

IN THIS CHAPTER

- » Understanding the fundamentals of CIAM
- » Seeing the difference between IAM and CIAM
- » Identifying the key business functions of CIAM
- » Following the evolution of CIAM
- » Appreciating CIAM as a consumer-facing identity provider
- » Using CIAM with digital transformation
- » Looking at deployment models
- » Justifying why CIAM makes business sense

Chapter 1

Surveying the CIAM Landscape

Consumer Identity and Access Management (CIAM) synthesizes the relationship between the consumer and brand. Consumers require a platform that supports features such as self-registration, a system to support authentication, and a method to collect consent for data usage in enterprise data systems and devices. CIAM enables a personalized and secure interaction for you to safely shop, play online games, or control your home devices.

In this chapter, you discover more about the business drivers, technology, and capabilities used to protect consumers in numerous environments that make CIAM an attractive option for an enterprise organization.

Introducing CIAM

CIAM solutions are mostly Software-as-a-Service (SaaS)-based cloud solutions. The CIAM solution that IT organizations utilize encases a single identity management system specially tailored toward consumer engagements, so reliability needs to be treated as business critical.

Because both Identity and Access Management (IAM) and CIAM support identity engagements, it's important to highlight some major differences. Three differentiators between workforce IAM and CIAM include

- » **Access for one versus many:** IAM solutions are designed to support access for the right person at the right time for the right reasons. You can think about this as giving access to a vault where you need to have the right access code to open it. CIAM solutions have a totally different objective. They want to give access to as many people as possible, but when authenticating, you want to capture users' identities to engage with them in a personal manor. Envision an entrance of an amusement park where many people want to enter. While entering, you get their names and details to ensure you can sell and market to them.
- » **Supporting self-service engagements:** CIAM solutions are mostly in support of marketing campaigns or ecommerce use cases where the customer self-registers for his product or service purchase. In IAM use cases, the individual is usually provisioned by Human Resources (HR) or the IT department based on a trusted relationship the user has with the employee or partner.
- » **Scale and impact:** IAM solutions are supporting companies and their employees to provide access to systems and services. This means IAM supports tens to hundreds of thousands of users. As CIAM is supporting the relationship between consumers and brands, these engagements support hundreds of millions of customers who are buying their latest products or services. CIAM can directly affect revenue and the impact on brand loyalty and image.

Figure 1-1 shows you a typical CIAM outline across various customer-facing websites and apps, potential social identity providers, and back-end systems with controlled access to customer data for personalized engagements.

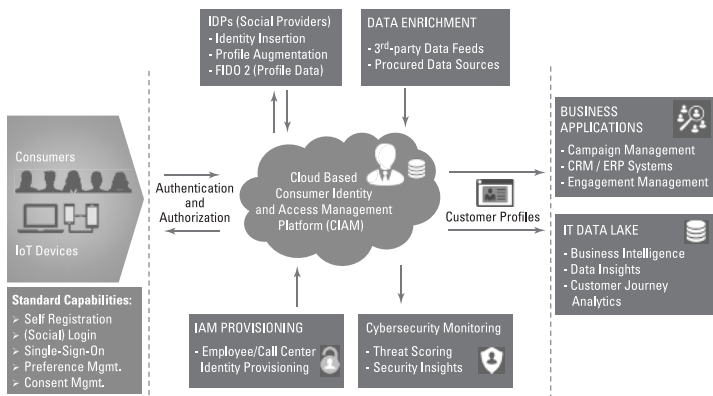


FIGURE 1-1: A typical CIAM implementation.

Because business applications and data stores can utilize the consumer data attributes from a centralized source, the CIAM solution becomes a formidable option to securely engage with consumers and build a trust relationship no matter what communication channel they're utilizing.

Understanding Why CIAM Is Not IAM

CIAM approaches security by using an omnichannel approach. When users sign themselves up for a website, mobile platform, or Internet of Things (IoT) application, they create their own profiles in the context of their personal objectives — like getting a coupon or shopping online. Employees' identities are managed by the corporate entity using traditional IAM tools where HR or the IT department provisions user privileges in the corporate setting.

Authentication is another reason why CIAM isn't like IAM. With CIAM, public standards, such as OpenID, allow social login aggregators to validate end-user identities with already-established identities. The user can also create multiple accounts or personas on a single platform. In the corporate environment, a user has a unique account that maps to an internal service directory. The user is a known, captive entity. Trust can be assumed in the corporate setting, but in the consumer environment, trust isn't assumed and needs to be earned over time.

Performance management is another differentiator between CIAM and IAM. The consumer is less tolerant of lackluster system performance. Because users have alternative choices, their thresholds for poor performance are low. At the corporate level, users deal with system latency, poor user experience, and network degradation as they have no other options to execute on their tasks.

System scalability varies considerably between CIAM and IAM. For consumers, a small system can contain as few as a million users to as many as hundreds of millions of active users. A corporate system leveraging traditional IAM will typically support tens to hundreds of thousands of concurrent users.

IT systems operate on various internal and external networks for different purposes. In the context of CIAM, system identity providers (IDPs) use public connections for decentralization. The same isn't valid for corporate systems because they often leverage a single identity provider.

Unlike IAM, you can't expect a user to utilize complex security mechanisms. For example, with enterprise IAM, employees or corporate users may be expected to use multifactor authentication (MFA). With such a use case, the population is finite. Using such tools is considered acceptable. However, with CIAM, user's sign-up for new security credentials all the time. If a vendor creates a complex user experience, the users will abandon your product.

Finally, customer data collection is process-driven in the context of CIAM. Activities such as transactions, marketing personalization, and business intelligence are inclusive of such collection practices. Additionally, the customer is often subject to a large number of privacy and data protection regulations, depending on their region. Corporations are more concerned about internal administrative and operational actions in addition to globally centered policies.

Looking at the Business Functions of CIAM

Business requirements often drive technology decision making. When certain features are expected to be a part of an enterprise's operations, it becomes a requirement. Business requirements can

be technical, functional, or even policy based. The key business drivers of CIAM focus on

- » **User conversion:** The end-user experience should be fluid across all channels, including web, mobile, and social. There's a fine balance between security and the friction impact of the experience. The developer should be able to build new applications securely by using Application Programmable Interfaces (APIs) that are easy to deploy and that keep great user experiences in mind.
- » **Security:** Applications should utilize single sign on, multi-factor authentication (MFA), or implement self-case and user management with easy-to-consume REST APIs to support common actions, including enrollment, registration, and other identity operations.
- » **Data protection and privacy:** Adherence to data privacy regulations, such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) is essential with a clear and transparent user consent function. Tracking privacy and consent preferences can give users control over their data.
- » **Performance management:** Applying analytics to monitor systems performance whether it's application usage, transaction management, or token usage improves the consumer experience and delivers risk management.
- » **Identity integrations:** Leverage a single platform for login capabilities across all channels by using streamlined authentication connectors, such as OAuth2, OpenID Connect, and Security Assertion Markup Language (SAML) 2.0, to support one application login for ease of use.

The Evolution of CIAM

For several decades, most organizations have made IT investments exclusively on enterprise-centric IAM. Most recently, however, a shift has occurred due to the consumer influence in today's corporate operations and digital transformation efforts.

Starting with the notion of Bring Your Own Identity (BYOID), the concept of (social) login IDP services was born in early 2000. This

birth allowed people to skip registration forms and register with an already established identity. Today, most CIAM vendors support many IDPs to allow for lower friction during registration or login activities. In this decade, more banks, healthcare providers, and governments are expected to embrace the concepts of decentralized identities to provide their services.

While most enterprise IT organizations have some level of centralized IAM services to support customer-facing services for their employees, these services are often attached to existing or legacy enterprise-IAM platforms. To date, this has been the status quo, but customers and lines of business leadership demand more. New services and engagement models are designed with customer identities at the center for the digitalization of business models. As a result, the future need to establishing a service-based CIAM platform is clear.

Supporting Modern Consumer Needs

The consumer is being empowered by more and more global initiatives of governments who are defining data subject rights. This means that next to a great experience, the access and ownership of consumers' data needs to be respected and can't be used without their consent.

How is this changing businesses and the functional requirements? To answer that, you have to look at different angles to understand the real impact of this consumer empowerment:



TIP

- » **Be unique and relevant.** Marketing is the driver to engage the consumer, and IT needs to support the transitions from UX to logins and authentications in a streamlined fashion.
- » **Provide a low friction.** Conversion rates are predicated on the level of friction that the user experiences. Using federated identities, having adaptive authentication methods, and providing clear interactive engagements are essential.
- » **Provide a secure, seamless, and unified customer experience.** This experience should provide an omnichannel experience to protect consumers. Consumers will engage from a web browser, a mobile app, or through a connected tool to respond to brands. The same user login and data access experience can deliver brand loyalty.

- » **Support the consumer.** Support should come across any interface as a means to simplify logins and build trust and brand awareness.
- » **Be highly scalable.** Due to unpredictable success of your campaign, you'll have unpredictable loads. Focus on scaling your system for large public audiences. The user base isn't usually tens to thousands; it's generally millions or more.
- » **Provide self-service.** Allow users to complete the activities on their own. Make it intuitive and user friendly. Strong user experience is essential.
- » **Offer privacy, consent, and preference.** Always ensure the user is aware of who's in control and how her data is being used. Make sure to provide the controls to manage her data.
- » **Allow for modular integrations.** Allow for the integration of social, mobile, API/software development kit (SDK), and enterprise systems using a consistent, repeatable process.
- » **Be reporting- and analytics-centric.** Focus on creating a quality relationship based on personally identifiable information (PII) and metadata outputs.

Supporting Digital Transformation

The consumer has a growing expectation for contextual, personalized experiences. The end-user expects that online experience, regardless of platform, is flawless, predictable, and consistent. To ensure that the consumer experience is delightful, organizations continually transform their operations to meet the needs of the digital economy.



REMEMBER

To meet these demands, both the marketing and technical teams must consider the following factors during the implementation of a CIAM system:

- » **Economic disruptors:** Customers expect that organizations remain innovative and technically adapt to today's customer's needs. There's often a blur between personal and business needs.
- » **IoT:** Almost every solution has become data-rich and includes a digital component, sensor, app, or ancillary app.

- » **Cybersecurity concerns:** Overreach and security concerns given deficient identity and data management practices remain a top concern.
- » **Perception:** Public perception of data collection practices has led to defensive behavior and a stronger desire for consumers to want more control over their data.
- » **Regulatory changes:** Because the consumer is becoming more aware of how his data is collected, used, and accessed, more regulatory controls are being put in place by governments to ensure protection, transparency, privacy, and power.
- » **Demographics:** The consumer is rapidly evolving. Younger users (Generation Y and Z, for example) are more actively using the Internet to conduct transactions almost exclusively for commerce-centric activities. The desire to protect and secure your identity directly ties to the use and adoption of a well-built CIAM platform.

Identifying Deployment Models

Consumer applications, interfaces, and login credentials, no matter how one accesses them, influence the consumer experience. Resources within the enterprise data center support traditional IAM as part of an on-premises hosting environment. When resources shift from a data center to the cloud, this is considered an off-premises solution. CIAM is mostly considered a cloud-based solution due to the unpredictable loads and availability requirements.

Off-premises infrastructure, such as cloud compute capabilities, often reduces the IT internal labor and resources footprint. The design of the infrastructure doesn't fit a cookie-cutter model for all organizations. As described by the National Institute of Standards and Technology (NIST), an organization may use four specific cloud infrastructure deployment models when deploying a CIAM solution:

- » **Private clouds:** Considered the most secure deployment model, this support model is used almost exclusively for single private organizations or internal customer instances.

- » **Public clouds:** Commonly used by independent organizations that share space, this deployment model is popular in the deployment of SaaS applications.
- » **Community clouds:** When there's a common purpose, mission, or audience, this model is often the preferred architecture.
- » **Hybrid cloud:** This model is a combination of two or more of these models in support of an organization's application or data storage needs.

CIAM services can be deployed as centrally hosted, via APIs, or in combination with other access management tools, often across one or more cloud environments. CIAM platforms allow an enterprise organization to deliver a trusted identity with a frictionless user experience that balances security and convenience.

Making Business Sense of CIAM

Consumers expect their online experience to be fluid, whether they're information seeking or committing a transaction. When it comes to entering and maintaining security, the user mandates a seamless experience. Such behavior is especially true for those that are well-versed with online interaction as they prefer self-control and personal engagement.

The modern organization can support security engagements by reducing cyber threats, increasing omnichannel interaction and flexibility, and reducing cost through the use of CIAM. The four key business distinctions that justify why CIAM makes business sense include the following:

- » **Increases loyalty and trust:** Deliver a streamlined, omnichannel experience that protects customer data regardless of format.
- » **Streamlines access:** CIAM allows the customer to access sign-on options and register how she feels comfortable by using balanced security approaches.

- » **Multi-channel personalization:** Deliver anywhere, anytime consistent personalized experiences no matter how the customer interacts with the brand via any device.
- » **Security and privacy:** CIAM protects the customer from fraud, breaches, and cyber threats through enforcement and privacy mandates.

Consumer identity isn't an easy task to tackle. Data needs must be evaluated from both the back and frontend, across various system integration points. CIAM platforms offer an affordable modular approach to handling identity experiences in the enterprise by using secure and low-friction capabilities.