Managing Identity So You Can Scale

okta

In today's market, the pace of innovation and technological change is unprecedented in its speed, scope and depth of impact. These innovations are occurring across all verticals and industries. Modern applications are delivering high quality customer experiences that are frictionless, personalized, intelligent, and offer users significant conveniences. In addition, there is a tremendous amount of innovation happening to the underlying technologies. Applications are becoming more powerful and quicker to bring to market with advancements in cloud infrastructure, data proliferation, connectivity between disparate systems through APIs, and a microservices architecture design pattern. All these innovations are changing customer expectations. Not only are customer expectations changing in how and where they are choosing to engage with businesses, but they also are changing with regard to what they expect products and services to be able to do.

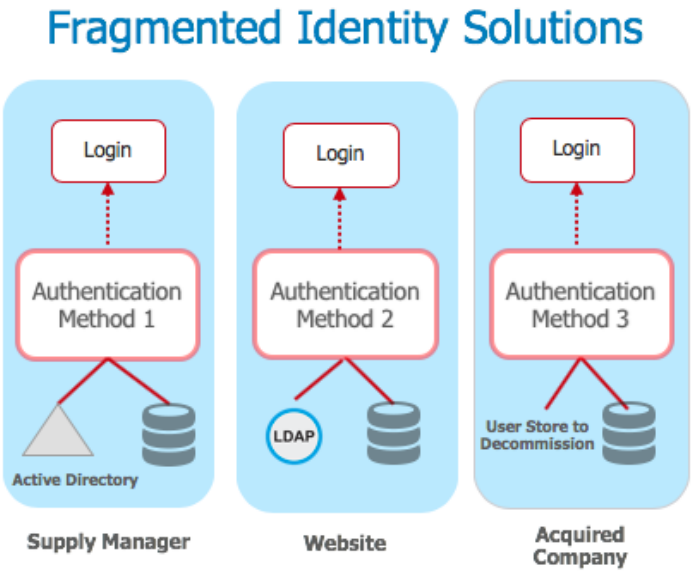
To meet the high expectations of today's customers, reduce development time of digital experiences, and eliminate potential security gaps, organizations need to put their customers' identity front and center. A modern customer identity and access management (CIAM) solution can do just that.

Building auth is hard

As customer experience becomes a C-level initiative, building out an authentication model for your apps from the ground up is not easy for your developers. From dealing with inconsistent user schemas to easing the flow of data between components, custom code for authentication leads to a number of problems.

With ***93% of app vulnerabilities*** stemming from custom code, maintaining a high standard of security without compromising on customer experience becomes increasingly difficult at scale. When building out authentication, large organizations typically have developers create fragmented identity solutions for hundreds of applications. When business units want to publish a new app, a local user store and user identity solution is often created leading to an identity nightmare, and a degradation of the customer experience.

As the number of applications proliferates, fragmented architecture prevents agility at scale. This leads to siloed user repositories, duplicated passwords, and siloed application stacks leading to a degraded user experience and weak security posture.



To make things worse, all this fragmented custom code causes significant technical debt. According to a ***2018 report by Stripe***, this 'bad code' costs companies $85 billion annually, with developers spending 17 hours a week dealing with maintenance issues. With developer productivity becoming a C-Level Initiative, enterprises with large scale applications should take a second look at building their authentication experience.

Focus on your core

Marc Andreessen in 2011 famously said, "software is eating the world." Today, the notion that every company is a software company is widely accepted. Every industry, every vertical, every business is either being run on software, delivered through digital channels, or enhanced with software. A new wave of technology providers are enabling companies and application developers to harness powerful capabilities and services through simple API integrations. These new API companies are fundamentally changing the

dynamics of how software is created, brought to market, and the speed at which it is created. The monolithic infrastructure of the past 20 years is being retired for the modern microservices design pattern. These rely on small, independent and reusable microservices that can be assembled relatively easily into more complex applications. As a result, developers can focus on their core functionality and surround it with fully functional, distributed processes developed by other specialists, which they then access through APIs.

Uber

There is no denying the scale at which Uber operates today. Uber, which launched in 2009, conducts more than 15 million rides each day with a network of over 75 million riders and 3 million drivers. At the center of their success is their famous mobile experience, which is powered by an infrastructure that processes billions of data points across their network and delivers real-time functionality to their users. To achieve this logistical feat, Uber relies on service specialists to power many of the key elements of their mobile application. Uber uses Amazon Web Services (AWS) for their infrastructure to be able to continuously operate without disruptions. For their mapping technology, Uber utilizes Google Maps to help riders and drivers find each other. Their messaging stack is provided by Twilio, ensuring you get that notification right when your driver arrives. They also send out emails and receipts for passengers with an email service that is built on SendGrid APIs. Uber leaves all these functional elements to the service specialists who focus on these areas as their core business, while Uber itself focuses on their core competency of delivering transportation to the masses.

Identity as a microservice

Every application needs a way to connect directly to the user and almost every app has an authentication component. A customer identity and access management (CIAM) solution is another such specialist service that provides a common set of fundamental features related to authentication, authorization, and user management. This provides application development teams the ability to increase speed-to-market, lower development costs, and focus in-house developers on the core features of the application while offloading the complexities of modern identity and access management.

Delivering on the needs of CIAM

A modern CIAM solution, provides a digital identity layer that can be embedded into your customer-facing apps and portals. There are four main capability pillars that a modern CIAM solution needs to deliver on when it comes to addressing customer needs:

- Frictionless user experiences
- Speed-to-market
- Centralization of access management
- Internet scale security

Frictionless user experiences

To successfully engage your customers and provide them frictionless experiences across all their devices, you need to know and understand your customers. You also need to be able to protect any of their personally identifiable information (PII) that you might store. You can't expect to retain customers for very long if their digital interactions with you are plagued with non-relevant content, inconsistent experiences, frustrating processes, or security concerns.

To deliver frictionless customer experiences, you need a 360-degree view of your customers as they come in from your various channels. To make that happen you need a secure, scalable cloud repository designed specifically to store and manage all of your customer information. Additionally, whether you're building out registration, login, or other common customer web-based workflows, you need to be able to customize those activities with your own branding and maintain consistent interactions.

MGM RESORTS INTERNATIONAL

MGM Resorts chooses to not only use Okta as its identity standard for managing and securing its workforce of more than 70,000 people, but also to provide a consistent and seamless identity layer for its millions of customers. MGM uses the Okta Universal Directory to securely store all of its customer data. Okta Single Sign-on enables MGM to ensure a customer only needs to sign in once to gain access to its mLife loyalty program and be seamlessly logged in to their various resort properties. Additionally, as MGM builds out modern apps for customers' smartphones and in-room tablets at their hotels, they'll continue to ensure consistent, seamless identity experiences for their customers using Okta's developer tools.

Speed-to-Market

As organizations build out new customer experiences, they want to bring those experiences to market fast. But if development teams have to build identity and security into those experiences from scratch, it can considerably slow down their speed-to-market. Like an identity Swiss army knife, developers need an array of CIAM development tools that work across modern programming languages; tools they can pull off the shelf as needed, whether they're building a web app, iOS app, or Android app. Developers also need identity and security to be future-proofed against an ever-evolving landscape of requirements and attack vectors.

Adobe

When Adobe began transitioning from a perpetual licensing model to a SaaS model with Creative Cloud, it recognized the agility, efficiency, and speed-to-market that Okta could provide its developers. Adobe wanted to give its enterprise customers seamless experiences when logging in, which meant integrating with enterprises' existing directories and identity providers. To enable that, Adobe first considered building integrations with their customers from scratch. Adobe product management quickly realized each of those integration efforts would take weeks to complete, which was far too long. To turn those weeks into minutes, Adobe instead leveraged the Okta Identity Cloud to become the identity layer for its Creative Cloud.

Centralization of access management

As the number of your customer experiences increase, it becomes essential to centralize all of your access control decisions organization-wide. Making and managing decisions on an app-by-app basis is inefficient and wastes time. It also leaves you vulnerable to security gaps as you lose the certainty of whether you're applying your access and security policies in a uniform manner across your entire enterprise.

In a CIAM setting you also must ensure you can consistently and securely implement those policies in the most frictionless manner possible. This requires contextual access management that can take into account factors like which app is being accessed, authentication attempts, location of access, time of access, strength of password, anomalies in customer behavior, devices being used, IP addresses, impossible travel scenarios and more. Additionally, the administrative user interface in Okta gives you one place where you can manage all your users, apps, groups, devices, APIs and policies. And it's intuitive enough for non-technical administrators to use, so you don't need to have high-salary developers manage those experiences.

experian

These types of capabilities were driving forces in Experian's decision to consolidate its identity management onto Okta, leaving behind the complexity and high cost of managing six disparate identity management solutions. To achieve greater operational efficiency, corporate IT at Experian also centralized IAM across its several business units spanning multiple geographies around the world.

Internet scale security

Critical to the experiences you provide to your customers is the ability to secure their access, as well as secure your infrastructure. That is why your primary objectives are typically to prevent or reduce breaches, and to be compliant with industry and geographic regulations that impact your interactions with your customers.

When securing customer access you need intelligent and usable security. Having secure access is worthless if the experience is so difficult and frustrating that customers decide it's too much work to engage with you. Strong security and great usability no longer have to be on opposite ends of the spectrum.

Modern CIAM with Okta Identity Cloud

Purpose built for the modern era, the Okta Identity Cloud offers a completely new category of technology that enables organizations to deliver secure, consistent digital experiences for their workforces, partners, suppliers and customers. It's a holistic IAM solution that seamlessly incorporates and unifies CIAM capabilities into a single technology stack that can transform your customer and workforce experiences.

Okta's simple-to-use APIs and out-of-the-box tools enable developers to create seamless experiences, while giving IT and security teams a central place to manage security policies. Okta's API Products serve as identity building blocks for your mobile or web applications providing several core services to accelerate the time-to-market of your digital transformation:

- **Embeddable Authentication—**Provide your users 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. Create single sign-on (SSO) experiences and manage the user lifecycle 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 with the programming language and framework of your choice.
- **Production Ready—**Scale with confidence with 99.99% availability SLA*. Monitor potential security threats in real-time with the admin System Log. HIPAA, FedRAMP, GDPR, and PSD2-compliant.

Resources

Why Software Is Eating The World, by Marc Andreessen
August 20, 2011
https://www.wsj.com/articles/SB10001424053111903480904576512250915629460

Company Information from Uber
Facts & Figures
https://www.uber.com/newsroom/company-info/

The Developer Coefficient from Stripe
September 2018
https://stripe.com/files/reports/the-developer-coefficient.pdf

About Okta

Okta is the foundation for secure connections between people and technology. Our IT products uniquely use identity information to grant people access to applications on any device at any time, while still enforcing strong security protections.

Our platform securely connects companies to their customers and partners. Today, thousands of organizations trust Okta to help them fulfill their missions as quickly as possible.
For more information, go to https://okta.com