Building Highly Scalable Apps: A Modern Identity Solution for Modern Businesses

We've all heard the adage "every company is a tech company." This means that organizations of all shapes and sizes are building digital apps to help streamline the delivery of products and services to end users. In today's tech landscape, developers are building apps on the cloud, or finding ways to migrate their existing infrastructure to it. Both these scenarios need authorization layers that secure the app with the added benefit of making it more scalable.

Part of deploying authorization in your app means incorporating an identity and access management (IAM) system with OAuth 2.0 protocols that outline fine-grained access policies for different user types. Responding to existing customer expectations of single sign-on capabilities, for instance, your app will also need delegated authorization workflows for integration with other applications. There are also various authorization use cases to keep in mind: does your app exist on multiple channels (e.g. web or mobile)? Will it integrate with third-party APIs?

With the rising complexity of developing in-house authorization in a cloud-based environment, businesses stand to benefit from an external customer identity and access management (CIAM) platform.

Challenges of In-House Access Management

IAM was once commonly built and managed in-house, but it's proving more difficult to fulfill customer expectations with an internal solution. Key challenges associated with in-house access management include:

- **An outdated customer experience.** Building in-house increases friction and slows down release dates, leading to a less-than-perfect customer experience.

- **Increased complexity.** A modern, secure, and seamless access management solution employs services like single sign-on (SSO), multi-factor authentication (MFA), and social login. This is necessary to combat today's sophisticated hackers and friction-adverse users, but when in-house developer teams fall into the rabbit hole of advanced features, it drains time that could be better spent on other projects.

- **Specialized experience.** Implementing standards such as SAML, OAuth, and OIDC requires specialized expertise that isn't necessarily important for your developer team's other activities.

- **High cost; low ROI.** When building in-house, developers must split their time and resources, rather than being able to focus on developing their core product. Especially as app usage scales, the identity component of the app becomes increasingly expensive to maintain.

- **Security threats.** On average, custom code accounts for 93% of app security vulnerabilities. That leaves your customers and users at risk.

In-house IAM challenges by the numbers

- Building your own identity and access management solution costs **4x more** than buying a solution with out-of-the-box functionality, according to a 2018 Forrester report.

- It's also **2x more** expensive to self-support ongoing maintenance.

- It can take up to **6 months** to build out identity and access management.

Offload Identity to a Trusted CIAM Solution

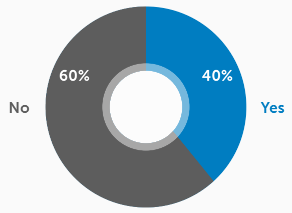
At its core, a CIAM solution enables organizations to capture and manage customer identity and data as well as control customer access to applications and services in a secure environment. At a minimum, your CIAM should manage the following tasks:

1. **Customer registration**
2. **Self-serve account management**
3. **SSO**
4. **MFA**
5. **Password resets**
6. **Access management**
7. **Data security and compliance**

To relieve some of the pressure placed on developers, many companies are leveraging third-party applications to take care of tertiary tasks such as billing and data tracking; however, they're lagging behind when it comes to IAM.

A recent report conducted by Pulse Q&A found that 40% of respondents built in-house customer authentication and/or customer identity processes without a third-party CIAM provider.

Have you built in-house customer authentication and/or customer identity processes without a 3rd party Customer Identity Management provider?



Scale Your App with Okta

A trusted name in identity and access management worldwide, Okta empowers organizations to scale their applications.

> *As an organization, we have clear objectives, one of which is to simplify the customer experience. Okta's smart authentication and contextual capabilities enable us to give our clients a seamless, secure online experience.*
>
> — Alain Goffi, Vice President, IT Infrastructures, National Bank of Canada

- **Get started in minutes.** Developers can hit the ground running with SDKs that have modern development environments and full protocol support. Hit your aggressive application development timelines and even accelerate time to market.

- **Reduce bottlenecks.** Okta provides identity and access management as a microservice, so applications are developed, maintained, and deployed independently.

- **Experience out-of-the-box compliance.** Rest assured that Okta's infrastructure is redundant and compliant with FedRamp, ISO, SOC, HIPPA, GDPR, and P2D2 standards.

- **Leverage best-in-breed security integrations.** Protect against breaches, fraud, and abuse with identity proofing, device fingerprinting, fraud scoring, and bot defense.

- **Scale with ease.** As your user base grows, so do the complexities of managing them. Okta is cloud native and designed to scale easily for any app.

Advanced Okta Solutions Come Out of the Box

Along with the basic features outlined earlier, Okta offers advanced solutions to ensure a seamless and secure customer experience no matter how many customers you acquire.

> *Okta, out of the box, satisfies all of the security and privacy requirements.*
>
> — Michael Rogers, Product Manager at Allergan

- **Embeddable authentication.** Provide your users with a frictionless, secure experience. Leverage Okta's prebuilt UI widgets for common user flows such as login, registration, and password reset, or build a completely customized experience with Okta's APIs.

- **Embeddable authorization.** Control which APIs your users and developers have access to using Okta's API Access Management. Customize claims and scopes, as well as insert external attributes using Okta's token extensibility.

- **User and policy management.** Manage your users and security policies programmatically via APIs or from our user-friendly admin console. Manage user lifecycles with automated onboarding and offboarding.

- **Developer efficient.** Ranging from "no-code" to "pro-code", get started with minimal development resources using Okta's hosted customization tools, or use Okta's SDK and REST API to build using the programming language and framework of your choice.

- **Production-ready.** Scale with confidence with guaranteed 99.9% uptime SLA. Monitor potential security threats in real-time with the admin System Log.

Okta is the identity layer that scales with your app

Okta Customer Identity is the leading identity service that enables apps to scale with user adoption. Flexibly apply authentication, authorization, and user management with APIs, SDKs, and out-of-the-box workflows with this developer-friendly platform.

For more information, visit www.okta.com.