Cloud Identity for Customer and Partner Portals

An Overview for IT Leaders

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

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

Introduction

There has never been a better time to be a CIO. In addition to traditional back-office responsibilities, IT is now increasingly the chief business enabler. When the marketing team demands insight into customer behavior, when the sales team requests new ordering capabilities in a mobile app, when the operations team asks to automate manual processes, and when every department requires a common way of identifying customers and partners, it's IT that delivers.

IT's expanded role is being pioneered by forward-thinking leaders in every industry. In aviation, airlines have moved loyalty programs to the cloud. In real estate, agent productivity is soaring thanks to new mobile and web-based tools. In software, companies are transitioning from selling packaged software to providing services in the cloud. From business-to-business initiatives like partner portals and mobile catalogs to consumer-focused projects like customer forums and mobile apps, IT is building value throughout the business.

In the past, integrating all these new initiatives into existing corporate infrastructures was a huge headache. Every new app or element of functionality required a notion of identity. Adding identity was expensive and slow. Initiatives that were meant to drive new business became a drag on operational efficiency and often failed for lack of adoption.

Fragmentation was a widespread problem. Each new project typically created at least one new identity. And some projects, like customer and partner portals, created multiple identities. This was a bad experience for users, who had to log in multiple times, and even worse for IT, which became responsible for operating, monitoring and patching each new system.

Fragmentation made it harder to secure the business. It created extra work—access rights had to be managed throughout the user lifecycle in multiple identity frameworks. Requests for password recovery alone piled up. And then there was the challenge of securing the code itself, making sure developers had followed best practices, scanning the code for vulnerabilities, limiting physical access to servers, and more.

Overcoming the Limitations of On-prem Identity with IDaas

IT leaders have responded to the challenges posed by legacy infrastructure and the shortcomings of on-premises solutions by adopting identity as a service (IDaaS). A cloud-based solution, IDaaS lowers the total cost of ownership, boosts security and provides a consistent user experience across an enterprise and its ecosystem of customers and partners.

By choosing Okta, the leading IDaaS provider, IT leaders have turned one-time impediments into opportunities. Apps that once suffered from low adoption are now generating new business Systems that were once security liabilities now function as the first line of defense against intrusions and breaches.

Below are examples of how IDaaS in general, and Okta, in particular, are helping IT improve performance across the organization while connecting with customers and partners.

Increased App Adoption and Engagement

Password fatigue has gotten so bad that the federal government is tempted to send in the troops. Last year, White House Cybersecurity Coordinator Michael Daniel said what he really wanted to do was "kill the password dead." Realistically, he said he'd settle for replacing it "with something that's actually easy for people to use."

As a business, the last thing you want to do is make it difficult for users to log in by asking them to remember multiple passwords or challenging them with cumbersome authentication processes.

IDaaS doesn't eliminate passwords, but it does make it easier for customers and partners to connect with your company by providing a single, cohesive user experience. Even if your existing infrastructure remains fragmented behind the scenes, Okta lets you lay a welcome mat in front of your digital front door. On the web, with Okta's Single Sign-On, users click once to sign in to everything. If they leave the web, they can continue to use that identity to interact with every part of your organization wherever they are— in the office, at a department store kiosk, or in a mobile app.

Rotary International experienced the benefits of IDaaS when it chose Okta to manage identity for the 1.2 million members of Rotary Clubs around the world. Rotary International had created a smorgasbord of web apps that allowed members to apply for grants, take advantage of e-learning curriculums, participate in webinars, and more.

> "What Okta is helping us do is lower barriers to adoption by making it easy for your everyday Rotarian to say I know how to get into this new functionality, I just use my same ID and password."
>
> *— Paul Markos, Chief Information Officer of Rotary International*

Streamlined Colllaboration

The secret to successful collaboration with customers and partners is flexible access management. One-size-fits-all approaches are doomed to failure. It's best to expect each customer or partner organization will have different needs, ranging from their own set of security requirements to administrative processes. Some organizations may want to directly administer users within your app, while others may want to manage access locally and federate into your application(s). Adding on-premises federation capabilities typically means someone on your IT staff will need to acquire the expertise to install and maintain a federation server. If that prospect is less than appealing, IDaaS not only provides an alternative to hosting, configuring and maintaining your own federation services, it also offers the additional benefits of scale and high availability.

Okta's centralized service offers the advantages of IDaaS along with the flexibility required to handle any scenario and any user population. Inbound Federation connects your app (or your portal, catalog, etc.) to any number of federated identity providers—then negotiates implementations and manages trust. Okta also supports auto-provisioning and self-registration so external users at customer or partner organizations can choose to simply add themselves into your system.

Once external users are added, Okta's Adaptive MFA ensures they can authenticate themselves with the factor of their choice. Okta offers a comprehensive selection of factors ranging from SMS to Okta Verify with Push and makes it possible to apply policies by group or to delegate access management to an administrator at a partner company.

Increased Operational Efficiency

IT leaders such as Gerri Martin-Flickinger, SVP and CIO of Adobe, report that the biggest efficiency gains from adopting IDaaS come from limiting IT's responsibilities. With IDaaS, IT does not need a dedicated team to take care of the hardware and software of identity systems. An IT employee does not have to be on-call to respond to problems with the systems. And IT does not need to worry about upgrading the systems to include new features or reflect changes in identity standards. By managing identity with Okta's cloud-based platform, it becomes much easier for customers and partners to do their own registration, onboarding, and credential recovery.

Adobe discovered the value of IDaaS for managing the identity of customers when the design-tools icon began its journey from selling packages of its Creative Suite software to offering subscriptions in the cloud in 2012. The first release of the Adobe Creative Cloud encountered a major hurdle. Many of Adobe's enterprise customers could not connect their corporate identity systems to Adobe Creative Cloud. To continue to use Adobe products, their IT departments needed to set up and manage an entirely new set of user credentials within the Adobe Creative Cloud. Needless to say, this did not make Adobe's customers happy.

Adobe turned to Okta to build a comprehensive identity management layer across the Adobe Creative Cloud for Enterprise. The connected solution federated identity information between Adobe and its customers, so administrators could quickly configure federation and users could access apps in the Creative Cloud using their existing corporate credentials.

> "Our company is full of engineers who build amazing products that work with creative magic. We don't have people who are IT professionals in identity and spend lots of time writing software. By implementing Okta's federated identity solutions, Adobe is freeing up resources to invest in the kind of creative magic our customers expect."
>
> *— Gerri Martin-Flickinger, SVP and CIO, Adobe*

Stronger Security

It is widely recognized that identity management and access control are vital in protecting a company from a data breach or malicious attack. This was the case even in the brick-and-mortar era. When a business opened its doors, it was invariably to an employee, customer, partner or vendor. What's changed in today's software-dominated world is that access is not only being granted to people but to devices and apps as well.

Securing a company's perimeter involves recognizing all manner of digital entities who are showing up at a multitude of entry points. Fragmented systems simply can't supply effective protection in this environment. Active users end up with the wrong permissions while users who should have been deactivated retain their access. The loss of critical data is almost inevitable.

One of the primary ways that IDaaS increases security is by providing centralized management of user authentication and access rights. Okta gives IT a single place to manage users and access to web and mobile apps.

By taking advantage of Okta's Adaptive MFA, Okta's customers are able to take a proactive approach to security. As part of the Okta platform, big data analytics is applied to authentication data from thousands of customers and millions of authentication events, allowing IT to automatically serve up the right level of assurance at the right time. For example, Okta can detect high-risk behavior patterns and require additional authentication factors while customers who conform to historical usage patterns can log in without extra steps.

Behind the scenes, Okta takes a comprehensive approach to securing identity infrastructure that is hard for individual companies to match. From physical and network security to secure engineering practices and personnel controls, every aspect of security is taken into account and extensively audited and certified by third parties.

For customers, it adds up to a simple argument. Okta can keep identity information safer than they can.

> "Okta has been tremendous and transformational for the way we do business and secure our applications."
>
> *—Stanislav Burdeynyy, IT Lead Systems Engineer at Zuora*

The Okta Difference

Okta doubles down on what's most important to IT: high availability, industry-leading security, and unlimited scalability. Because Okta's sole focus is delivering identity and mobility management as a service, Okta's infrastructure is extremely robust in terms of redundancy, security, and scale.

High Availability

With 99.99% availability, Okta is committed to being available to any application, any device, and any user, at any time and from any part of the world. Anyone can monitor Okta's uptime performance at okta.com/trust.

Deep Security Expertise

The Okta Platform is built, operated, and maintained by security experts, and security is a priority at every level. All controls are independently audited, and Okta is SSAE (SOC 2) Type 2 certified.

Unlimited Scalability

The Okta Platform allows companies to connect with an unlimited number of customers and partners anywhere in the world and to securely use any application on any device.

Okta Offers Rich Product Functionality

Universal Directory	A single source of truth for all users
Direcory Integration	Secure, lightweight integration with Active Directory & LDAP
Social Authentication and Profile Sync	Secure social login support
Inbound Federation	Standards-based federation enhances the user experience
Single Sign-on	A comprehensive solution that integrates new apps in minutes
Adaptive MFA	Strong, flexible, user-friendly authentication
Provisioning	Fully extensible provisioning to external services on-prem and in the cloud with built-in connectors

Conclusion

A single, integrated platform, built 100 percent in the cloud, Okta is designed to help IT leaders achieve broader objectives by assuming the responsibility for handling identity in all its forms. The Okta platform allows stakeholders throughout an organization to add a reliable, secure, and scalable layer of identity to any application or portal and to engage customers and partners. Compared to alternatives, Okta also offers much more rapid time to value. Okta encourages adoption, streamlinescollaboration, reduces cost and ensures everyone is more secure.

About Okta

Okta is the foundation for secure connections between people and technology. By harnessing the power of the cloud, Okta allows people to access applications on any device at any time, while still enforcing strong security protections. It integrates directly with an organization's existing directories and identity systems, as well as 4,000+ applications.

Thousands of customers, including Adobe, Allergan, Chiquita, LinkedIn, MGM Resorts International 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.