okta

Transform the Customer Experience with a Modern Customer Identity and Access Management (CIAM) Solution

Okta Inc.
301 Brannan St
San Francisco
CA 94107
info@okta.com
1 888 722 7871

> “The growing range of channels, devices, platforms, and touchpoints is driving the need for CIAM.”

A Swiftly Changing Landscape

Every company today is becoming a technology company as it digitally transforms its customer experiences. With an explosion of devices, rapidly-evolving customer requirements, and higher customer expectations for security and privacy, companies who want to succeed must find ways to ensure their customers can engage with their apps or services at any time, from any device, in a secure and safe manner.

This is where customer identity and access management (CIAM) comes in. CIAM allows for modern, frictionless customer experiences to be built and brought to market quickly while balancing the need for future-proofed identity, security, and scalability. CIAM is foundational technology that meets increasingly complex customer requirements and enables companies to deliver secure, seamless digital experiences.

The growing range of channels, devices, platforms, and touchpoints is driving the need for CIAM. But there’s more to CIAM than just enabling the right individuals to access the right resources at the right times.

Traditionally, CIAM has been for consumer (B2C) use cases. However, the customer of an organization could also be a business (B2B). As customers expect more from the companies they do business with, requirements can span multiple audiences and use cases. For instance, companies building mobile applications for their customers might need to display inventory data traditionally sourced from an ERP system connected to a workforce IAM solution. Or, employees may need to access customer experiences when troubleshooting customer issues. These are only a few examples, with more varied integrations happening between applications and user types everyday.

As a result, vendor-based CIAM solutions are increasingly becoming a must-have for companies. Over 69% of respondents to a Gartner IAM survey are using or are planning to use various IAM technologies for B2C constituencies by end of 2018.* Gartner recommends that businesses “design and manage [their] CIAM system as a strategic platform.”*

Key Trends in CIAM Solution Design

As businesses consider a CIAM solution and build out their design, they should take into account changes in the customer identity space. Here are four key trends to guide organizations as they design a CIAM solution that will meet their current and future needs:

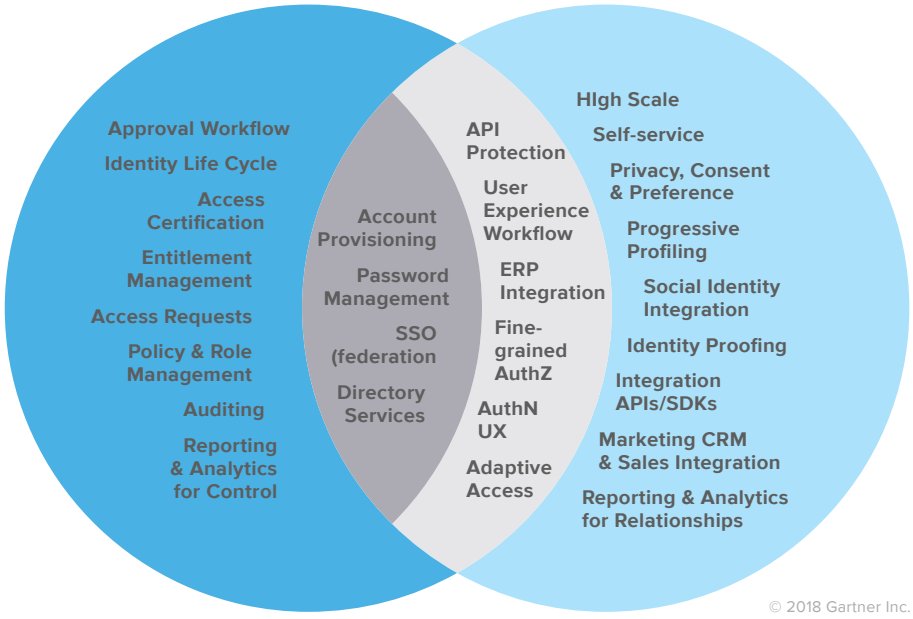
CIAM and IAM features are increasingly overlapping

A CIAM solution may traditionally be targeted toward consumers, but the rise in complexity of the customer experience, the additional audiences that need to be considered, and the overlap in use cases requires more traditional IAM features. Traditional IAM solutions have a deep history in fine-grained access controls and security considerations that are increasingly required to fulfill CIAM use cases. As illustrated by the figure below, the number of IAM capabilities that must be leveraged for both a consumer IAM deployment and a workforce deployment will continue to grow.

The traditional areas of overlap (shown in dark gray and published as part of late 2016 research) include only a handful of core features such as password management and single sign-on (SSO). But the functional overlap between IAM and CIAM is expanding rapidly with the addition of new capabilities (shown in light gray, and added just 1.5 years later).

One feature overlap is API protection—which involves securing APIs from malicious attacks and threats—such as APIs to support mobile apps. Another feature overlap is adaptive access. This allows for contextual access management through intelligent access and authentication policies based on login context, including device, location, and network. Adaptive access can reduce authentication risk without increasing friction for all users of an organization—consumers, employees, partners, and other users. Meanwhile, fine-grained authorization—traditionally associated with employees and business partners accessing sensitive data—now applies to customers receiving access to just the right level of information.

CIAM and IAM Feature Overlap is Increasing



Gartner Figure 3, **CIAM and Workforce IAM Feature Overlap Is Increasing**, *Top 5 Trends in CIAM Solution Design*, 5 March 2018

Source: **Gartner (March 2018)**

According to the report, overlap between CIAM and other IAM deployments continues to grow. Implementations that serve multiple user constituencies are becoming common—for example, both B2C and B2B, or the IoT and B2C, on the same CIAM platform.* Important workforce IAM requirements like identity lifecycle are increasingly required for CIAM use cases to combat malicious attackers. Auditing, reporting, and analytics for control are also important to tie CIAM deployments tightly to an organization's security and DevOps processes. Further, common CIAM requirements around integration SDKs/APIs and self-service are now being used in workforce IAM solutions for modern application development, as well as employees that have acquired consumer experience expectations. This single implementation can offer operational efficiencies, and should also adapt to the ever-changing needs of businesses and their users.

Frictionless, consistent omni-channel experiences facilitated by single sign-on

Customers rely on a large number of devices—and those numbers continue to rise. Customer demand for biometrics as a second factor of authentication, or even passwordless access, is also increasing. Because of this, companies should focus on ways to reduce friction, as unnecessary friction leads to customer churn. Managing customer identities can therefore be a significant challenge, not only because organizations need to support all these channels, but they also need to ensure that the user experience is optimized for each one while still being consistent across all.

To achieve this, Gartner recommends providing "a unified logon (SSO) across all digital properties, if the organization has not already done so." Enabling a single login that can be used to access all of the organization's consumer-facing systems reduces friction for the consumer and provides a single source of authoritative first-party information.*

Improved developer support

In a world where every company is a technology company CIAM systems must provide a platform for continuous change and that CIAM systems are evolving into more flexible developer platforms. Developers play a key role in building out sophisticated customer experiences. They need an agile CIAM solution that enables faster time-to-market to meet rapidly-changing customer needs. Additionally, a CIAM solution should support developers in delivering an identity layer for secure customer experiences. This way, they don't have to reinvent the wheel when it comes to authentication, authorization, and user management, and can instead focus on building the features that differentiate their app.

Among the many components of a CIAM solution, companies should look for more developer-friendly features such as:

- **Well-documented APIs with sample code**
- **Language and framework support (SDKs)**
- **Comprehensive documentation**
- **Customizable UI and workflows**
- **Ability to integrate with API gateways**
- **Support for event-driven processing**

Gartner suggests choosing CIAM offerings that include capabilities that further empower developers as a way to continuously adapt to new customer and business needs.* A CIAM solution needs to be developer-driven and agile enough to accommodate new architecture, protocols, services, and other advancements.

Further emphasis on security and compliance

Security is paramount—customer data can be compromised in an instant. And when this happens, it can have tremendous implications on a company's viability and customers' view of an organization. This highlights the need for next-generation security features and solutions.

According to Gartner, "security architecture must underpin all CIAM initiatives."* Customer access should be protected through adaptive methods of authentication that implement a context-aware approach to verifying a customer's identity. Companies need to consider how to secure customer interactions while still optimizing for usability and a frictionless authentication experience. Adaptive access would take into account dynamic identifiers such as a customer's location, device, IP address, and other vendor-gathered data. For instance, customers using a new device to log in to a sensitive app will be prompted for MFA. On the other hand, customers logging in using a previously registered mobile device can use passwordless authentication, resulting in improved security and better usability.

As the report states: "Many of the most sophisticated consumer-facing initiatives, such as creating a custom mobile app or new browser-based application, involve developing new APIs that are accessed by consumers over the web. These external APIs need to be protected by a combination of security and IAM measures. For any externally consumed API (and many internal ones), an API gateway, often part of a broader API lifecycle management solution, must be included in the API protection infrastructure. For CIAM use cases, the CIAM system is the identity provider that interfaces with the API gateway using OAuth and/or OpenID Connect. Depending on the specific use case, you may also need one or more of the newer extensions to the OAuth standard."*

In addition to security, companies need to plan for compliance as well. Measures to protect customer data are increasingly rigorous, as seen in the global reach of the European Union's General Data Protection Regulation (GDPR); California's new data privacy law; and industry-specific requirements such as MFA for financial applications in New York. A CIAM solution can allow for a smooth customer journey in any jurisdiction by providing an automated approach to common requirements.

"Security is paramount—customer data can be compromised in an instant."

The Okta Identity Cloud: A Modern CIAM Solution

A modern CIAM solution should not only meet today's security and compliance standards, but it should also consider the requirements to build next-generation, frictionless customer experiences. The Okta Identity Cloud does exactly that, delivering the industry's most secure and reliable CIAM solution to keep customer data safe, while also offering a range of sophisticated developer tools for future agility.

Okta is born and built in the cloud; Okta's Identity Cloud solution offers a single, complete, integrated service for every type of user. With capabilities that support overlapping IAM and CIAM use cases, the Okta Identity Cloud provides centralized access control across every experience, and enables increased efficiency for IT teams managing user access and developers building user experiences. It scales to efficiently meet the demands of any organization; and in doing so, it enables millions of users to securely connect to the experiences they need. Companies can choose to use Okta's out-of-the-box functionality or harness Okta's APIs and toolkits to create tailor-made customer experiences.

The Okta Identity Cloud aligns with all key trends in CIAM solution design through a number of products and features, including:

Single Sign-On

Okta's Identity Cloud offers single sign-on capabilities, linking any set of portals and applications with a single set of credentials—or in the case of passwordless, with no credential at all. Users only have to click once to sign in to everything.

Adaptive Multi-Factor Authentication

Okta Adaptive MFA pairs a broad range of second factors and robust policy framework, preventing identity attacks with an added layer of authentication. This feature allows organizations to set policies for prompting MFA based on user profile, application, and authentication context. With support for a range of verification factors such as SMS, Okta Verify with Push, and biometrics, Okta Adaptive MFA flexes to apply the right level of security to users' varying needs.

Universal Directory

Okta's Universal Directory provides a central place for businesses to manage users, apps, devices and APIs. Universal Directory can store an unlimited number of customer attributes, including consent and privacy preferences. Additionally, Universal Directory can sync with any application and directory to provide a 360-degree view of a customer. As a result, organizations can build a repository for user identity information from which to create a consistent, personalized experience across all apps.

API Access Management

More and more custom apps are developed with an API backend. Okta's API Access Management features are designed for modern mobile and web apps with standard-compliant support for OAuth 2.0. These tools save two weeks of developer time per year and protect an unlimited number of API resources behind any API gateway.

APIs and Developer Tools

Okta APIs and developer tools provide programmatic access to the Okta Identity Cloud, enabling developers to add authentication, authorization, and user management into their apps in minutes. Okta has developer toolkits (SDKs) in every major programming environment, supported by a rich set of documentation and quick start wizards to enable developer productivity. Register today for a free Okta developer account to start building.

Security Analytics and Compliance

Okta takes a comprehensive approach to security through its audited, secure infrastructure and processes, which includes personnel, the development lifecycle, and data center strategies and operations. Additionally, Okta enables holistic visibility and response through real-time reporting that can also be integrated into a security analytics solution.

Okta Integration Network

Okta's extensive network of integrations allows developers to get new applications to market sooner, all while keeping customers safe and providing them with a frictionless user experience through integrations such as API gateways and ID proofing.

The Okta Identity Cloud provides a wide breadth of CIAM capabilities. Because of this, Okta is the leading CIAM solution designed to protect customer accounts, engage more users, and drive more revenue for businesses.

DID YOU KNOW?
Okta has been ranked **a leader in Gartner's IdaaS and Access Management Magic Quadrant for the past five years.****

READY TO GET STARTED?
Get in touch

*Gartner, Top 5 Trends in CIAM Solution Design, 5 March 2018

**Gartner, Inc., Magic Quadrant for Access Management, Worldwide, Gregg Kreizman, 18 June 2018.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.