Whitepaper

Why Customer Identity?

Learn how a modern Customer Identity infrastructure can grow revenue, increase efficiency, and strengthen cybersecurity

Table of contents

Introduction

Three business imperatives we hear time and again from the marketplace are the needs to:

- Fuel long-term revenue growth
- Control costs and increase efficiencies
- Boost security and cost-effectively support compliance obligations

When we ask what's harming efforts to achieve these results, a recurring theme is fragmentation.

Customer Identity fights fragmentation

At the foundational level, technology stacks are typically a mix of best-of-breed software-as-a-service (SaaS) applications and broader enterprise suites. In practice, these components are either poorly integrated or not integrated at all, with the result that they barely deliver to the sum of their parts — let alone to their collective potential.

This technology fragmentation frequently causes (or, to a lesser extent, contributes to) Identity fragmentation, with the organization lacking a central, authoritative, and accurate repository of customer identities and related information. This Identity fragmentation is the proximate cause of:

- Strategy fragmentation, which occurs when decisions are based on incomplete information and lack deep customer insights
- Experience fragmentation, which manifests as inconsistent and disjointed touchpoints for customers (especially when multiple channels are in use)
- Security fragmentation, including a lack of visibility and inadequate control, which exposes customers and the organization to risks while also complicating compliance efforts

Customer Identity, also known as Customer Identity and Access Management (CIAM), integrates across an organization's wider technology stack to establish a single, authoritative record of each customer's Identity. By doing so, it enables convenient, private, and secure customer experiences while also contributing to compliance and serving as the foundation of customer-centric analytics.

By directly addressing the fragmentation at the root of so many challenges, CIAM positions organizations to meaningfully pursue the three imperatives listed above.

From B2C origins, Customer Identity is now a driving force in B2B

While the literal definition of CIAM remains consistent, its true meaning — in terms of what use cases it enables, using what functional components, for what types of organizations — has evolved as digital transformation has changed how customers and businesses build relationships and interact.

Traditionally, CIAM was primarily a tool for managing business-to-consumer (B2C) relationships — especially as a way to streamline and personalize experiences, protect against Identity-related cyberattacks, and support compliance with privacy regulations.

However, as companies have undergone digital transformation and embraced SaaS, Customer Identity has shown its utility and value in business-to-business (B2B) scenarios, too.

Okta's Businesses at Work 2024 report revealed that the average company has deployed more than 90 such apps. The figure rises to more than 200 apps for enterprises. For a multitude of reasons, access to each of these apps needs to be carefully controlled.

Going one step deeper, consider that within a single app different users in the same organization need different levels of access to different resources.

For a B2B SaaS provider, administering the multitude of identities within each corporate customer, across the entire customer base, is complex.

CIAM provides the answer — and benefits users, administrators, and independent software vendors (ISVs) — by empowering B2B SaaS customers to self-manage Identity and by providing important features that businesses need (e.g., a range of secure authentication options, enterprise federation, integration with their existing Identity services, user lifecycle management, etc.).

Thus, Customer Identity empowers a B2B SaaS provider to enable highly customized experiences that align with the unique needs of each business customer.

Looking ahead

The bulk of this document answers the question posed in the title, exploring how Customer Identity helps organizations to grow revenue, increase efficiencies, and strengthen cybersecurity (and support compliance).

But before we dive into those benefits, we'll start with a quick overview of Customer Identity's essential components.

Customer Identity's essential components

In Identity terms, four foundational functions of an effective CIAM implementation are:

- **User registration**
  to create the behind-the-scenes record associated with each user
- **Proper authentication**
  to establish with confidence that the users logging into accounts are who they say they are, using one or more factors to do so
- **Effective authorization**
  to provide a user with the appropriate level of access to privileges, resources, applications (etc.)
- **Comprehensive Identity management**
  to enable customers and administrators to make updates and changes to users' data and access

Collectively, these functions allow organizations to implement customer journeys (e.g., signups, logins, account updates, password resets, etc.), to implement basic protections against Identity attacks, and to support compliance objectives.

However, Customer Identity doesn't exist in a silo, and most organizations that deploy CIAM for these basics will soon need to:

- Introduce specialized Identity functions
- Integrate their Identity stack with a range of existing IT and business systems

Satisfying such advanced use cases often requires transacting with other business systems and third parties to exchange information and execute complex conditional flows.

And that's where extensibility comes in, by allowing you to implement specialized and even unforeseen use cases through a design that supports the efficient addition of new capabilities and functionality.

Extensibility enables a whole host of Identity-related functions — here are six of the most common

Identity Proofing

Verify a user's claimed Identity against their actual Identity

CDP & CRM Solutions

Enrich profiles in Customer Data Platforms (CDPs) and Customer Relationship Management (CRM) solutions with valuable Identity data by connecting disparate information sources

Consent Management

Support compliance with data privacy regulations by logging and tracking user consent

SMS & MFA Providers

Enable multi-factor authentication for your applications using popular SMS providers

Web3 & Decentralized Identity

Develop applications using Web3 constructs for decentralized Identity

Log Streaming

Ingest and monitor large amounts of customer Identity data for better insights

To put the possibilities (and potential demands) in perspective, consider that the Auth0 Marketplace includes more than 330 pre-built integrations across 13 different categories!

These wouldn't exist if not for the real-world needs of our customers, and they speak to Customer Identity being both a hub and a spoke for so much of what today's organizations need.

Building such capabilities (or even merely integrations) from scratch is yet another distraction for developers, and results in yet more custom code to maintain in perpetuity.

In contrast, an extensible CIAM capability increases your agility and adaptability, allowing you to implement specialized and even unforeseen use cases — ideally with a range of implementation approaches (e.g., pro code, no/low-code, plug-and-play) to suit your needs and resourcing.

Now that we've introduced the essential components of a modern CIAM capability, let's turn our attention to the business benefits such implementations deliver.

Who 'owns' Customer Identity?
In practice, Customer Identity often straddles organizational boundaries:

- Because CIAM sits at the heart of customer-facing systems — serving as an input into market analysis and influencing acquisition, conversion, and retention efforts — its primary users are in product, marketing, or customer experience (CX) departments
- At the same time, developers and engineers may spearhead Customer Identity initiatives to address essential application and product needs
- Plus, as CIAM has a direct impact on security and privacy, it's squarely in the sights of CISOs, CIOs, and compliance officers
- And — fundamentally — CIAM is a set of technologies, placing it under the purview of IT organizations, or even CTOs (when regarded as an enabler of digital transformation)

Regardless of who 'owns' the Customer Identity implementation, Identity is mission-critical and requires cross-functional collaboration to ensure optimal outcomes.

Benefit #1

Increase revenue

Put simply, a modern CIAM capability allows you to craft the efficient and user-friendly customer journeys so vital to achieving your revenue objectives.

And for B2B organizations, a robust CIAM implementation is typically an unavoidable requirement for landing enterprise customers.

Optimizing customer experiences

Today's companies must enable their customers to engage with their apps or services at any time, from any device, in a secure and safe manner. At the same time, companies must also ensure that these engagements are convenient and consistent across the full range of digital channels.

As a result, organizations are under pressure to continually evolve the user experience (UX) they deliver, to keep pace with the best experiences users encounter elsewhere.

A modern Customer Identity implementation provides the necessary capabilities.

Friction is revenue's natural enemy

In the physical world, friction is the force that resists the relative motion of solid surfaces, fluid layers, and material elements sliding against each other. In the digital world, friction refers to anything that slows down or otherwise impedes a user's interactions with your service — in a Customer Identity context, these interactions may include (but are not limited to) a user:

- Signing up for your service / registering an account with your organization
- Logging in to their existing account
- Providing you with consent to collect and use their data
- Updating their information and preferences
- Completing a transaction
- Resetting their password

While some amount of friction during these interactions is required — to establish trust and provide security controls — unnecessary friction both directly and indirectly applies a downward force on revenue. For example:

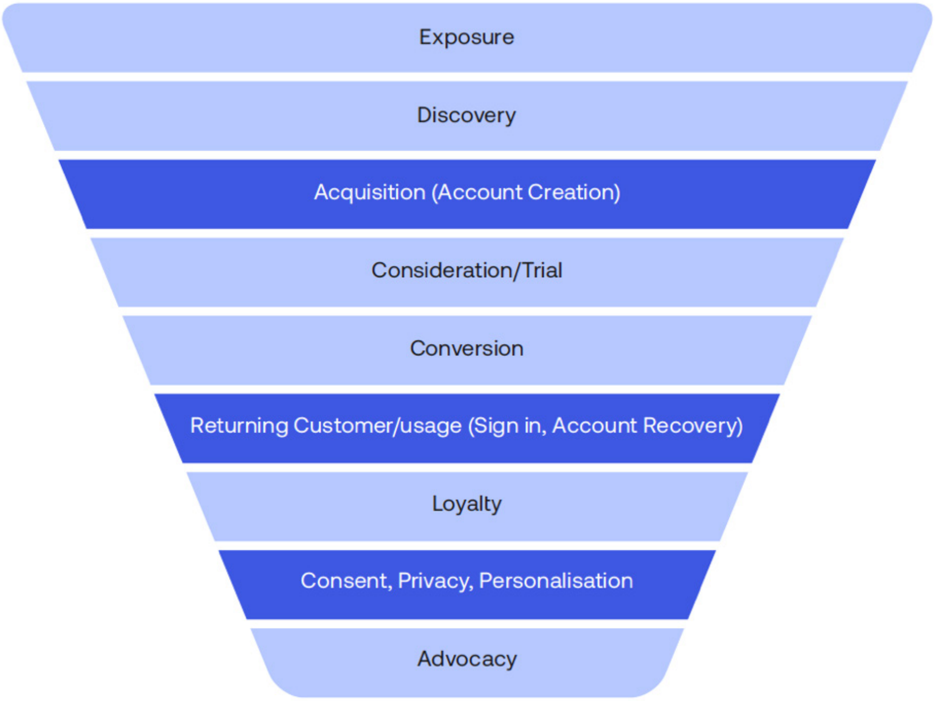
- Okta's Customer Identity Trends Report 2023 revealed that nearly 60% of consumers would be more likely to spend money when services offered "a simple, secure, and frictionless login process" — with the much-coveted younger demographics especially favoring such convenient experiences.
- According to research published in 2024 by UserPilot, 74% of potential enterprise customers will switch to other solutions if the onboarding process is complicated.

Plus, by causing abandonment or by inadvertently driving anonymized interactions (e.g., guest check out), friction undermines your efforts to gather the data needed to build accurate customer profiles — ultimately impairing strategic decisions and negatively impacting acquisition, retention, and overall revenues.

Identity flows are fundamental parts of the customer journey

Fortunately, Customer Identity can help to minimize the friction your customers experience when engaging with your digital channels and/or SaaS applications. That's because Identity flows (shown in dark blue in the example funnel, below) are ubiquitous within the customer journey (e.g., to acquire and authenticate users, to capture consent, and to collect valuable data).

Optimizing these flows — say, by shaving off milliseconds on authentication, pre-filling forms, etc. — can have a direct impact on your overall conversion rates.


Exposure
Discovery
Acquisition (Account Creation)
Consideration/Trial
Conversion
Returning Customer/usage (Sign in, Account Recovery)
Loyalty
Consent, Privacy, Personalisation
Advocacy

Personalization is powered by Identity

An effective CIAM implementation creates a single customer Identity layer that unifies multiple customer entry points, plus front- and back-end systems. In doing so, it enables you to effectively orchestrate the customer journey and make better strategic decisions that drive additional revenue.

By managing omni-channel Identity flows, and Identity orchestration via two-way integrations, CIAM can enable the execution of consistent, highly personalized customer experiences across all of your digital channels. For example:

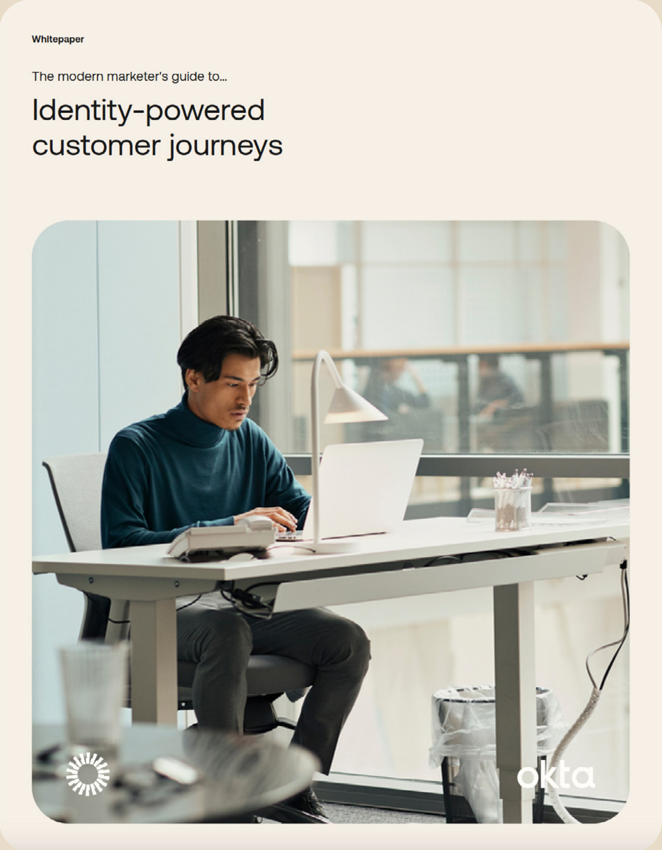
- Through integration with CRM and analytics tools, CIAM contributes to a richer understanding of your customers — including their preferences, behaviors, and where they may be encountering friction when accessing your services — surfacing and informing opportunities for personalized outreach and continuous improvement.
- Integration with marketing automation systems can trigger adding a customer to a campaign based on login frequency or context.

Know your customers, grow your revenue
In the emerging privacy-conscious and user experience-oriented environment, two forms of customer data will become invaluable for marketers:

- Zero-party data (ZPD) that customers willingly share, such as fields on a sign-up form, their shipping details, or an email survey they completed
- First-party data (FPD) that customers generate as they interact with your site or application, including search history, analytics information, session metadata, and more

CIAM is a uniquely valuable element within the larger marketing technology stack — powering both behind-the-scenes capabilities and customer-facing interactions, and enabling the compliant acquisition and activation of ZPD and FPD.

→ Download the guide



Whitepaper

The modern marketer's guide to...

Identity-powered
customer journeys

Enabling up-market growth paths

Going upmarket is a frequent goal for B2B SaaS vendors, but it isn't easy. In addition to ensuring your core features meet the needs of enterprise buyers, you also have to satisfy a long list of additional requirements in other areas — including Identity.

While the needs of comparatively smaller customers may have been met with fairly straightforward authentication, authorization, and Identity management features, enterprise decision-makers impose demands that are very difficult to satisfy without a mature approach to Customer Identity.

As thousands of organizations have already discovered, these range from some fundamental Identity elements like:

- Enterprise single sign-on (SSO), to simplify and better secure their login experience
- Robust authorization and access controls that strengthen their security posture

- Directory synchronization, which allows B2B SaaS vendors to synchronize end users from their customers' organizations with their applications
- Multi-tenancy, widely regarded as a requirement for SaaS vendors
- Delegated administration, to allow B2B vendors to expose functionality to enable self-service admin

...to a long list of extras and surprises that often take scaling companies by surprise, including:

- Availability and scalability
- Development, product, and application security
- Supporting compliance and certifications
- Monitoring and logging
- Choice of cloud infrastructure
- Onboarding and support
- Branding

Plus, because every enterprise is different and Identity is an evolving concept, your ability to adapt to change by extending your Identity engine and integrating it with other systems is another important factor.

Seen through this lens, a modern Customer Identity implementation is a valuable — in fact, necessary — tool in your efforts to land larger customers.

Enterprise-ready Identity
Becoming “enterprise ready” is one of the most talked-about challenges in B2B technology — and with good reason.

Enterprise clients drive significantly larger deal sizes and higher retention rates, both of which positively influence the lifeblood of any SaaS company: annual recurring revenue (ARR).

Plus, a recognizable enterprise logo can also decisively impact future sales simply because it sends a signal to the market that an offering has reached a trusted level of maturity and is now ready for the “big leagues”.

This guide walks through the non-negotiable Customer Identity requirements and ancillary functionality that enterprises demand.

→ Download the guide

auth0

Enterprise-Ready Identity

A guide to the identity features B2B SaaS companies need to move upmarket and win enterprise customers

EBOOK

auth0.com

Benefit #2

Improve efficiency and control costs

A modern Customer Identity implementation makes it easy for developers to implement essential features, with the dual benefits of allowing devs to focus on your core applications and of shortening time-to-market (TTM).

At the same time, CIAM's detailed customer-centric logs and ability to integrate with other business systems can contribute to lower costs of complying with a broad range of regulations, frameworks, and standards.

Freeing developers to focus on core product needs

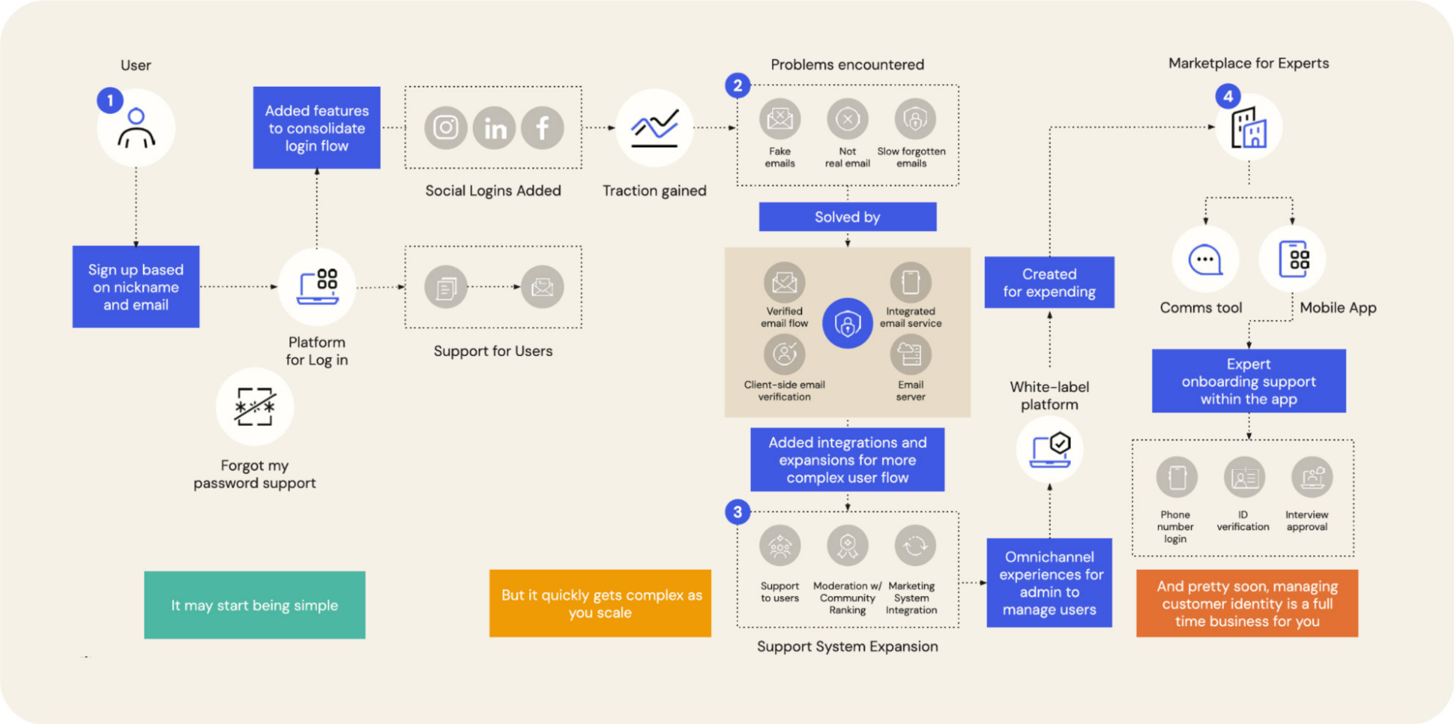
Most B2C and B2B companies don't set out with the intention to build and maintain their own Customer Identity functionality.

Yet it's not uncommon for exactly this situation to occur, usually as the result of incremental — and largely unplanned — work to address business needs as they arise.

While every organization's Customer Identity journey is unique, the diagram below illustrates a representative example:

- **Things start simple enough**, with an identified need to manage user registrations and authentication for a mobile app. Other than availability, performance isn't much of a concern, as there are relatively few users.
- **Very soon, a few extras are needed**, like an automated password recovery mechanism to preserve the support team's time, a web app, and a way to consolidate login flows. To simplify user registrations and to automatically acquire some basic user data, social logins are introduced.
- **As traction improves, new challenges appear**. Fake accounts are consuming resources and adding noise to customer analytics, necessitating the introduction of new safeguards during user registration. Threat actors have also begun brute-forcing the login box to discover and take over existing accounts, creating a need for resilient attack defenses. With each new capability, the team is forced to build something from scratch or acquire and integrate a point solution. And the Identity stack's availability and latency are now points of concern, with real-world customer satisfaction and revenue at stake.

- **Maintaining, managing, and continually extending the Identity stack is now a significant expense with an enormous opportunity cost.** With increasing frequency, other business systems need to be connected to the Identity stack. There are governance concerns about how sensitive user data is acquired, stored, and used. Customers are demanding more convenient ways of authenticating. Enterprise prospects demand federation, performance guarantees, and a host of other requirements.


User
1
Sign up based on nickname and email
Added features to consolidate login flow
Social Logins Added
Traction gained
Platform for Log in
Support for Users
Forgot my password support
Problems encountered
2
Fake emails
Not real email
Slow forgotten emails
Solved by
Verified email flow
Integrated email service
Client-side email verification
Email server
Added integrations and expansions for more complex user flow
3
Support to users
Moderation w/ Community Ranking
Marketing System Integration
Support System Expansion
Created for expending
White-label platform
Omnichannel experiences for admin to manage users
Marketplace for Experts
4
Comms tool
Mobile App
Expert onboarding support within the app
Phone number login
ID verification
Interview approval
It may start being simple
But it quickly gets complex as you scale
And pretty soon, managing customer identity is a full time business for you

One takeaway here is that most B2C and B2B organizations will, at some point, need a larger-than-anticipated set of Customer Identity features. Building, maintaining, extending, and supporting your own Identity stack is a massive undertaking with surprises and new commitments around every turn.

Alternatively, proactively investing in a Customer Identity implementation not only provides you with what you need, today, but also allows you to efficiently introduce new capabilities going forward — without unnecessarily drawing upon engineering and development resources that are supposed to be focusing on core product needs.

Importantly, by treating Customer Identity as you would treat many other important enabling components that are outside your main value proposition, you can accelerate the delivery of projects and features that support your main company objectives.

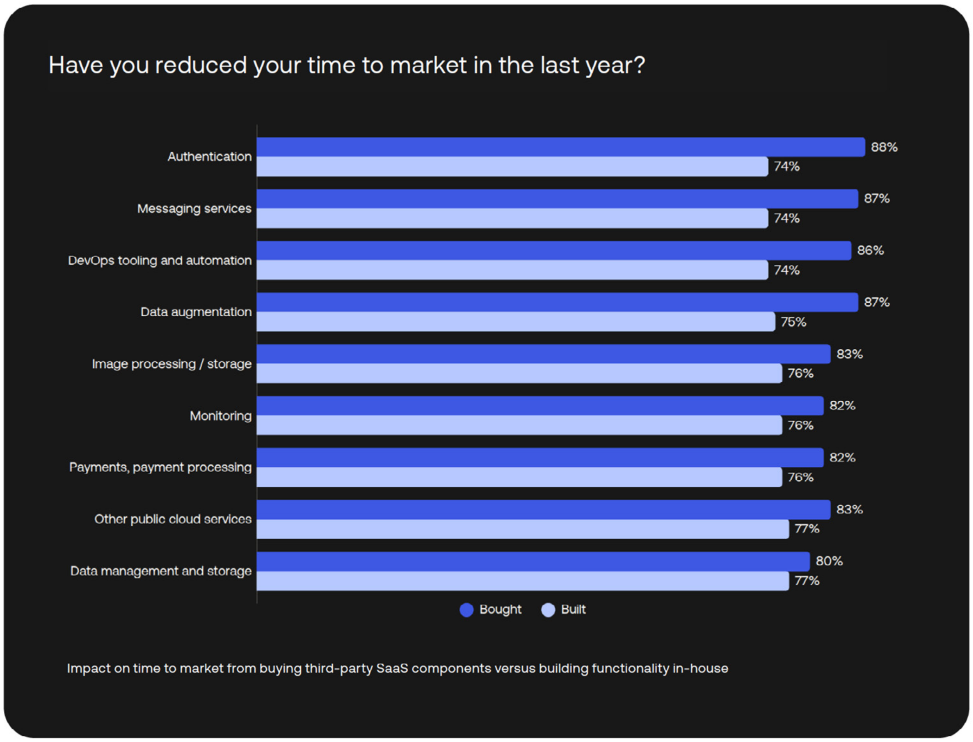
Shortening time-to-market

Published in 2023, Okta's How development teams purchase SaaS shows that purchasing an out-of-the-box Identity solution delivers important business benefits. For example, survey respondents indicated that:

- Authentication functions take the third-most time to build and maintain in house, behind only Data Management and Storage, and DevOps Tooling and Automation.
- 88% of organizations that use a third-party SaaS platform for authentication reported reducing time-to-market — more than was reported for any other component (per the figure, below).

Now, recall that authentication is just one of CIAM's core functions, and consider that building other Customer Identity capabilities in house would be similar undertakings likely involving custom code with ongoing maintenance obligations and little that can be reused.

Alternatively, relying on a Customer Identity solution allows developers to focus the bulk of their efforts elsewhere — further reducing TTM with every avoided in-house implementation effort.



Source: How development teams purchase SaaS (Okta, 2023)

Reducing compliance costs

In the next section, we'll outline Customer Identity's general role in governance, risk management, and compliance (GRC) — but for now we'll introduce the subject by noting that:

1. B2B and B2C organizations have to comply with a number of regulations around how customer data is managed

2. Customer Identity helps to lessen the costs associated with these activities

When customer data is collected and stored in a siloed fashion across customer-facing channels (e.g., e-commerce, customer support, web app, mobile app, etc.) and internal systems/databases, achieving and maintaining compliance becomes an enormous — and costly — challenge.

And, as the dependence upon such data grows, so too does the importance of Customer Identity — both as an enabler of compliant collection and as a means of putting the data to use.

Benefit #3

Strengthen security and support compliance

(without impeding growth)

In today’s threat environment, Identity is security — and this equality is as true in a Customer Identity context as it is for Workforce Identity.

Accordingly, a robust CIAM implementation creates strong safeguards — before, at, and after login — that protect your organization and your customers, while also supporting compliance with regulations, frameworks, and standards.

However, care must be taken to ensure such safeguards don’t introduce unnecessary or overly burdensome friction for users, lest security pursuits come into conflict with revenue and growth objectives.

Identity security is a top-of-mind enterprise issue

As Identity has become the main enterprise security entry point for workforce and consumer apps, there's industry-wide recognition of the need to advance Identity security with open and interoperable standards that enable consistent security outcomes across any SaaS application — regardless of the provider.
Rather than placing a burden upon developers, such standardization would actually make it easier to build secure enterprise apps.

Just as important, a standardized approach would make it easier for enterprise administrators to manage and secure the many apps their organization deploys — in much the same way that standards have simplified adoption of SSO, MFA, and other security-enhancing features.

Plus, such standardization efforts not only strengthen security, but also drive consistency across SaaS applications, simplifying compliance and reducing integration challenges. By adopting applicable standards, rather than reinventing things, app developers can focus more effort on driving unique differentiation.

Ultimately, as the industry moves forward, there's a shared responsibility among Identity providers, independent software vendors, and customers to collaborate in creating and adopting these open, interoperable standards. This unified approach will ultimately lead to a more secure ecosystem for all parties involved in the B2B landscape

→ Learn more about Okta’s mission to standardize Identity Security

Protecting your customers and your organization

Okta's The State of Secure Identity Report 2023 demonstrates that signup fraud, credential stuffing, and MFA bypass are all everyday threats that must be managed by practically every organization with an Internet-facing login box or API. Per the report, from January 1, 2023 through June 30, 2023:

13.9%

of attempted account registrations met the criteria of a signup attack, in which malicious users create fraudulent accounts

24.3%

of login attempts overall met the criteria of credential stuffing, in which attackers pursue account takeovers (ATOs) by trying compromised credentials

12.7%

of MFA attempts appeared to be malicious attempts to bypass the MFA defensive layer (Okta, 2023)

These attacks have major consequences for the organizations being targeted, who incur costs to investigate and remediate abuse and who face severe regulatory penalties and reputational damage should a data breach occur.

As cybercriminals direct more effort and expertise into getting past the login box — including by leveraging the same generative AI capabilities that are transforming society and business — protecting it requires ever-more layers of ever-more sophisticated defenses.

A robust Customer Identity capability helps to harden your defenses against these risks, with:

- Host, platform, and application-layer defenses to detect and respond to malicious entities such as bad bots before they can even access the login box or API

- Login-layer defenses that prevent fraudulent signups and account takeovers
- Post-login defenses to secure sessions and authorization controls to manage access (e.g., viewing sensitive information, conducting transactions, updating account info, changing security settings) after a user has authenticated
- Observability tools that allow you to identify potential attacks, quickly respond to them in real time, share information with security operations tools (e.g., SIEM, SOAR, XDR), and optimize your security posture
- Strong encryption, modern hashing algorithms, API security, robust data management and system access procedures — and much more behind-the-scenes infrastructure

Notably, these are specialized capabilities that generally aren't part of your wider security stack.

Fake signups are more than a nuisance

Fraudulent registration predominantly targets organizations that operate in a B2C context, particularly those in which a user can create an account for free and without any precondition (e.g., a proof of purchase).

Especially when performed at scale, fake signups can create significant problems and lead to unnecessary expenses.

First, fake users may negatively impact the experience of legitimate users (e.g., by scooping up in-demand products), leading to customer dissatisfaction and reputational damage for the business; plus, they consume resources and may abuse their access to directly attack or harm the organization.

Second, because one of the major objectives for B2C organizations is to turn prospects into first-time customers, entire conversion flows are often optimized based upon analytics data that shows how users interact with the service. Fraudulent registrations pollute this data, significantly complicating business analytics activities and potentially leading to expensive clean-up projects.

Unfortunately, because B2C organizations in particular are so dependent upon maximizing conversion rates, there's an incentive to minimize friction during the registration process — but reducing friction for legitimate users also lowers the barriers for abusers.

The appropriate balance between security and convenience will differ from one organization to another, but a modern CIAM solution should equip you with at least a few different 'levers' to help find what works for you.

Securing Identity while minimizing friction

An idealized Identity implementation provides infinite friction for attackers and something near zero for genuine users (because a little bit of friction in the right place at the right time can help to build trust).

While such a solution is a worthy objective, the real world frequently involves tradeoffs. For example, deploying a mechanism to detect and impede large-scale, scripted bot attacks will increase an application's overall resilience — but may achieve this result at the expense of some human users experiencing added friction in the form of a security challenge.

Once deployed, operational insights can be used to fine-tune the mechanism and strike the appropriate balance between security and convenience. Practically, this balance will vary from application to application, organization to organization, and industry to industry, because each combination of customer base, threat landscape, and security preferences is unique.

To complicate matters further, the balance may shift over time, as threat actors adjust their Tactics, Techniques, and Procedures (TTPs) and select new targets, and as customer desires shift.

But organizations that put in the effort and find a balance stand to reap significant rewards: as noted earlier, Okta's Customer Identity Trends Report 2023 revealed that nearly 60% of consumers would be more likely to spend money when services offered a simple, secure, and frictionless login process (Okta, 2023).

Up until a few years ago, an argument could be reasonably made that it was impossible (or at least impractical) to simultaneously satisfy the need for secure authentication with the imperative of a convenient user experience. However, that tradeoff is increasingly a relic of the past:

- **Adaptive MFA** is a flexible, extensible MFA policy that can help prevent ATOs without increasing friction for real users. It does so by assessing potential risk during every login transaction, and then prompting the user for additional verification only when necessary.

- **New MFA methods are secure and convenient**. MFA methods based on WebAuthn-enabled device biometrics (e.g., Apple Face ID, Apple Touch ID, Windows Hello) or WebAuthn-enabled security keys (e.g., YubiKey, Feitian, Titan) simultaneously deliver high security (threat actors hate WebAuthn) and high usability, bringing authentication ever closer to the ideal.

While it remains unlikely that consumers at large will adopt dedicated security keys, biometric capabilities are becoming much more common within affordable devices. And, in a welcome twist, users often regard biometric authentication more as a convenience feature (i.e., “one-touch authentication”) rather than as a security feature!

Passkeys: phishing-resistant authentication meets convenience

While some legacy authentication techniques force significant trade-offs between the customer experience and security — think long, complex passwords and cumbersome MFA flows — passkeys demonstrate that it’s possible to deliver a CX that’s both user friendly and phishing resistant.

For example, passkeys are:

- **Intuitive**, creating an experience that is as familiar to end-users as unlocking their mobile device
- **Secure**, with public-key cryptography-based phishing resistance built in
- **Non-reusable**, because they are unique per online service
- **Convenient**, allowing users to access an application on multiple devices using a variety of methods including biometrics and security keys

Regardless of their personal motivation, once a user has opted to use passkeys for one application, they will quickly expect all their other apps to support this new authentication mechanism — your Customer Identity stack should make enabling passkeys as simple as toggling a setting.

→ Find out more at learnpasskeys.io

Supporting compliance objectives

Because of Identity's essential role in securely connecting users to the technology and resources they need, and its proximity to sensitive data, Identity as a domain is governed by an increasing — and increasingly complex — array of data privacy (e.g., HIPAA in healthcare, GLBA in finance, GDPR in the EU, LGPD in Brazil, CCPA/CRPA in California, etc.) and open data sharing regulations and standards (e.g., PSD2, UK Open Banking, the Dodd-Frank Act Section 1033, FDX).

Among other things, these regulations typically require you to:

- **Implement effective safeguards** to protect credentials, Personally Identifiable Information (PII), Protected Health Information (PHI), and other personal and sensitive data highly valued by cybercriminals
- **Put users in control of their own data** — how it's used, by whom, for what — through mechanisms that allow them to share data across digital touchpoints, to provide consent for use, and to take their data with them if they choose to end a relationship with a service provider
- **Interoperate** within the open data economy — an emerging web of industry (e.g., healthcare, finance) and Identity (e.g., social login) ecosystems that will enable vast new consumer value and efficiencies while also preserving data privacy and security.

Additionally, Identity requirements are frequently included within a wide range of related regulations, frameworks, and standards. For example:

- Because most of the data making up corporate financial statements is created by information technology systems, carefully controlling access to these systems via IAM and related controls is vital to **Sarbanes-Oxley** compliance.
- With threat actors increasingly targeting Identity to gain initial access and to execute intrusions, robust Identity-related controls are an essential component of cybersecurity frameworks including **SOC 2 (Service Organization Control 2).**

- The **Payment Card Industry Data Security Standard (PCI DSS, or simply PCI)** explains industry best practices, including certain requirements about limiting — to the absolute minimum — the number of employees who can access payment card data.

Through a combination of attributes and capabilities — including centralized management, built-in interoperability, user-friendly Identity management features, cutting-edge security measures, and appropriate data management and residency practices — Customer Identity can lessen the compliance burden, dramatically reducing the costs associated with meeting the many needs of regulations, frameworks, and standards.

Summing up

To meet revenue objectives and stay relevant in the digital-first world, organizations in virtually all industries and of all sizes need to enable consistent and convenient omnichannel experiences for their customers, partners, suppliers, constituents, and other external users.

They also need to make the most effective use of scarce developer resources, by applying talent to projects that move the business forward, rather than on maintaining the status quo or working on ancillary components.

And these same organizations must comply with strict regulations governing data privacy, customer control, and interoperability — a task made all the more challenging when a company operates in multiple jurisdictions.

Existing at the intersection of CX, security, privacy, and analytics — and providing essential tools needed to manage Customer Identity through the entire lifecycle — CIAM provides an answer.

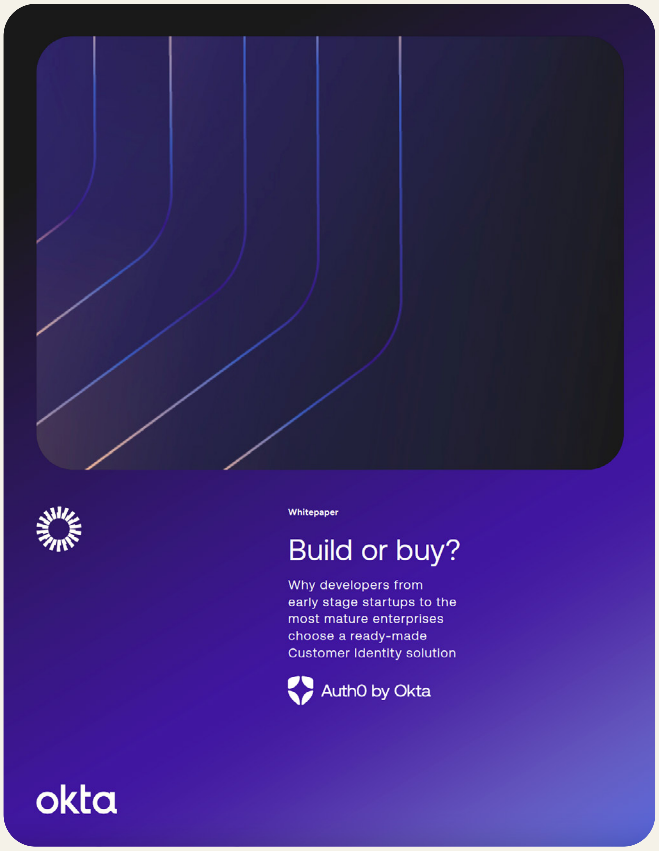
To build or to buy?

Once an organization recognizes the need for Customer Identity, the first major decision that follows is usually whether to build or to buy.

We firmly believe that, outside of the most basic scenario (e.g., a simple, internal proof of concept), integrating a third-party CIAM solution into your app or service makes the most sense — for many reasons (including cost!).

For 'macro' evidence, we need look no further than analyst assessments. For instance, KuppingerCole projects CIAM market volume to reach $4.55 billion USD in 2025, on the strength of a compound annual growth rate (CAGR) of 13.1%.

→ Download our Build or Buy? guide to learn why so many developers and decision-makers — in B2B and B2C — have concluded that buying a CIAM solution is the way to go



Whitepaper

Build or buy?

Why developers from early stage startups to the most mature enterprises choose a ready-made Customer Identity solution

Auth0 by Okta

okta

These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements.