Access Management to get your teams quickly and securely to all their AWS resources

okta

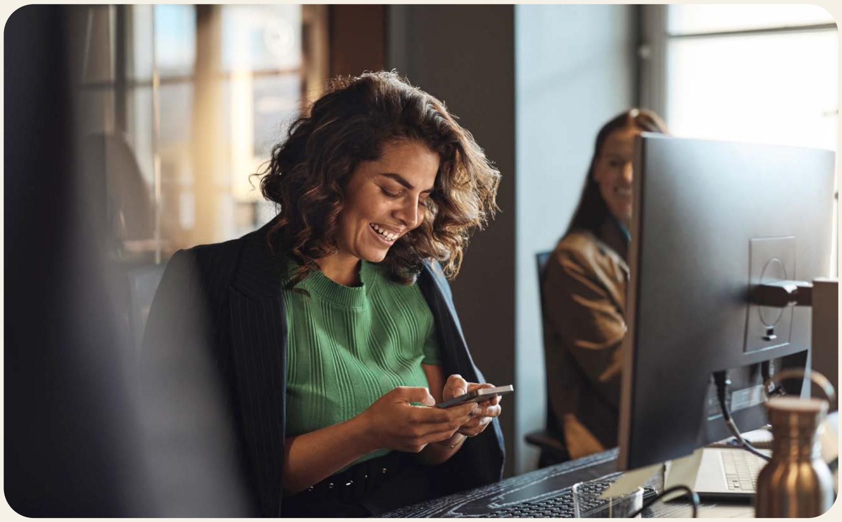
aws

Evolving Drivers of Cloud Adoption

For many enterprises, migrating on-premises enterprise apps and resources to more efficient cloud solutions has become a business imperative. Organizations embracing the cloud are reaping the benefits of lower costs, higher productivity and seamless accessibility for their dynamic hybrid workforces. Shifting your applications to the cloud —quickly, safely, and efficiently—is now a competitive necessity.



In 2024, **65%** of organizations cited cost efficiency or savings as their top metric for measuring progress in the cloud.[1]



[1] **Source: State of the Cloud 2024 Report, Flexera**

Today, enterprises need to support flexible workforces that can work from anywhere, at any time, on any device. Organizations need centralized control over access, and the ability to be able to quickly scale operations up or down as these workforces and their projects fluctuate. And they need to provide frictionless experiences across channels, for their workforces as well as for their customers. In this way, businesses can encourage customer engagement, create new revenue opportunities, secure employee loyalty, and build trust.

Moving to the cloud is pivotal to meeting these needs. The challenge is getting there thoughtfully and at scale, while overcoming barriers like IT inefficiencies and the extended security threat surface presented by the cloud.

The key to making it happen? Smart, safe, and efficient cloud migration with Okta and AWS.

Strategies for successful cloud migration

For many enterprises, digital transformation starts with an audit of current on-premises applications, and some key decisions about what, when, and how to optimize these for the cloud while minimizing cost and disruption.

As technology leaders review their app portfolios, determine how to address myriad demands, and work to reduce capital expenditures (CapEx) along the way, there's no one-size-fits-all approach. The best cloud strategy for each app depends on its budget, complexity, criticality, and other factors.

For **workforce apps**—that is, apps used by your internal employees, contractors and partners—additional considerations might include prioritizing apps that support emerging phenomena like remote, dynamic, and mobile work requirements.

For **customer apps**—that is, consumer-facing apps and APIs —companies might prioritize apps that support strategic ends like deploying or scaling personalized, relevant, cohesive omni-channel experiences that help grow and retain revenue.

Whatever specific pressures are driving your organization to move workloads to the cloud, there are several methodologies that can help you make the right choices. Experts at Gartner and Amazon Web Services (AWS) divide the approaches for technology leaders into these seven categories. (We'll delve into each in more detail later in this document.)

Retire

Retain

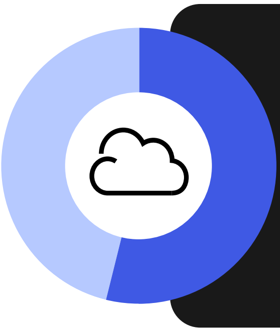
Rehost

Relocate

Repurchase

Replatform

Re-architect



54% of organizations reported understanding app dependencies as their top cloud migration challenge.[2]

[2] **Source: State of the Cloud 2024 Report, Flexera**

1. Retire

This is the migration strategy for the applications that you want to decommission or archive, perhaps because there is no business value in retaining them, you want to eliminate the cost of hosting them, or they use an operating system that is no longer supported.

2. Retain

There may be some on-premises applications in your digital portfolio that you need to leave as is—either for the long term, because they're too sensitive or mission-critical to be touched, or until later phases of an overall app retirement strategy.

3. Rehost

To speed the pace of migration, tech teams often employ a 'lift-and-shift' strategy where possible, by simply moving some apps and workloads to run in the cloud without optimizing them.

4. Relocate

Using this strategy you can transfer a large number of servers comprising applications from an on-premises platform to cloud, or from one cloud to another. During relocation, the applications continue to serve users, minimizing disruption and downtime.

5. Repurchase

For older or outdated apps (whether commercial off-the-shelf or homegrown), the solution is often to replace them with best-of-breed, cloud-first SaaS solutions like Salesforce for CRM, Workday for HR, AWS for a variety of networking services, and Okta for Identity and access management (IAM). This solution opens up new possibilities for integrating multiple cloud-first services, such as Okta and AWS.

6. Replatform

Also known as ‘lift, tinker and shift’, this strategy involves moving an application to the cloud with some degree of optimization to ensure it operates efficiently or to take advantage of cloud capabilities.

7. Re-architect

In this scenario, teams materially change an on-premise app’s underlying architecture to fully embrace cloud-optimized techniques: for scale, business continuity, performance, and other improvements. Making nontrivial changes to your application before rehosting it in the cloud takes time, but typically results in a more powerful cloud-first solution.

Should you re-architect?

Check if your application shows symptoms that it’s ripe for rebuild, like an ageing UI, insufficient features, low ROI, security vulnerabilities or high maintenance costs. Cloud migration will often not be the main reason to rebuild an app, but a supporting argument to other business goals.

The strategies above identify the options available, but each enterprise has to strategically decide on its own complex mix: as business models and budgets evolve, as legacy apps diminish in value, as customer and employee situations change. Whatever your journey, centralizing Identity management and access control is critical to successful cloud migration – helping you safely and efficiently provision your users, secure your resources, and accelerate your adoption of a Zero Trust security posture.

Key Considerations for Efficient Cloud Migration

Before selecting a migration strategy for each of the apps in your tech stack, we recommend creating a detailed technical, operational, and business profile of each application. It can be helpful to use a consistent framework for making those decisions.

Across the Okta and AWS common customer base, we have seen leaders focus on five top factors when moving apps to the cloud.

Security

- How well does this approach improve our security posture?
- Can we now adopt modern techniques, standards, and protocols—like phishing-resistant multi-factor authentication (MFA), OAuth, and OpenID Connect?
- Can it be easily managed and updated without having to rely on developers?
- How can we tighten controls to ensure least privilege and just-in-time provisioning?
- How can we harness AI to boost our resilience and response to threats?
- How can we strengthen the security of critical assets?
- Will I be able to gain visibility across all of the layers of this 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)?

Future-proofing

- To what extent is usage of this app expected to grow?
- How important is it to keep it up to date and integrate it with other cloud services?
- How important is it to improve access for people working remotely?
- How will this strategy help protect the app from evolving security threats?

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

As today's work-from-home reality multiplies user identities and cloud projects, IT teams are often spending more and more time managing AWS users, accounts, and roles. But there's a better solution: using Okta to manage AWS resources, either through Account Federation or Single Sign-On (SSO). This allows you to leverage existing Active Directory or LDAP credentials and give an entire workforce—wherever they are, whatever device they're using—the access they need to their AWS resources at every point in the employee lifecycle.

Each worker gains secure, one-click access into all their AWS resources, from AppStream to Developer to Amazon Marketing Services and more, via the Amazon Web Console or the Command Line Interface. This access evolves automatically as employees onboard, change roles and groups, and offboard, with all changes in Active Directory automatically flowing to Okta and AWS. Together with passwordless authentication, phishing-resistant MFA, and Privileged Access Management to protect your most critical assets, you can strike the right balance between robust security and a seamless user experience. No more password sprawl and reset fiascos, no more teams stalled waiting for resource access, and no more wasted IT time provisioning and reprovisioning dozens or hundreds of users manually.

Organizations can go even further with AWS IAM Identity Center (SSO), adding request-based access to AWS entitlements as part of Okta Identity Governance. With Okta and AWS integrated, assigning permissions and access rights can be reliably automated based on roles and rules, tapping into the granular capabilities of the tech stack without overburdening your existing IT Team.

To help companies avoid common pitfalls across the seven migration strategies mentioned earlier, we've gleaned best practices and recommendations from the many Okta and AWS customers who've leveraged this integration to accelerate their cloud migration. Here's what we've learned.

Retire

Embarking on a cloud migration program is an opportunity to decommission applications that are no longer useful or needed by your business. These apps could be creating a security risk because they use an OS that is no longer supported, or may simply be ‘zombie applications’ sitting on your systems barely being used but costing you money to maintain and host.

The best way to identify zombie or idle applications is by scrutinising their utilization and performance data. Any application with an average CPU and memory usage below 5 percent is likely to be ripe for retirement. Okta’s detailed usage reports and insights from Okta Identity Governance will help you identify which applications have little to no usage. Once you’ve made a decision to decommission, Access Management allows you to safely deactivate applications while ensuring that any residual data or access points are properly managed and secured.

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 to 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, Okta lets you add an Identity layer to those legacy apps with SSO and MFA, and give employees a simple access point for all of their cloud-to-ground resources in one portal. The Okta Access Gateway enables your IT team to manage and secure on-premises applications without changing the source code, providing seamless access to these as well as cloud applications.

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 your cost and efficiency gains will be limited by your technology team's existing application stack and development processes.

A rehost is an opportunity to rethink some of the common components that bolt into your applications to improve their security and usability. Okta's solutions are well integrated with AWS and can simplify and secure app rehosting in a multitude of ways. They allow you to replace on-prem Identity components with cloud-native hybrid IT access management and apply consistent Identity management across environments. They centralize and automate AWS provisioning decisions via AWS IAM Identity Center (SSO) or federation. They enable secure server access while allowing you to remove intermediary directory or access management systems, such as LDAP. And they enhance security by supporting ephemeral admin access and Zero Trust integrations with your investments in cloud network security, observability and device security.

Relocate

Relocation involves moving a large number of servers, comprising one or more applications, at a given time from your on-premises platform to a cloud version of the platform, or a different virtual private cloud (VPC) or AWS account. The advantage of this approach is that users can continue to access applications without disruption, as no rewriting, re-architecting or operational changes are required.

Although the existing architecture is preserved, relocation can introduce security and compliance vulnerabilities as workloads are shifted from one environment to another. A modern Identity platform can mitigate these risks by centralizing Identity management and applying consistent access control policies across all environments, including secure management of privileged accounts through features like Okta Privileged Access Management. Okta's federated Identity model also allows users to access applications on AWS with their existing credentials, simplifying the relocation process.

Repurchase

This strategy is valuable if your business is looking to shift away from expensive and problematic homegrown apps and towards a cloud-first, best-of-breed SaaS ecosystem. 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—by shifting them to the third-party app developers—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 Okta's independent Identity platform, with thousands of pre-built integrations, you can quickly adopt new SaaS applications, establish a single source of Identity truth across your tech stack, and automate account provisioning and deprovisioning—further improving your business' security posture. Identity Governance ensures new applications adhere to existing access policies and compliance requirements, and Identity Threat Protection automates threat detection and remediation, protecting identities from the start.

Replatform

A replatforming strategy is useful where an application would benefit from some optimization, for example a change to the operating system or database, allowing you to achieve efficiency improvements, avoid licensing costs or take advantage of cloud capabilities.

This approach is more complex than a straight lift and shift, but also gives you an opportunity to considerably enhance the security and usability of key applications. For example, you can strengthen security with phishing-resistant adaptive MFA, and implement AWS IAM Identity Center (SSO) to provide more convenience for users. Automating lifecycle management with Okta Identity Governance also ensures swift and secure access, faster deployment and lays the foundation for easier scalability. To mitigate the risk of a data breach during the replatforming process, Okta Identity Protection with Okta AI continuously evaluates users and their sessions to assess risks, detect threats and respond to them as soon as they happen.

Re-architect

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 AWS's elastic Infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) for cost optimization and growth. This effort delivers positive ROI through accelerated digital transformation and massive gains in agility and adaptability.

With minor code changes, you can also adopt Okta-supported modern Identity protocols, like OpenID Connect (OIDC) and OAuth, for enhanced security. 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). Security can be further enhanced with Identity Governance to enforce access policies consistently, and Privileged Access Management to secure access to critical systems.

With a robust Customer Identity platform, you can also support deeper integration with your CRM, call center, and customer data hub systems. You can even streamline and secure access to legacy apps that aren't yet ready to be moved to the cloud, by integrating them with Okta Access Gateway.

Key Customer Integrations

Case Study: Okta and AWS for GitLab

GitLab specializes in web-based, open-source code and DevOps lifecycle tools. As the business experienced unprecedented growth, securing its dispersed team and complying with regulatory requirements was a must. But with a large network of users, provisioning and deprovisioning accounts and access across the company's increasing number of apps was difficult and it had little visibility into individual devices. To achieve its goal of a full-scale Zero Trust framework, GitLab selected Okta as its Identity provider. Thanks to Okta Single Sign-On and the Okta Integration Network, GitLab gained an Identity solution that could seamlessly integrate with its many SaaS apps. Okta Lifecycle Management also automated onboarding and offboarding for an unlimited number of users, offering the scalability GitLab needed after growing from 300 employees to 1,200 in a single year. For more details, check out the full case study here.

> "Without a product like Okta, you really can't achieve that Zero Trust model."
>
> Bryan Wise, Vice President Head of IT
>
> GitLab

Case Study: Okta and AWS for Siemens

Siemens is a dynamic engineering and manufacturing company with a presence in more than 200 countries. Its nearly 300,000 employees focus on intelligent infrastructure, automation and digitization, including transportation efficiency solutions, delivered through Siemens Mobility Services. To modernize its legacy IT department to lean into future solutions, Siemens shifted to Amazon Web Services (AWS) for its flexible platform-as-a-service solutions, and Okta as its cloud-first Identity provider. Since shifting to the AWS platform with access secured by a range of Okta's Identity solutions including Single Sign-On and Multi-Factor Authentication, Siemens has enjoyed increased access visibility, a streamlined user experience, reductions in helpdesk requests and unplanned customer maintenance, and simplified and accelerated cloud deployment across more than 100 apps. For more details, check out the blog here.

> "We use Okta to secure our departments' entire development environment. That includes our AWS login, multiple AWS accounts, our secure login, and continuous integration and development tools."
>
> Friedrich Gloeckner, Team Lead Architecture
> and Software Development
> at Siemens Mobility Services
>
> SIEMENS

Case Study: Okta and AWS for Cengage

From modest beginnings as an educational textbook publisher 100 years ago, Cengage has evolved into one of the largest and most digital-forward US-based education and technology organizations. Millions of students and educators have come to depend on Cengage 24/7 for secure and reliable access to digital learning resources, and Cengage recognized it needed to scale its platform quickly to meet this growing demand. But scaling up to handle hundreds of thousands of simultaneous logins while maintaining a great user experience for all was a daunting challenge. Cengage chose AWS to provide flexible infrastructure they needed to scale operations in the cloud, and Okta's Identity solutions, including Single Sign-On and Multi-Factor Authentication, to keep the experience smooth for students and other users, even at peak usage times. Together, the integrated AWS and Okta solution helped Cengage continue to grow while staying focused its core mission of developing young minds. For more details, check out the full case study here.

> "Moving to Okta has allowed us to take some of our best and brightest engineers, who were working hard on solving the Identity problem, and let them not have to worry about it...
>
> Those teams are now able to develop new features, improve personalization, build Cengage's subscription service, and improve the student learning experience."
>
> George Moore, Chief Technology Officer Cengage

Conclusion

The Okta and AWS integration allows enterprises to safely accelerate their cloud migration, by establishing an Identity-based Zero Trust security foundation and centralizing and automating access control and administration over AWS resources. The combination of Okta and AWS covers a wide range of AWS technologies, enabling seamless and secure user and customer experiences across all aspects of your organization.

For IT admins:

- Provide secure, intuitive Single Sign-on user access to all of your teams' AWS accounts and resources
- Centrally view and control enterprise access, automating permissions based on policy-based controls around user groups and roles
- Apply strong MFA to secure access to Amazon WorkSpaces and other AWS applications including Amazon Chime, Amazon QuickSight, Amazon WorkMail, Amazon WorkDocs, and Amazon AppStream 2.0
- Sync user information from HR systems like Workday and UltiPro, simplifying management and audit compliance

For developers:

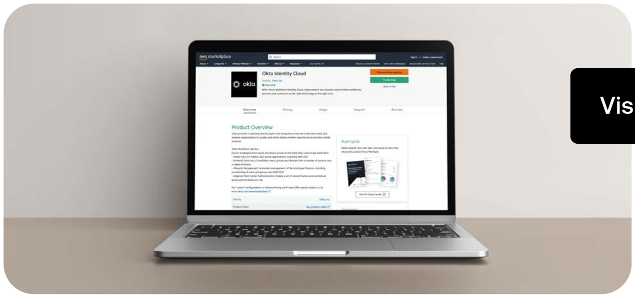
- Bridge the gaps between partner AD/LDAP and legacy SAML Identity Provider infrastructure to applications built on AWS so partner employees can authenticate with their AD/LDAP
- Take advantage of rich user and group information to authorize granular access to your applications built on AWS
- Enable team members to authenticate with their Okta credentials, safeguarded by phishing-resistant multi-factor authentication, and access your AWS accounts through the AWS Command Line interface (CLI)
- Integrate a single-page app, new portal, or mobile integration with Okta authentication and authorization for added security and a secure, seamless customer experience
- Adopt social authentication, OpenID Connect, and other authentication options for a more secure and convenient user experience

For DevOps:

- Provide secure, easy, and appropriate access to cloud resources, while simplifying and automating access management
- Use Okta’s Privileged Access Management (PAM) to enable Zero-Trust access into AWS EC2 instances, replacing risky static keys and frustrating role-switching with session-based authorization that centralizes control
- Give your DevOps secure, easy access to the AWS Console, using AWS SSO or Account Federation for a single place to manage Identity permissions
- Allow Okta and AWS SSO users to login once with Okta credentials to access AWS resources via the Command Line Interface (CLI)

For Government:

- Provide secure, audited infrastructure and processes with certifications including FedRAMP ATO, FIPS 140-2, HIPAA, SOC 3, IL4, IL5 and more (Okta also supports PIV/CAC for authentication)
- Ensure compliance and security features that meet government needs. View Okta service certifications here.



Visit Okta in AWS Marketplace

About Amazon Web Services (AWS)

Amazon Web Services (AWS) is the world’s most comprehensive and broadly adopted cloud platform, offering over 175 fully featured services globally. Millions of customers — including the fastest-growing startups, largest enterprises, and leading government agencies — trust AWS to power their infrastructure, become more agile, and lower costs. To learn more, visit aws.amazon.com

About Okta

Okta is the World’s Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology — anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We’re building a world where Identity belongs to you. Learn more at okta.com

okta

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