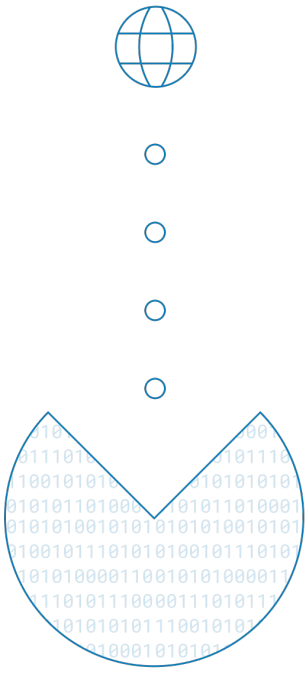
okta

Consumer Identity Management for the C-Suite



Software is Eating the World

Cloud. Mobile. Digital. It's hard to turn a corner today without hearing about the technology trends that are creating new markets and reshaping those in their wake. In a Gartner report from January 2020, 78% of CEOs believe their companies are industry pioneers or fast followers but their organizations have been slow to adopt many of the technologies and capabilities that generally define "digital transformation." While it's at the top of the CEO agenda, everyone in the C-suite has a role for a simple reason: It's hard to find an industry or sector in the economy that is not being disrupted by software. Software has gone from being an internal operational and employee productivity tool to being at the core of how companies operate and serve their customers.

When it comes to consumer businesses, customer expectations have changed. Consumers are demanding services whenever they want them, wherever they are, and on whatever device they're using at that moment. Further, businesses that once did the bulk of their business in person have had to figure out how to quickly pivot to seamless and secure digital experiences, while still remaining unique and compelling. Consumers want flexibility, personalization, and privacy simultaneously—and it's finally possible to satisfy them.

If CEOs today do not act with the speed and decisiveness necessary, they risk a more nimble “digital” company entering their market and establishing beachheads and chipping away at previously “safe” market segments. The strategy consulting firm, Innosight, concluded that 75% of the S&P 500 could be replaced due to “creative disruption” in the next 15 years. Companies that do not embrace digital will become commodity producers known for lackluster customer experiences at best, or at worst, will simply go away.

The Importance of Consumer IAM (CIAM)

As companies undertake ambitious innovation programs, they must choose tools that will both accelerate time to market and give them the flexibility to experiment over time. Innovation is never a linear process. In the best of times, it requires frequent experiments, quick feedback cycles, discarding bad ideas, and focusing on the useful ideas, hence agile development and a lean approach will yield the best solutions for customers quickly with as little wasted effort as possible.

Among the critical layers in any technology stack is the identity layer, which handles user onboarding, authentication, and overall user management. When identity management comes as an afterthought, customer experience is fragmented; users need separate credentials to log in to different applications, profile information is dispersed across databases, user activity is challenging to track, legal compliance is questionable, and security is at risk. And these problems grow over time as your teams and application portfolios change and grow.

Done right, a unified customer identity and access management (CIAM) driven approach makes it easy to launch new customer-facing applications faster, enables a cohesive and delightful user experience across channels, ensures the security of user accounts, improves compliance around sensitive personally identifiable information (PII), and drives marketing ROI through better understanding of users, targeting, and personalization. That said, the requirements and benefits are different depending on your individual mandate and areas of concern.

CIAM requirements for the C-Suite

In the earliest days of CIAM, customer identity was likely limited to a tactical point solution by the marketing team through a marketing automation platform. While that was a useful approach, it leaves out the strategic capabilities that can serve all parts of the business. For a modern approach on CIAM, here is an overview of requirements by stakeholder.

Chief Marketing Officer and Chief Digital Officer

The marketing team relies on CIAM to solve several core needs:

- **360 degree view of the user**
  Many services create and store user profile data, but to deliver a consistent experience across all interactions and devices, the profile must travel with the user so that access is easy and context carries forward. A CIAM solution that creates a unified customer profile from disparate sources, whether that’s a data warehouse, marketing automation system, or custom app, is key.

- **Cohesive omni-channel experiences**
  Users should be able to access any experience with the same identity and account.

- **Frictionless registration and login**
  When users encounter friction in the registration experience—too many fields, too many asks for sensitive information, too many security questions—they bail. It's critical to ask for the right information from your customers at the right time, and to use security measures that feel logical within the context of a given experience. Businesses should increase friction at the right time—when data shows a bad actor is attempting to log in, or when a customer is trying to access sensitive personal information—and decrease friction when it's clear someone is who they say they are. The good news is that it's possible to increase security seamlessly with new technology, such as biometric authentication, something that's already become a widespread standard on mobile devices.

- **Privacy and consent management**
  Personalized experiences based on user data win loyalty, but if you misuse that data, consumers will abandon your brand without hesitation. And as regulatory requirements like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) become more widespread, the ability to replicate and automate policies in new geographies is critical. A CIAM solution can help you operationalize and automate compliance so that you can satisfy regulators, as well as safeguard data privacy, so you can create happy customers.

CPO and Product

The product team has the vital but challenging task of iterating on user experience, product capabilities, and driving customer value every day.

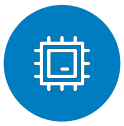
Therefore, product teams depend on a handful of key capabilities:

- **Schedule**
  While a login box looks simple, the complexity of building your own registration processes, password reset flows, and multifactor enrollment adds unnecessary tasks and risk to your project plan. Using Okta and the underlying industry standards of OpenID Connect and OAuth allows your team to focus on making your application useful and valuable.

- **Adoption**
  Once a team ships their application, driving adoption becomes the top priority. Simplifying registration pages through progressive profiling is a good approach, but even before that, we can integrate social login to bootstrap a user's profile in seconds. And for high assurance or sensitive use cases, integrating with identity proofing services and capturing consent addresses security concerns quickly and easily.

- **Revenue**
  As more people find and use your application and your customer base grows, you will be targeted for more and more sophisticated attacks. Preventing fake user registrations and eliminating account takeover gives you better metrics on adoption and mitigates fraud, chargebacks, and billing issues. Stopping these issues at the source is faster and safer than detecting and fixing problems later.

- **Innovation**
  Finally, your team knows today's requirements but can only guess at the requirements, standards, and regulations coming tomorrow. Working with a platform that handles multifactor authentication methods with a few clicks, implements the latest protocols, and builds on a GDPR and CCPA compliant infrastructure simplifies today and tomorrow's efforts.



CISO and Security

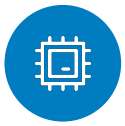
As you get deeper into CIAM, improving the customer experience is crucial, but it must be supported by appropriate security practices and policy. Consumer data is among your most sensitive information and assuring its protection is critical for maintaining brand loyalty, trust, reputation, and legal compliance.

CISOs will require the following core capabilities:

- **Password policy**
  Most of us are tempted to reuse passwords and odds are, your users already have on dozens of sites. When one site or app is breached, that creates vulnerabilities for consumers across all of their accounts. Nudge your users to use better passwords or even no password at all with a comprehensive password policy that puts other, more secure factors first.

- **Adaptive multi-factor authentication (MFA)**
  Threats to password security have never been more prevalent. With the plunging cost of computing, the fluidity of cloud infrastructure, and the growing value of a compromised account, brute force attacks are more feasible and ubiquitous than ever before. You'll want to consider a portfolio of different factor options to suit diverse use cases and apply policies that will allow you to step up based on risk-based policies driven by your customers' context and actions.

- **Secure, audited infrastructure and operations**
  Securing your consumer sign-in and PII requires processes and controls across all layers of the service—from screening the people who operate the service, to screening code before it's committed to the code base, to penetration testing. The fewer places this information is stored or replicated, the easier your compliance becomes.



CTO and Technology

To rationalize and take advantage of a CIAM platform, it must be both generic enough to support unpredictable future needs and specific enough to address today's problems.

It's important that technology stakeholders value:

- **Reliability and scalability**
  As the front door to your applications, you can't risk downtime, scheduled or otherwise, before, during, or after launching your applications. Further, your team must plan for success and your CIAM platform must be prepared to scale for peak periods.

- **Support for standards**
  To speed integration with your current and future applications, your CIAM platform must support common standards such as OAuth2.0, OpenID Connect, SAML, and SCIM out of the box.

- **One service for all identities and all points of access**
  A unified approach to managing every identity that touches your company yields immense leverage. Deployed once, your CIAM solution can then rapidly connect to existing and new applications quickly and easily. Further, you can connect it to the APIs, services, and servers that power those applications, so you have a single point to create, apply, and enforce authentication and authorization policies for every layer of the technology stack. Okta lets you integrate more components faster to save your team's time and effort.

The Okta Identity Cloud: A Modern Approach to CIAM

New initiatives and priorities to address new challenges require a rethinking of the foundation. This foundation needs to address all modern use cases (B2E, B2B, B2C, and IoT) while acknowledging that the boundaries between those use cases are not always clear. This foundation needs to enable the line of business and IT to choose the best applications and technologies to build out digital experiences with the greatest ROI. Delays lead to projects never getting off the ground, missed revenue, failure to meet compliance requirements, and competitors gaining market share. Speed and agility are non-negotiable. With the breadth of IAM capabilities across all scenarios, the IAM system can be the glue that enables the business to transform and deliver end-to-end experiences for all users in all scenarios at all times.

Okta is the modern identity foundation for digital transformation that organizations need to deliver secure digital experiences. Okta was born in the cloud, delivers enterprise-grade security and scalability, and is built for change. Organizations that use Okta go live quickly, stay online through massive growth, are free to be opportunistic in the market, and get the ROI desired from digital initiatives.

Okta provides a wide breadth of capability across applications, the APIs that power them, and the servers and containers that host them — all as one modern cloud service. With this unique capability, Okta is the best foundation for enabling organizations to deliver end-to-end experiences with extreme agility.

Organizations have the choice of using Okta's out-of-the-box end-user experience or using Okta's API, SDKs, and toolkits to deliver a highly branded, completely custom end-user experience.

Cutting across the breadth of Okta's products are four key points of unification in the system:

Frictionless experience
Users should be able to access any experience across devices with the same identity and account to simplify registration and authentication at all times in all places.

Speed to market
The best security isn't useful if your application hasn't shipped. Okta works to speed your development team with packaged, proven components ready for production.

Centralized management
At its foundation, Okta is a user directory that enables organizations to connect all sources of user profiles and data, transform attributes, and manage group membership, all while applying authentication and authorization policies in exactly one place.

Internet-scale security
As you integrate more devices, applications, and systems, the sheer volume of data you collect, how you store it, and how you manage it become liabilities. Okta helps you protect and secure access to PII to reduce your risk of data breaches and compliance issues now and into the future.

Okta is the modern identity foundation for digital transformation that organizations need to deliver secure digital experiences. Okta was born in the cloud, delivers enterprise-grade security and scalability, and is built for change.

For a concrete path to take your Customer Identity and Access Management approach from where you are to where you need to be, check out our free playbook: From Zero to Hero: The Path to CIAM Maturity.

About Okta

Okta is the leading 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 6,000 applications, the Okta Identity Cloud enables simple and secure access from any device. Thousands of customers, including Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks and Adobe trust Okta to 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. For more information, visit us at www.okta.com or follow us on www.okta.com/blog.