okta

Bring Secure, Frictionless Customer Experiences to Market Faster with Modern CIAM

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

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

Bring Secure, Frictionless Customer Experiences to Market Faster with Modern CIAM 3

Delivering on the Needs of CIAM 3

Frictionless User Experiences 3

Speed-to-Market 4

Centralization of Access Management 5

Internet Scale Security 6

Modern CIAM with Okta Identity Cloud 7

Trusted and Future-Proofed Customer Identity and Access Management 8

About Okta 8

Bring Secure, Frictionless Customer Experiences to Market Faster with Modern CIAM

The way organizations interact with customers has evolved dramatically over the years, and will continue to evolve. Websites used to be an organization's main interaction point where customers could read some basic, static information about the organization's business. The explosion of different devices and communication channels has changed all that. In today's highly mobile world, 77% of U.S. adults own a smartphone and 53% own a tablet.[1] In response to that, 73% of U.S. marketers indicate they've designed their websites specifically with smartphones in mind and 50% have designed their websites with tablets in mind.[2] From the Internet of Things (IoT) to an array of other smart devices, customers also connect in a multitude of other ways to get access to digital services and consume dynamic content. And each time they connect, they expect a seamless, consistent experience regardless of the device or channel they use.

Customers also expect those experiences to be secure and private. The requirement for secure experiences has always been there for an organization's workforce, especially since it's in the best interest of the organization to safeguard its digital assets. But with all the different high-profile security and data breaches in the headlines, consumers' demand for greater security and privacy in regards to protecting their personal information and digital experiences has risen above what some organizations might have provided their workforces only a few short years ago.

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.

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 keep customers for very long if their digital interactions with you are plagued with non-relevant content, inconsistent experiences, frustrating processes, or security concerns.

[1] "Mobile Fact Sheet", Pew Research Center, February 5, 2018. www.pewinternet.org/fact-sheet/mobile/
[2] "The Next Mobile Decade", Adobe 2018 Mobile Study.

To be able to deliver frictionless customer experiences, you really need a 360-degree view of your customers as they come in from all your different 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, as well as with consistent interactions.

That's why 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 to also provide a consistent and seamless identity layer for its millions of customers too. 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 into all of the 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 its 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. Akin to 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.

To help developers focus more on core application logic, gain greater development agility, and get to market faster, Okta provides these much needed array of identity tools by making it quick and easy for developers to integrate Okta identity and security capabilities. That includes robust APIs with easy to use SDKs and developer tool kits built on open standards that span a wide array of modern programming languages. Okta also provides extensive documentation, wizards, quick start guides, and API management integration. You can even add modern identity capabilities into an app in less than 15 minutes by simply putting a hosted customizable Okta widget in front of your apps and portals.

All of these different developer tools help free up your developers to focus more of their efforts on building the core services for your apps and other digital experiences. They no longer have to worry about designing and coding common hacker-proof workflows to handle registration, sign-in, account recovery, forgotten passwords, MFA enrollment, and more. Developers also no longer have to worry about keeping up with evolving identity and security needs. With the CIAM platform that enterprises trust, Okta enables your developers to be as agile and productive as possible with security and privacy built in.

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 from scratch integrations with their customers. Adobe product management quickly realized each of those integration efforts would take weeks to complete, which was way 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 as to whether you're applying your access and security policies in a uniform manner across your entire enterprise.

For example, you might decide to increase your overall security posture by migrating from using text messages as your second authentication factor to a more secure biometric or push notification as your second factor. Implementing that policy change one app at a time not only can take a lot of time and effort, but you're likely to miss an update or two. Unfortunately, the discovery of that oversight won't likely come until a breach wreaks havoc on your reputation and financial standing. You eliminate that worry with centralization.

In a CIAM setting you also have to make sure you can consistently and securely implement those policies in the most frictionless manner possible. That requires contextual access management that can take into account things like what 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.

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. Your main objectives in these regards 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 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. Okta allows you to leverage a broad set of authentication factors combined with authentication threat intelligence and contextual response capabilities in adaptive MFA to create highly secure, frictionless customer access experiences. This includes the ability to introduce "responsible" password-less authentication that can use a biometric or push verification instead of less trustworthy passwords.

To help you with your security efforts, Okta dashboards and reports give you real-time visibility into what's happening in your IAM environment as recorded in the Okta System Log. Okta also makes that syslog data available to various analytics solutions, further enabling your response team to investigate and remediate issues as quickly as possible.

To further keep your customers secure, Okta takes a comprehensive approach to securing its own infrastructure with practices and processes that span its hiring practices, architecture, data center operations, and software development. It employs SOC 2 Type I and Type II processes to successfully audit its operational and security processes. It has achieved Cloud Security Alliance (CSA) Security, Trust, & Assurance Registry (STAR) Level 2 Attestation. Its ISO 27001:2013 and ISO 27018:2014 certifications attest to Okta's commitment to provide a secure service to its customers and to secure personally identifiable information (PII) in the cloud. In essence, Okta employs all these security and compliance best practices so you don't have to.

Additionally, Okta offers a HIPAA Compliant Service instance for organizations that serve the healthcare industry. For those who work in government circles, Okta has an official authorized status with the Federal Risk and Authorization Management Program (FedRAMP) Moderate authority to operate (ATO). Plus, Okta Threat Insight lets you leverage the authentication intelligence it has gathered from thousands of different organizations like yours, enabling you to make better access decisions for your customers.

> "Okta has demonstrated, not just to us, but to industry analysts and security experts that they take security very seriously, and that it's a service that we'll be able to trust."
>
> — **Den Jones, Senior Manager IT Services, Adobe**

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 three core services to accelerate the time-to-market of your digital transformation:

- **Embeddable Authentication**—Okta's prebuilt UI widgets let you create frictionless and secure user experiences with common user flows such as login, registration, and password reset, or build completely customized experiences with Okta's APIs.

- **Embeddable Authorization**—You can control which APIs your users and developers have access to using Okta's API Access Management. You can also customize claims and scopes, as well as insert external attributes using Okta's token extensibility.

- **User and Policy Management**—Okta lets you manage your users and security policies programmatically via APIs or from our user-friendly admin console. You can also create single sign-on (SSO) experiences and manage the user lifecycle with automated onboarding and offboarding.

In addition to the Okta CIAM solution, Okta provides an entire ecosystem around supporting your customer experiences. With more than 5,000 out-of-the-box integrations, Okta makes it easy to bring identity to various elements of your infrastructure. We provide integrations with applications like Zendesk and Salesforce to enable seamless access and synchronization of customer data. To facilitate modern application development you can take advantage of our support for API gateways. Identity proofing integrations improve identity confidence that your customers are who they say they are when higher assurance is needed. And integrations with network gateways such as F5 and Palo Alto Networks help support your customer-facing legacy on-premises apps.

Trusted and Future-Proofed Customer Identity and Access Management

The success or failure of your efforts to drive more business through better, more engaging customer experiences hinges largely on choosing a modern CIAM. Born in the cloud and supporting a best-of-breed technology stack, Okta Identity Cloud helps you ensure that success. Rooted in identity leadership that enterprises trust and agility that developers love, Okta allows you to build modern, frictionless, and secure customer experiences that can be brought to market quickly. It enables you to unify and consolidate all your IAM efforts across your enterprise for greater efficiency, security, and cost savings. Okta Identity Cloud gives you identity and security at internet scale that you can trust to address your IAM and CIAM concerns today and in the future.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device.

Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

Learn more at: www.okta.com


okta