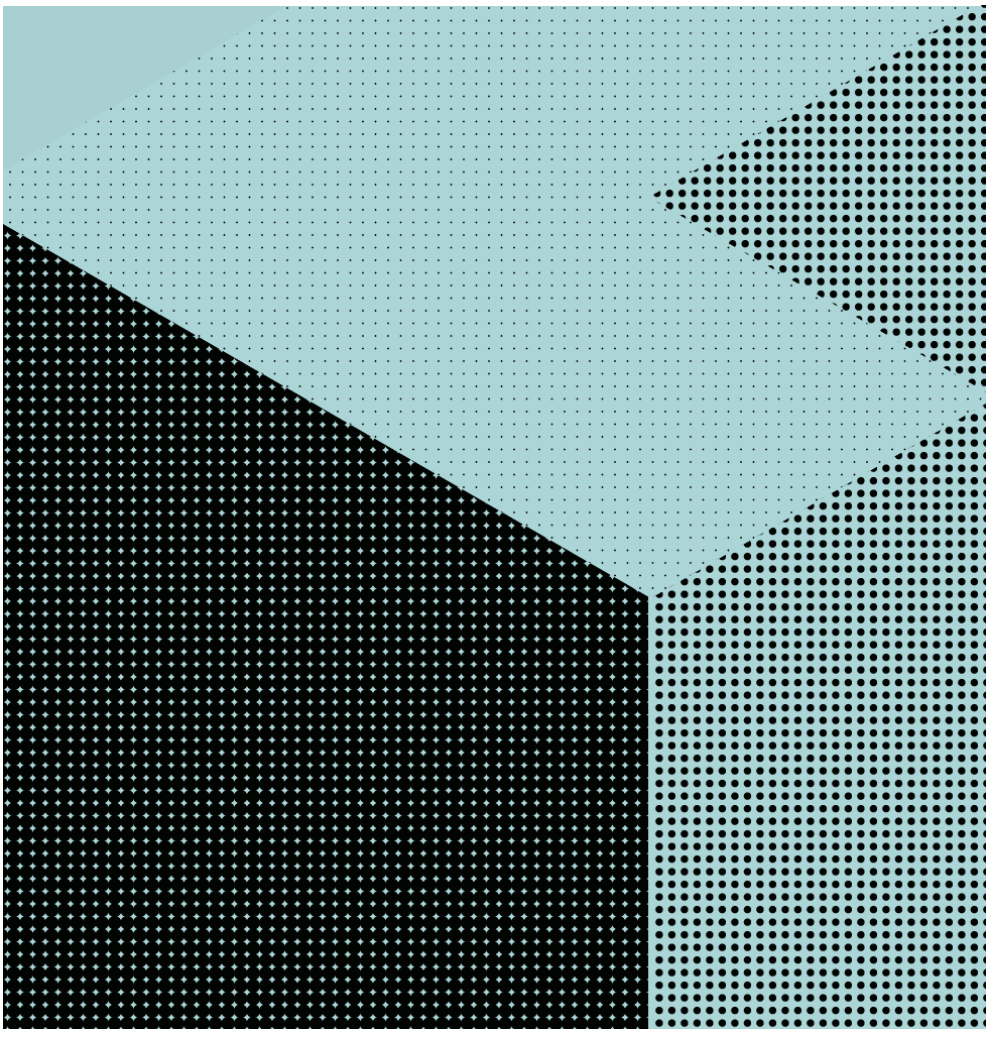
April 2021

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



okta

Okta and AWS

Contents

Evolving Drivers of Cloud Adoption

For a lot of enterprises, migrating on-premises enterprise apps and resources to more efficient cloud solutions was once a long-term goal. That timetable has rapidly accelerated, thanks to a shift to dynamic hybrid workforces plus increased demand for high quality digital employee and customer experiences. Today, migrating your applications to the cloud—quickly, safely, and efficiently—is a higher priority 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

In the new normal, 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.

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

Popular Strategies for Cloud Migration

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

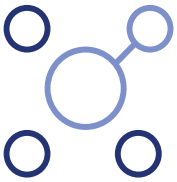
As technology leaders review their app portfolios, determine how to address myriad demands, and work to reduce capital expenditures (CapEx) along the way, there's no one-size-fits-all approach. The best cloud strategy for each app depends on its budget, complexity, criticality, and other factors.

- For workforce apps, additional considerations might include prioritizing apps that support emerging phenomena like remote, dynamic, and mobile work requirements.
- For customer apps, 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 modernize its on-premises ecosystem, there are several methodologies that can help you make the right choices. Experts at Gartner and Amazon Web Services divide the approaches for technology leaders into these six categories. (We'll delve into each in more detail later in this paper.)

1. Rehost

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



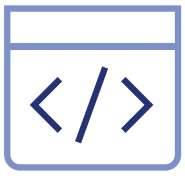
2. Revise

It's often advisable to update certain components of apps—like load balancers, databases, certification management, or zero trust network access tools—with a more cloud-friendly "lift, tinker, and shift" approach, leveraging managed services where feasible while retaining the app's core source code.

3. 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.

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



4. Rebuild

With a rebuild strategy, your developers start over from scratch to create your highest priority business-critical apps. This most draconian approach allows you to write off long-term technical debt and convert outdated tools into true, cloud-native applications.

5. Replace

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. Retain

Of course, 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.

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. But whatever your journey, the goal is clear: Migrating to cloud is about centralizing identity management and access control so you can safely and efficiently provision your users and secure your resources.

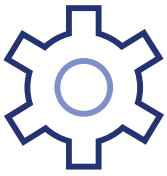
Key Considerations for Efficient Cloud Migration

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 Okta and AWS' common customer base, we have seen leaders zero in on four top factors when deciding what, when, and how to move apps 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?
- 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)?

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 the world's new work-from-home reality has multiplied 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. No more password sprawl and reset fiascos, no more teams stalled waiting for resource access, no more wasted IT time provisioning and reprovisioning dozens or hundreds of users manually.

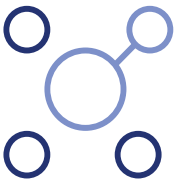
Organizations can go even further with AWS SSO, automating the provisioning of AWS entitlements as part of defined Okta Workflows. With Okta and AWS integrated, actions like these can be reliably automated based on roles and rules, tapping into the granular capabilities of the tech stack without overburdening your existing IT Team.

To help companies avoid common pitfalls across the six 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.

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 plus scalable network solutions from AWS can increase your impact in a rehost scenario: first, by replacing on-prem identity components with cloud-native hybrid IT access management, and second, by centralizing and automating AWS provisioning decisions via AWS SSO or federation. The integration also enables secure server access while allowing you to remove intermediary directory or access management systems such as LDAP.



Revise

A revise strategy involves updating specific components of an application so you can expedite innovation and achieve total cost of ownership gains by making small changes to your application. By updating DevOps processes (for example, supporting secure, intuitive Command Line Interface access for DevOps teams) and further leveraging AWS’ 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 by applying Okta’s 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.

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 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 Okta-supported 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.

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 built-in efficiencies of AWS's 100% elastic infrastructure, and cloud-native apps make it easier to exploit advanced identity capabilities—like Okta's Advanced Server Access (ASA) in order to establish and maintain world-class, zero trust security.

Replace

The fifth 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 an ever-growing set of thousands of pre-built SaaS integrations, you can establish a single source of identity truth across your tech stack, 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 deeper with CIAM APIs that offer full branding customization (either of which will create a frictionless authentication experience for users).

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.

Key Customer Integrations

vivint.Solar

"Instead of paying $170,000 in Active Directory user CALs, I'm paying a fraction of the cost in subscriptions for cloud services. Okta makes this huge cost savings possible."

—Mike Hincks, Director of IT Infrastructure at Vivint Solar

Case Study: Okta and AWS for Vivint Solar

Vivint Solar in 2015 moved from a traditional, on-prem IT model to 100% cloud, developing custom sales tools on the Amazon Web Services platform. But their IT team experienced difficulties deploying and managing cloud apps and infrastructure with its on-premises identity solution. By partnering with Okta, Vivint Solar was able to move the password store from AD to Universal Directory, and sync with Workday as a master for employee attributes, pushing the data out to apps and automating employee onboarding and offboarding. To support AD-dependent apps, Vivint Solar was now able to use AWS-hosted AD, saving hundreds of thousands of dollars in licensing and infrastructure. The Okta integration consolidated data, offered customers more value, and helped Vivint Solar measure an ROI of more than 900%. For more details, check out the full case study here.

SIEMENS

"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

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 full case study here.

ellucian

"AWS is an essential element of our cloud deployment strategy. AWS enables scale, flexibility and resiliency—and Okta enables us to manage access for our large population of AWS users effectively and efficiently."

—Lee Congdon, CIO at Ellucian

Case Study: Okta and AWS for Ellucian

Ellucian is one of the world's leading providers of software and services that power the essential work of more than 2,500 colleges and universities in nearly 50 countries, serving more than 18 million students. But internal access to essential cloud-based applications was proving cumbersome. They needed to increase IT efficiencies and provide secure, seamless access to cloud-based AWS applications for an ever-growing number of employees as well as its global customer base. By consolidating access on AWS through Okta Identity Cloud, Ellucian was able to reduce user friction, streamline their login experience, efficiently onboard and offboard employees, and make it easy for employees and customers alike to securely access their AWS and other applications. For more details, check out the full case study here.

CENGAGE

"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 at Cengage

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.

Conclusion

The Okta and AWS integration allows enterprises to safely accelerate their cloud migration, by establishing 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 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
- Make use of Social Authentication, OpenID Connect, and other authentication options

For DevOps:

- Provide secure, easy, and appropriate access to cloud resources, while simplifying and automating access management
- Use Okta's Advanced Server Access (ASA) 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:

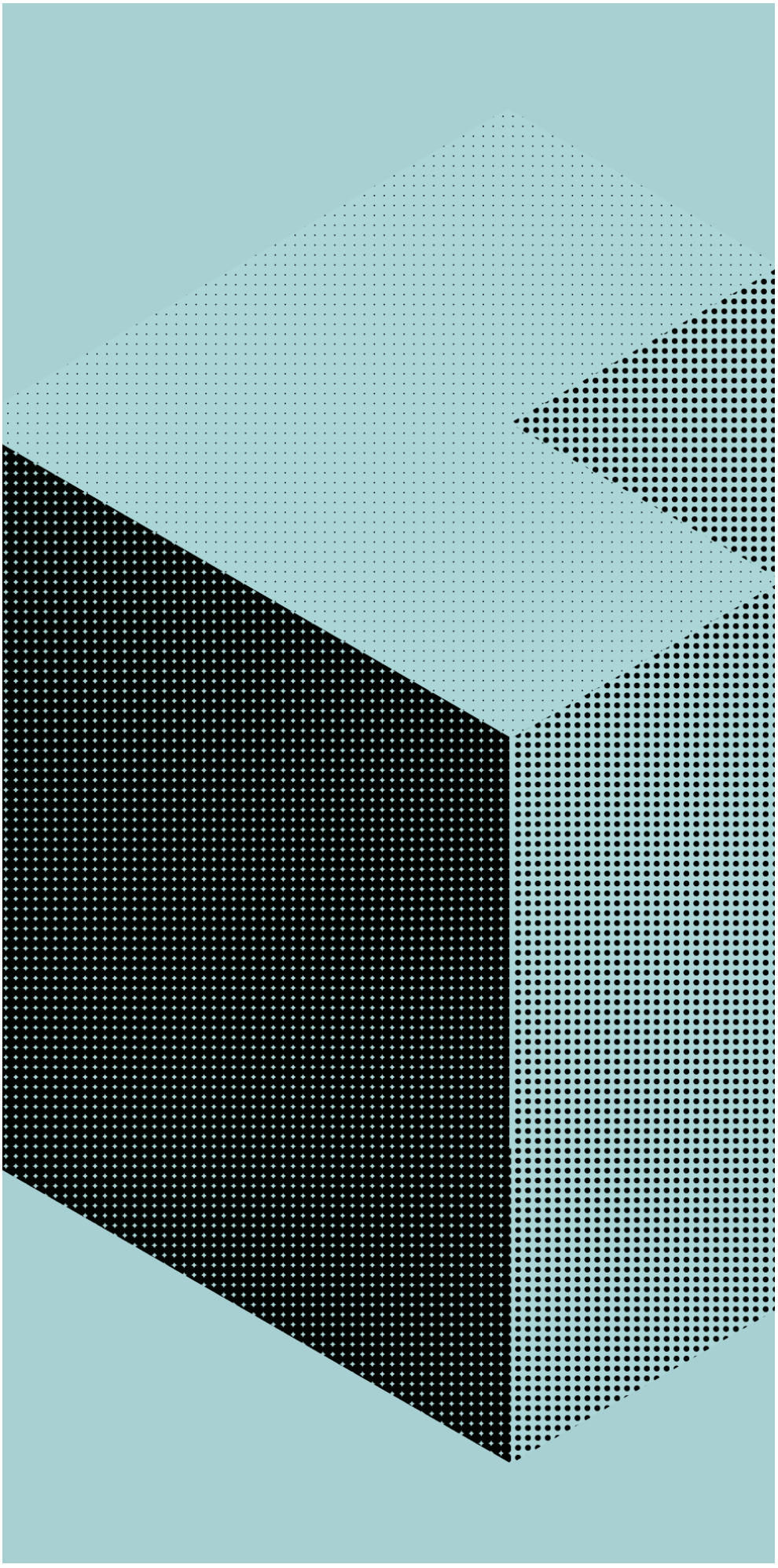
- Provide secure, audited infrastructure and processes with certifications including FedRAMP ATO, FIPS 140-2, HIPAA, and more (Okta also supports PIV/CAC for authentication)
- Ensure compliance and security features that meet government needs

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 10,000 organizations, including JetBlue, Nordstrom, Siemens, Slack, T-Mobile, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. To learn more at **www.okta.com**.

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**.



Visit Okta in
AWS Marketplace

aws marketplace