The Future of CIAM: 4 Trends Shaping Identity and Access Management

Okta Inc.
100 First Street
San Francisco, CA 94105

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

Balancing usability and security

Life moves fast—but we all know that technology moves even faster. The solutions we used a year ago won't necessarily work today, at least not in their original form. At the same time, customer expectations are more refined than ever before, with many accustomed to the seamless digital experiences from leaders such as Amazon, Apple, and Netflix.

But it's not just how someone engages with a platform that matters. Today's consumers also expect companies to protect their personal information—in a way that doesn't disrupt how they use an application or service. It's no longer enough for businesses to authenticate customers with just a username and password. They have to stay ahead of the curve, employ the latest digital technologies, and create experiences that are as secure as they are enjoyable.

Complex identities need complex solutions

To paint a picture of the complex customer identity needs that businesses should account for, let's take a look at how a retailer might interact with its customers.

- Imagine a company creates an app that allows customers to browse and purchase goods online. It needs to quickly build relationships with unknown users that have never interacted with the brand and allow them to browse for products and request alerts, then prompt them to register.
- At this point, the business will start collecting user consent to gather their personal information and send them marketing emails and partner promotions. It also needs to store that data securely and ensure that all data use complies with relevant privacy regulations.
- When the user is ready to purchase a product, the app should be able to authenticate them and collect any additional necessary profile information, enabling the user to quickly and securely create an account.
- As the user traverses both digital and physical experiences, their journey needs to be personalized and localized via tight integrations with the company's marketing technology stack.
- As the business grows and becomes increasingly complex, it requires an identity platform that can span all of this, grow with it, and adapt to its unique challenges along the way. And, of course, continue to offer a seamless experience to its users.

Having a robust, modern customer identity and access management (CIAM) architecture in place helps businesses do more than deliver seamless experiences to customers. It can also help them succeed in their digital transformation initiatives, and differentiate themselves in their respective industries. With that in mind, here are four trends that are shaping the future of CIAM, and the solutions you need to capitalize on them.

Trend 1: Driving customer engagement

Customer-facing organizations are under constant pressure to innovate and enhance how users interact with their brand. It makes sense, then, that one of the biggest trends shaping the future of CIAM is improved customer engagement and lowered time to value. Ultimately, if you're building a product, you want users to engage with that product—and delivering a superior experience is vital to fostering those relationships. But of course, all brands are built on trust, which can only be gained over time.

One of the best ways to build trust is to ask for user information progressively, and to introduce only minimal friction when absolutely necessary. The user registration process, for example, can create a choke point where businesses lose potential customers. If it occurs too early, the user might be turned off from further exploring your site. And if it occurs too late, you risk missing the opportunity of actively engaging that user. By providing the right prompts and content at the right time—to the right people—businesses can solidify their connections with users.

It's also important to provide a consistent look and feel across all touchpoints, regardless of the number of brands you operate or where they are located, and to speak the user's language.

How Okta can help

There are four things that Okta is doing to help businesses develop seamless, powerful CIAM experiences and get them to market as quickly as possible:

- **Maintain a consistent brand experience:** With Okta, organizations can embed their brand assets into every step of the identity journey, and update branding using developer tools and APIs.
- **Create custom out-of-band factor experiences:** Our Devices SDK allows you to create passwordless experiences for users. Custom biometric, time-based one-time passwords, and push notification methods can be used to authenticate users within an organization's native mobile applications.
- **Speak to customers in their language:** Okta's "Bring Your Own Language" translation platform ensures you can speak to customers in their native tongues and effectively account for regional nuances (e.g., Québécois vs. Parisian French, American vs. Canadian English) or new languages.
- **Build a user's profile over time.** Okta's capabilities in progressive profiling and social account linking can support businesses in obtaining customer data at the precise point in the customer journey that it is needed.

Creating a valuable and enjoyable experience is one of the quickest ways to drive customer engagement—and we all know that highly engaged users are likely to purchase more products, more frequently.

Trend 2: Delivering better security outcomes

Many businesses believe that good security is achieved by deploying multi-factor authentication (MFA) and adaptive policies on their apps. But that approach alone isn't sufficient when customers have the ultimate choice over whether or not they use MFA.

Instead, businesses can drive better outcomes—for themselves and their customers—by empowering users to keep their data secure at a level they are comfortable with, and by adding security controls that do not require direct customer input. Therefore, rather than implementing the highest, most disruptive security options, you should focus on applying the right security at the right time, providing flexible policies, and keeping things simple where possible.

Think back to the example at the beginning of this whitepaper. If that business had chosen to introduce strict security measures during a time when customers were simply browsing for products, it would have likely lost a large percentage of users before they ever transacted. A better approach for the future is to have multiple customer access and authentication policies in place—apps that only allow customers to check the status of an order, for example, require a different level of security than apps that allow customers to register and make a purchase.

How Okta can help

Considering how much—and frequently—security shifts in the customer landscape, we're working on providing businesses with more flexible options for customer identity and access management:

- **Apply the right security at the right time:** Even businesses that have thousands of customer-facing apps can keep things simple by applying the right security at the right time. With Okta, low-friction apps can have different policies than highly sensitive ones; admins can also link multiple apps to the same policy or add new apps to existing policies to ensure specific levels of assurance are enforced.
- **Let customers choose how they secure accounts:** The best experiences are ones that allow users to make their own decisions. That's why Okta is introducing opt-in MFA, which will only prompt users if they have enrolled it for the account in question. We'll also be building campaigns that prompt customers to regularly improve their security hygiene.
- **Prompt users only when necessary:** Making sign-on policies more flexible is crucial to delivering better security outcomes. We're working on enabling businesses to prompt users when it matters most (e.g., when they try to access a sensitive resource, or take a high-risk action such as transferring large sums of money) to create the right balance between security and usability.
- **Make recovery easier:** Recovery experiences have traditionally been limited to a few factors, such as email, security questions, and SMS. To make this easier, Okta is going to enable users that have forgotten a password to use any factor that they have enrolled—which should reduce the burden on help desks and customer support.
- **Extend the identity experience:** To help customers achieve the identity experience that is necessary for their organization, we're integrating with the rest of their security technology stack. Working closely with our partners to create out-of-the-box integrations will allow businesses to apply the right level of friction by confirming user identities with driver's licenses or ingesting fraud signals and bot detection to eliminate additional user input.

These new factors, policies, adoption campaigns, and partner integrations are far more effective than putting MFA alone in front of every app, and will help businesses drive better security outcomes. What's more, this new approach to CIAM makes customer experiences both seamless and secure, further reducing time to value.

Trend 3: Safeguarding user privacy

With the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) in effect—and several other privacy regulations making their way through legislatures—safeguarding privacy and allowing users to control their data has become paramount. Customers now expect businesses to detail what information they collect, clearly ask for permission to store and share data, and delete data if requested.

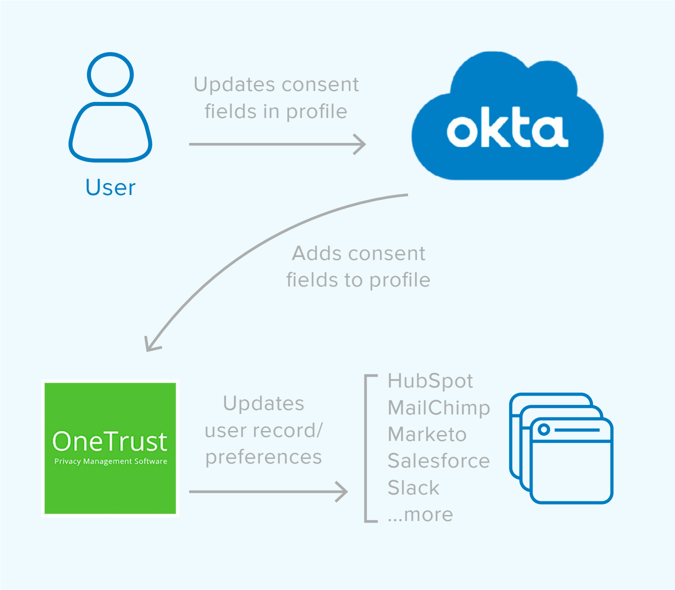
Data privacy concerns have already reshaped advertising and social media, and it's only a matter of time before they impact your organization. To continue building trust—and give users peace of mind—businesses must strike a delicate balance between aggregation, attribute mastering, cookie consent prompts, data mapping, preference management, data download capabilities, and process automation, among other components.

How Okta can help

There are three ways that Okta can help you protect users' privacy:

- Preference management: processing and storage
- Privacy management: data sharing
- Compliance management: data mapping and deletion

In addition to privacy features that capture users' consent to data processing and storage, we're building out-of-the-box capabilities that prompt for custom terms and conditions during registration—and retain consent along with policy and versioning information. Integration partners such as DataGrail and OneTrust play a key role in this process for more complex requirements.


User
Updates consent fields in profile
okta
Adds consent fields to profile
OneTrust
Privacy Management Software
Updates user record/ preferences
HubSpot
MailChimp
Marketo
Salesforce
Slack
...more

In practice, Okta can capture consent upfront when a user registers or logs in and reprompt them when that consent expires. Okta can then propagate the data into downstream systems like Marketo or HubSpot—or directly to a dedicated privacy solution like OneTrust and Datagrail—that will then orchestrate a workflow when a user requests to see what data a business has about them.

Now more than ever before, safeguarding user privacy is crucial to growth and sustainability for any customer-facing business. Okta's new capabilities are geared at simplifying this increasingly complex process, making it easier for companies to adapt as they move forward into a new regulatory landscape.

Trend 4: Managing complexity

Most organizations now deal with a level of complexity that isn't always obvious when looking at the surface of an app. Many have to operate multiple applications and external identity stores spread across various sources such as enterprise IDPs, social login solutions, and niche social providers. CIAM is no longer a case of users logging in to a single application.

Many businesses also have to manage different development environments to ensure a variety of stakeholders can interact with the customer identity system. And as they grow, organizations have to account for several business units, multiple application development teams, and merger and acquisition processes that can impact their identity environment. As a result, IT and development teams are likely overworked as they try to navigate and manage these various complexities.

How Okta can help

Okta brings structure to CIAM with capabilities across inbound federation, org management, and Universal Directory. We're making several investments into providing a single pane of glass that reduces business' identity debt and streamlines customer identity and access management across teams, including:

- **Multi-org management:** Businesses are increasingly managing multiple tenants for their development, staging, and production environments. In addition, multiple orgs are being used to connect separate legacy systems and partners, segregate data, and build B2B SaaS products. We're enhancing our platform to better serve multi-org cases that should have multiple Okta orgs and reduce the need for those that don't. This includes:
    - Extending API coverage to enable automated configuration of orgs
    - Introducing cross-org administration capabilities
    - Automating org management for CI and CD pipelines
    - Segregating data access in a single Okta org
    - Configuring backup export and auto import
- **Organize fragmented identity systems:** Okta customers can already connect to other identity providers through SAML, OpenID Connect, and our built-in social authentication connectors. But the roll-out of Sign In With Apple and other new tools will give organizations more options to control how users from other identity systems are created in Okta with account linking and inbound federation hooks.

These tools will provide much more control when organizations are connecting multiple systems to Okta—but only scratches the surface of reducing complexity. Still, together they can vastly enhance the user experience for customers, which in turn helps to build engagement, enhances trust, and ensures security across the user lifecycle.

A flexible, secure CIAM future

Traditionally, businesses have been faced with an unenviable choice: either build a custom identity solution from scratch which can be time intensive and leave gaps in security, or purchase a pre-defined solution that compromises on user experience.

But now, faced with rising customer expectations and stringent data regulations, businesses need the best of both worlds. They require out-of-the-box solutions that are secure and customizable in order to build journeys that delight customers—and earn their trust.

The capabilities, solutions, and technologies required to capitalize on the four trends outlined above are important in helping organizations to differentiate. However, they must also sit on top of a flexible, scalable, and reliable identity platform that meet the variety of use cases a company will have today and ensure it's future-proofed for tomorrow.

Secure and seamless access

Okta's Identity Engine is a set of customizable building blocks for every access experience, breaking apart pre-defined authentication, authorization, and registration flows. The platform powers secure, seamless access through its new policy architecture, starting with contextual information, such as the user, device, application, network, and location.

Your business can then use this context to create dynamic user journeys with minimal code and deliver solutions for numerous identity use cases. With the Identity Engine, you can drive your users through the access experience, prompting them for credentials, profile attributes, and other remediation before issuing tokens to protected resources.

This unique platform gives businesses a set of tools and infrastructure to provide secure, tailored, low-friction identity experiences. Not only that, but it also powers app-level policies, flexible account recovery, and new integration ecosystems—these are already available in limited EA and will roll-out fully in the near future.

Enhanced developer experiences

A flexible platform is only helpful if a business has the right tools and processes in place to take advantage of it. To assist with this, Okta is continuing to invest in developer experiences that increase your team's efficiency and speed to market, including:

- New and extended SDK support
- Rich developer documentation
- Greater community contributions

As companies across industries move their customer experiences to the cloud, they must ensure they can seamlessly handle large influxes of user logins from major sales, marketing campaigns, and product launches. Okta supports this with DynamicScale, which is being expanded to handle more complex use cases and even higher volumes of authentication of more than one million per minute. Alongside that, we will also be introducing enhanced rate-limiting and visibility, which will be available to customers with and without DynamicScale.

Workflows for CIAM

Identity sits at the center of the modern technology stack, enabling businesses to be agile with development, synchronize marketing, and defend themselves against modern-day attack vectors.

Returning to the earlier example, identity-related activity needs to be propagated throughout an organization's technology stack. For example, when a new user is registered they also need to be added to the company's CRM system, and when they log in that information needs to be synced with other marketing systems to allow for personalized content. Not only that, but consent preferences need to be shared with privacy solutions.

Managing all of this can be difficult for many organizations, especially as different business units typically own different pieces of their technology stack. This is where Okta Workflows comes into play: it automates code-free, identity-specific processes across apps.

When an event takes place, Workflows triggers a function and a series of "if this, then that" functions. For example, in the event a new user registers for a banking application, Okta can ensure the customer is also added to the relevant communications channels with the appropriate welcome message and is assigned a local banker.

This is a powerful, easy-to-use approach to automating tasks that have traditionally been manual. It features a simple drag-and-drop interface that enables organizations to create workflows with zero coding and contains a number of pre-built connectors to the most popular collaboration tools. Businesses are also able to write advanced logic that automatically creates flows based on certain events.

Workflows is important for powering four critical customer identity use cases:

- **Lifecycle management:** As a customer is onboarded, or changes roles or groups within an organization, Okta can share that information with relevant systems and resources. This ensures that all business units are synced on customer updates to guarantee they have the right access and only receive relevant marketing and promotional information.
- **Registration and login customization:** Today, customers can modify registration and login with Okta using Hooks. But we often see the need for more elaborate processes, such as proving a customer's identity with a photo of their driver's license. Workflows will help businesses to seamlessly achieve this by reaching out to an external identity proofing vendor to complete the process.

- **Consent and privacy:** When a user gives consent for their information to be used for marketing purposes, this information needs to be distributed to a number of different locations, not only in Okta but also partner systems. Workflows is a great vehicle for securely sharing this consent and privacy information.
- **Extending Okta without code:** Businesses currently using Hooks that no longer want to write custom code can now build all of that within Okta Workflows.

Building robust and secure customer experiences

As we look ahead to the future of access management, one thing is clear: the days of providing customers with only a simple login page to manage their user experience are over. It's more important than ever for businesses to create seamless omnichannel experiences that not only engage and delight customers, but also meet their privacy expectations and comply with various data regulations. By choosing Okta, you can enable your business to stay ahead of the game.

We're committed to helping customers create experiences that increase engagement, build trust, and encourage loyalty, which in turn can deliver better security outcomes. We want to ensure that you have an identity platform that you can rely on today—and one that is flexible and scalable enough to meet the challenges of the future.

For more information about how Okta's identity platform helps customers delight their users, get in touch.

About Okta

Okta is the leading independent provider of identity for developers and the enterprise. The Okta Identity Cloud securely connects enterprises to their customers, partners, and employees. With deep integrations to over 6,000 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