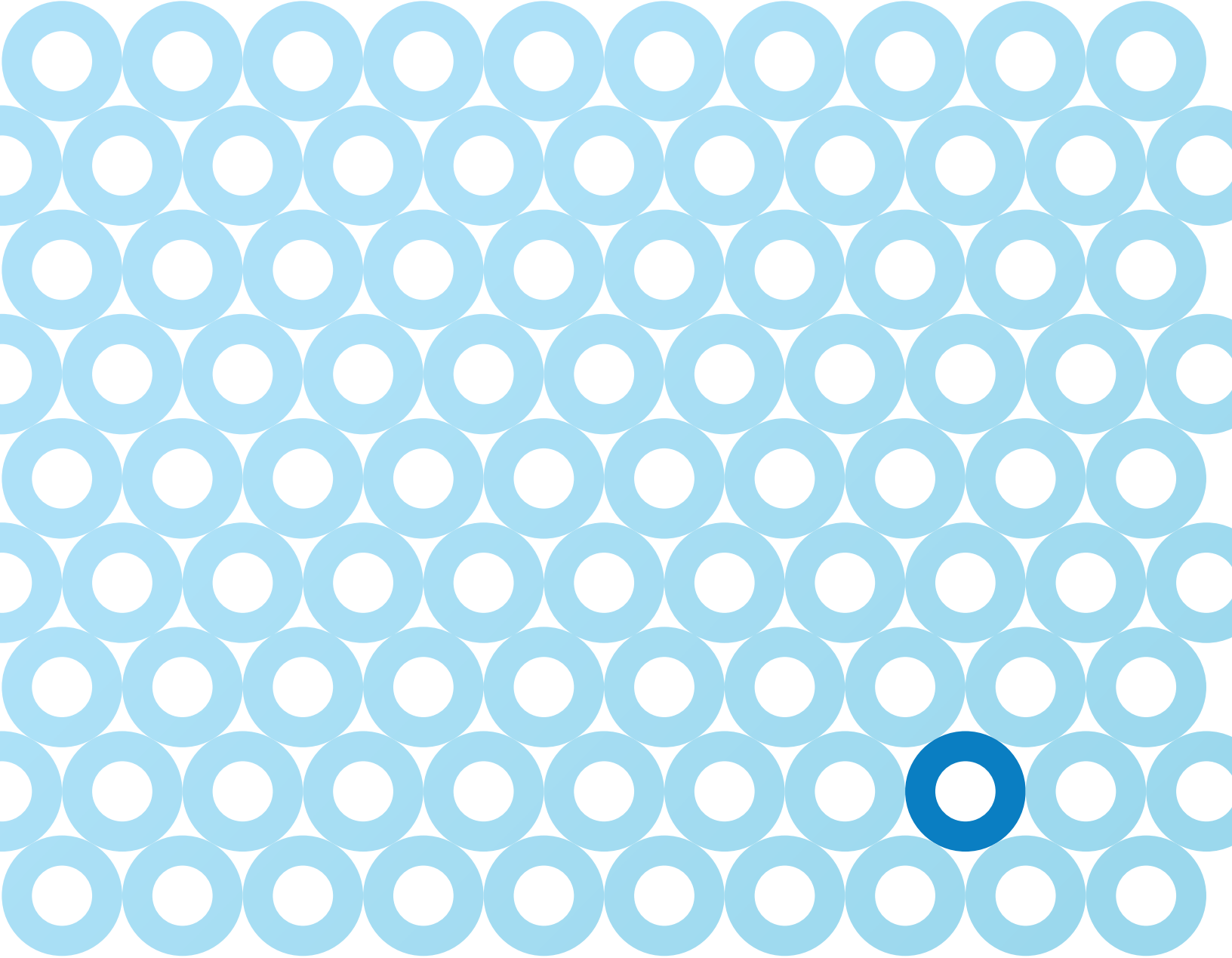
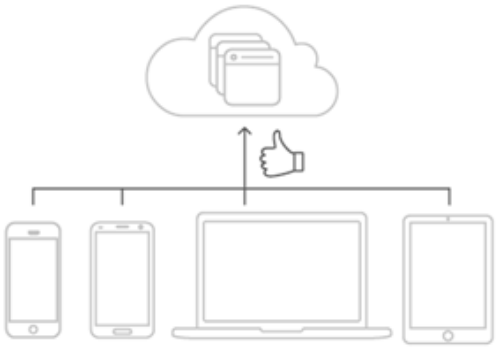


okta | aws

Staying Ahead of the Curve with a Foundation for Cloud-first IT

Welcome to the department of Yes

Gone is the notion of command and control IT, where all devices, applications, and user experiences were dictated centrally. Adoption of the Amazon Web Services (AWS) Cloud, with a boost from the Okta Integration Network, has enabled organizations of all sizes to start saying "yes" more often to business groups and end users. New marketing app? Yes! New tablet? Yes! New special-purpose project management tool? Absolutely!

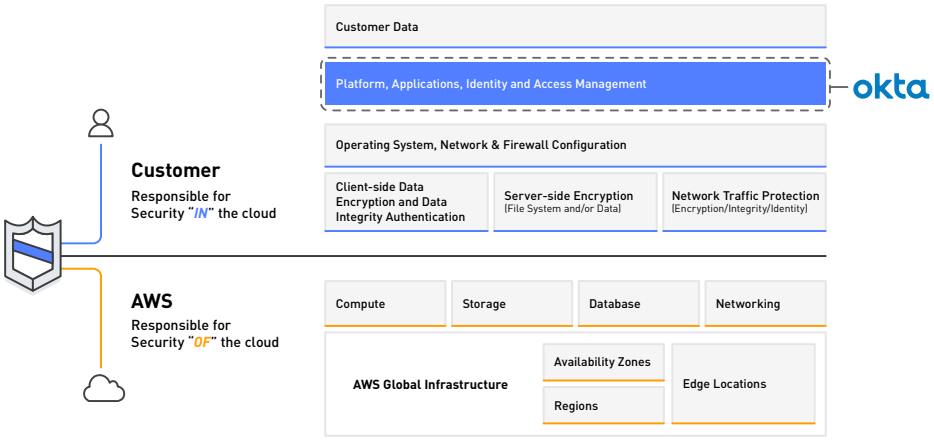


With all these yeses, the number of cloud apps an organization uses explodes. Customers tell us that before they purchase Okta, they typically have five to seven cloud apps. Within six months of purchasing Okta, customers connect 10 applications, with 10% of Okta customers eventually connecting more than 40 applications. In the Okta Businesses @ Work report, we found that the average Okta customer has 13 cloud applications.

Putting these cloud applications into use brings new opportunities to streamline the connections between your organization and your workforce, business partners, and customers. With these new opportunities come new logistical challenges.

Connecting apps for single sign-on (SSO) and automating provisioning for IT apps like email and ITSM are great, but really just the start. As you get deeper into automating the identity lifecycle for your full catalogue of cloud and web applications, you start seeing the complexities of having a truly secure system.

It's important when operating on the AWS Cloud to understand which cloud security aspects are handled by AWS, and which are your responsibility. As you see in the diagram below, AWS manages security of the cloud, security in the cloud is the responsibility of the customer. You retain control of what security you choose to implement to protect your own content, platform, applications, systems and networks, no differently than they would for applications in an on-site datacenter.



With all these yeses, the number of cloud apps an organization uses explodes. Customers tell us that before they purchase Okta, they typically have five to seven cloud apps. Within six months of purchasing Okta, customers connect 10 applications, with 10% of Okta customers eventually connecting more than 40 applications. In the Okta Businesses @ Work report, we found that the average Okta customer has 13 cloud applications.

Integration to Apps is Not Enough

Okta's unique role in managing the identity lifecycle for thousands of organizations enables us to look at trends in our customers' use of AWS services and apps to gain a deeper understanding of what organizations need. We recently found that organizations were not using as many provisioning integrations as they could be. Of the applications they had connected for single sign-on, there were several where Okta had a provisioning integration as well, but the customer had not enabled provisioning for that app.

The root cause of this low usage of provisioning integrations was that IT needed additional "intelligence" around identity lifecycle management and governance in order to automate more applications. IT organizations spend a lot of time just keeping track of who should have access to what, and at what time, and for how long. Keeping up with application requests from users as well makes their job even more difficult.

And finally, business teams often have their own application admins that can manage users without the knowledge of IT. IT needs to be able to keep an eye on overall changes within an application and sync those changes back to Okta or correct them in the app.

There are four scenarios in which IT needs to manage secure access to cloud applications.

First are "birthright" applications like email, expenses and ITSM that are provisioned to everyone in the company, and which often have similar entitlements. However, since these are core IT applications, they require rich synchronization of attributes. They are often heavily tied to the process around employee onboarding and offboarding.

The second group are DevOps apps like the AWS Management Console, PagerDuty, and JIRA. These are often provisioned based on a business unit—like CRM being provisioned to a salesperson, or a marketing demand gen app to someone in marketing. Users can also have multiple AWS accounts to manage with much more nuanced entitlements, based on role, seniority, or other factors. Often, the knowledge of how a user should be provisioned sits with an admin in the business unit—not someone in IT, let alone on the identity team.

Third are business partners and suppliers. These applications contain data that pertains to the suppliers, distributors, and retailors that your organization interacts with on a regular basis. These partners will need access to only specific data, meaning you need to ensure that they can only access what they're meant to.

Fourth are websites and applications that your customers use directly. These customers are looking to securely access your website or application without requiring an arduous login process. Customers want this streamlined, low-effort app access while also trusting that you'll keep their sensitive information private and secure. There are clearly many deeper issues to solve here in order to operate an efficient IT shop in a cloud-first world. The common thread across these issues is identity lifecycle management.

Integration to Apps is Not Enough

The need for digital transformation is here for most businesses today. Whether you're just beginning the process and are far into your modernization initiatives on the cloud, Okta has a host of solutions that create a cohesive security solution throughout your organization.

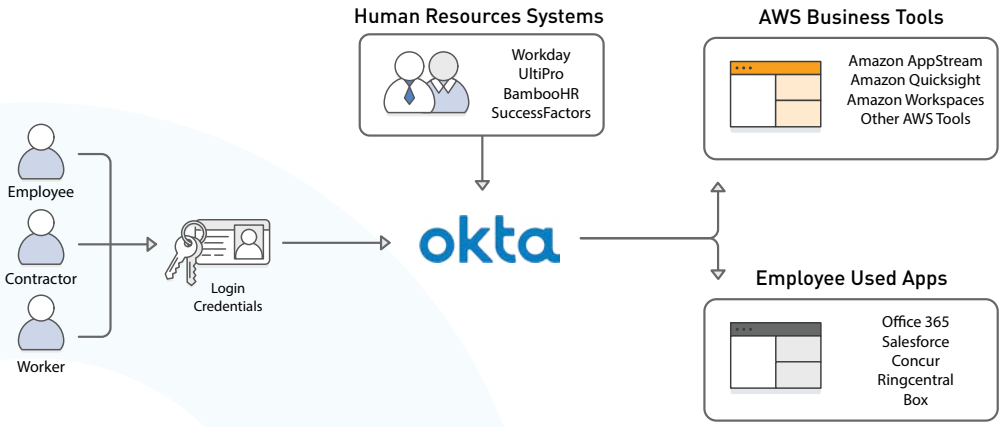
IT leaders and administrators consistently provide feedback to Okta that efficient identity lifecycle management is the absolute foundation to IT on the cloud in the drive for digital transformation. It determinations who has access to what—everything else proceeds from there. VPN access, MFA policy, BYOD policy, and application access entitlements all depend on the foundation of user lifecycle management. To achieve full adoption of provisioning, you have to solve lifecycle management across your organization.

Okta and AWS offer a solution for the modern world. Created with insight from across our customer base, Okta uses the best practices of efficient IT organizations and implements them with easy-to-configure options. With Okta on AWS, IT can get the most out of the largest network of deep provisioning integrations.

Below are some examples of how Okta implementation can have far-reaching effects throughout your organization.

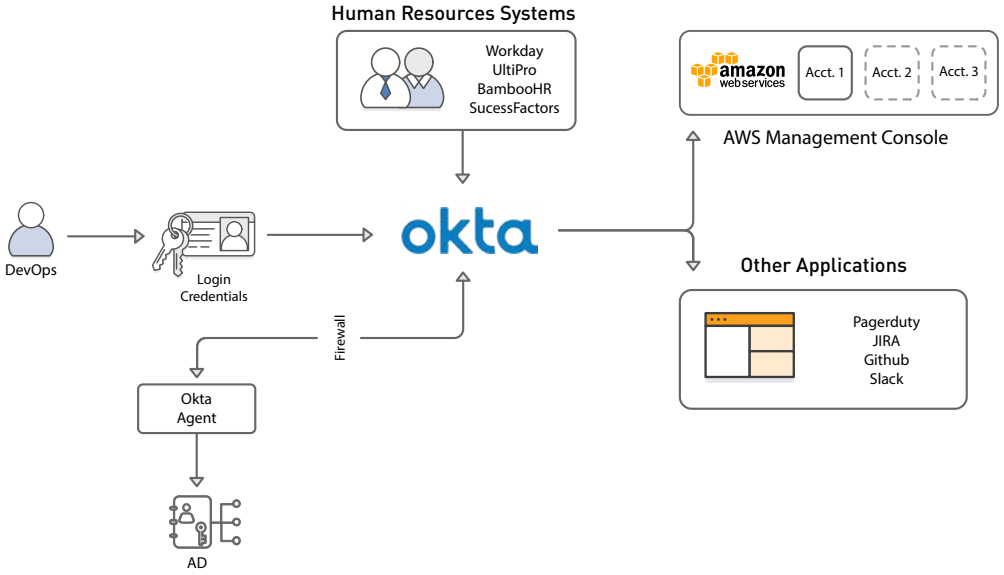
Simplify Employee Access to AWS and Other Cloud Based Services

Efficiently provide and revoke secure application access to your employees and contractors as their roles change.



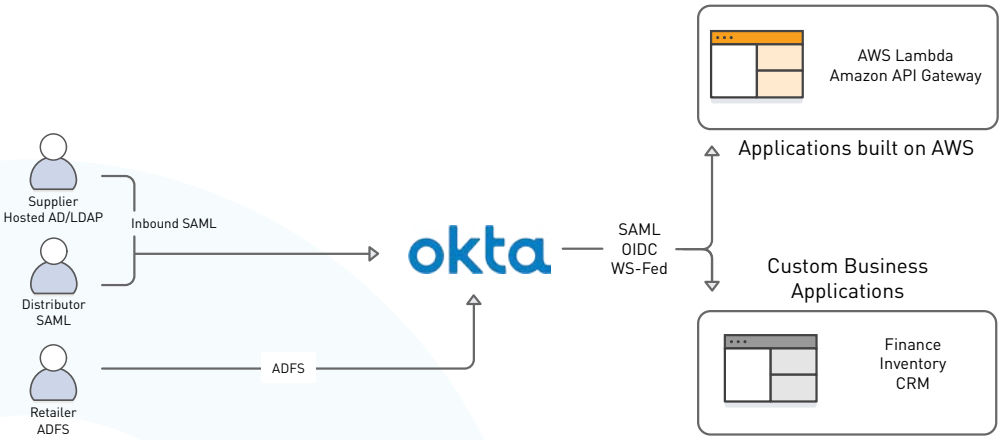
Secure Access to the AWS Management Console

Secure access to your AWS Management Console, with multiple AWS accounts and cross-account roles.



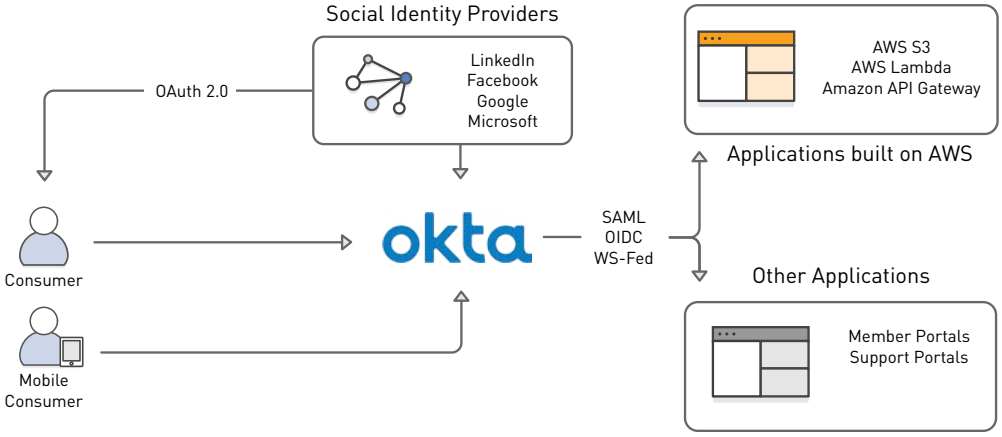
Secure Access to AWS for Suppliers and Partners

Grant business partners and suppliers secure access to only the data they are meant to access.



Streamline User Access to Cloud-Based Applications

Allow customers to securely access your website or application with requiring an arduous login process.



A lifecycle management engine helps drive the process around provisioning. It enables IT to orchestrate more of the onboarding process, automate how users are assigned groups, provide flexibility for how business applications are provisioned, and provide admins in the business with more power in the provisioning process. Organizations can then build on this foundation with Okta Adaptive MFA and Okta Mobility Management, to make IT more agile and secure.

About Okta

Okta is the leading provider of identity and mobility management solutions for the cloud and mobile enterprise. By harnessing the power of the cloud, Okta allows people to access applications on any device at any time, while still enforcing strong security policies. It integrates directly with an organization's existing directories and identity systems, as well as 4,000+ applications. Because Okta runs on an integrated platform, organizations can implement the service quickly at large scale and low total cost. Thousands of customers including Adobe, Allergan, Chiquita, LinkedIn, and Western Union, trust Okta to help their organizations work faster, boost revenue and stay secure.

For more information, visit us at **www.okta.com** or follow us on **www.okta.com/blog.**

About AWS

For 10 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers more than 90 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 42 Availability Zones (AZs) across 16 geographic regions in the U.S., Australia, Brazil, Canada, China, Germany, India, Ireland, Japan, Korea, Singapore, and the UK. AWS services are trusted by millions of active customers around the world monthly — including the fastest growing startups, largest enterprises, and leading government agencies — to power their infrastructure, make them more agile, and lower costs.

To learn more about AWS, visit **https://aws.amazon.com.**