Whitepaper

Why Customer Identity?

Learn how a renewed focus on customer identity can unlock innovation and inspire new capabilities

Contents

Introduction

Digital engagement shapes the way users and consumers interact with their services, starting with customer identity. The experience is much more than just a way to log in to and gain access to services. In the first few months of 2020, digital channels went from a “nice to have” to a “must have” for countless businesses; for many, digital channels suddenly became the only way to engage with customers.

In the rush to implement digital transformation strategies, push innovation at the speed of digital-first business, and meet changing consumer demands, new challenges and consequences emerged:

61%

of data breaches involve credentials

88%

of customers say that the experience a company provides is just as important as the product

40%

Number of regulatory fines for privacy increased from 2020 to 2021

61% of data breaches involve credentials, highlighting both the need to safeguard sensitive data and to detect when compromised credentials are being used by attackers.

88% of customers say that the experience a company provides is just as important as the product, and providers who fail to offer convenience, security, and privacy are losing out to those who are.

Regulatory fines for privacy violations increased 40% from 2020 to 2021, and are projected to continue increasing, forcing companies to face up to the necessity of protecting privacy.

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. However, they must do so without drawing heavily on developer resources that are needed to extend core competencies. Plus, they must satisfy both of these goals without overlooking regulatory requirements or compromising on security.

A modern customer identity and access management (CIAM) solution empowers organizations to address—efficiently and effectively—all of these pressures and more.

Existing at the intersection of security, customer experience, and analytics, CIAM is a set of solutions built to help organizations balance convenience, privacy, and security for every type of user who needs access to their applications and services. 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. The result: CIAM in action is not static. When we ask, "Why customer identity?", identity becomes a more powerful aspect—and critical component—of the complete consumer experience and contributor to growth and efficiency.

Customer Identity's essential building blocks

An effective CIAM solution is built on three essential features: **authentication, authorization, and identity management:**

- Proper **authentication** ensures that the users logging into their accounts are who they say they are, preventing bad actors from accessing sensitive user data (e.g., payment details, address, social security number, demographic information, etc.)
- Effective **authorization** helps businesses confirm that a user has the right level of access to an application and/or resources—ensuring each user has access to what they need, when they need it.
- Comprehensive **identity management** allows administrators to update user access permissions and implement security policies, better enabling seamless and secure experiences; this feature also enables customers to manage—to the extent permitted by the use case and required by regulations—their own identities, data, and preferences.

These identity elements, though, are insufficient at capturating the full story of what you can do with them.

Whether you're looking at the top or bottom of the income statement, CIAM offers a range of business benefits.

Business Benefits

Catalyze growth by optimizing customer experiences

Increasingly, digital experience is how customers measure your brand. If this statement didn't completely apply to your business before 2020, it probably does today. In fact, Gartner® projects that, "By 2024, more than 90% of B2C organizations will compete on the basis of customer UX. The digital experience will become the differentiation.[1]"

When each application or digital channel functions as its own identity silo, customer data becomes fragmented and untrustworthy, making this desired user experience elusive and expensive to implement.

But when customer data, preferences, and behaviors are understood, the results can be transformative—and that's the impact CIAM can make:

1. By centralizing customer data into a single source of truth, CIAM enables you to make better macro-level strategic decisions.
2. By integrating with CRM and analytics tools, CIAM contributes to a richer understanding of who your customers are.
3. By managing omnichannel identity flows, CIAM allows you to optimize microlevel execution through consistent, personalized customer experiences across all your digital channels.

The result is more efficient customer lifecycle management that improves acquisition, conversion, and retention rates—driving top-line revenue with convenient experiences.

---

[1] Teixeira, Henrique; Kelley, Michael; Khan, Akif; and Phillips, Tricia. "Innovation Insight for Customer Identity and Access Management." 09 December 2021 GARTNER

Customer Identity addresses multiple business needs

Because CIAM sits at the heart of customer-facing systems serving as an input into market analysis and influencing acquisition, conversion, and retention efforts—it aligns with marketing and customer experience departments.

At the same time, CIAM has a direct impact on security and privacy, putting it squarely in the sights of CISOs, CIOs, and compliance officers.

And—fundamentally—CIAM is a set of technology solutions, causing it to fall under IT organizations, or even CTOs (when regarded as an enabler of digital transformation).

To find the right balance between quality of customer experience and system security, in the context of desired use cases, customer types, data types, andindustry-specific risks, leaders across these functions should work together to implement CIAM.

Shorten time to market by increasing developer efficiency

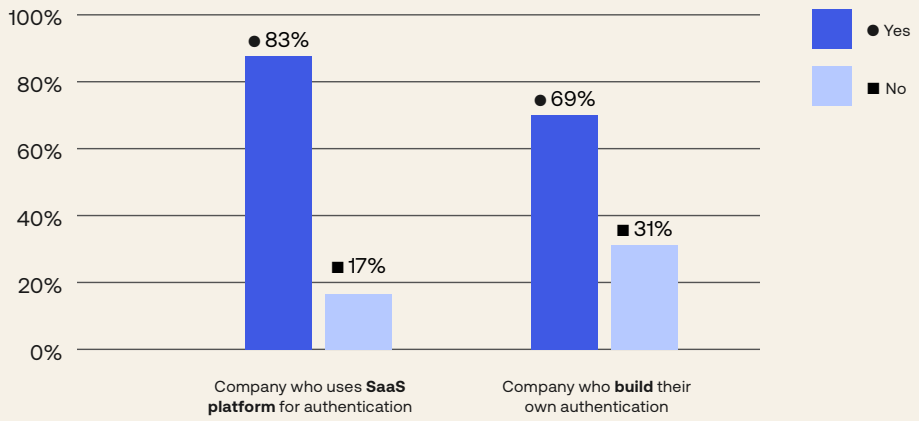
Identity is difficult—even seasoned professionals find building identity solutions complex and time-consuming. As a result, organizations often struggle to scale their identity features and bring them to market at a competitive pace.

Once built, identity capabilities need to be maintained and extended—introducing additional workload for developers that could be needed elsewhere.

CIAM allows businesses to focus on innovation and advancing revenue-generating applications and services rather than on building and maintaining an in-house identity solution.

By ‘solving’ identity, CIAM solutions allow organizations to free up their developers and engineers to focus on high-value tasks that drive the business forward. Our survey of more than 350 application development teams found that the use of third party components correlated with faster release cadence. More than half of those with a monthly or faster release cadence incorporated third-party components into more than 50% of their applications; those with less frequent releases were far less likely to leverage such ready-built components.

Have you reduced your time to market in the last year? Responses from 2020:[2]



[2]: **"How Development Teams Purchase SaaS"**, 2020

Unleashing development talent

In Developer Velocity: How software excellence fuels business performance, McKinsey argues that "empowering developers, creating the right environment for them to innovate, and removing points of friction," is directly correlated to revenue growth, customer satisfaction, brand perception, and talent management.

Finding the right CIAM solution—rather than taking developers away from core business—and including them in the selection process can go a long way toward recruiting, retaining, and getting the most out of the top talent you need to drive innovation and thrive as a digital business.

Reduce compliance costs by effectively managing customer data

Identity as a domain is governed by an increasing complex array of data regulations (e.g., 21st Century Cures Act in healthcare, Open Banking in finance, GDPR in the EU, LGPD in Brazil, CCPA/CRPA in California, etc.) that cover:

- Implementing safeguards to protect credentials, IP addresses, personally identifiable information (PII), protected health information (PHI) and other sensitive data highly valued by cybercriminals

- Putting users in control of their own data—how it's used, by whom, for what— through mechanisms that allow them to provide and revoke consent across digital touchpoints and to take their data with them if they choose to end a relationship with a service provider
- Ensuring the participants within industry (e.g., healthcare, finance) and identity ecosystems can communicate with each other, enabling vast webs of commerce and cooperation while enhancing privacy and security

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 challenge. That's because doing so requires both a comprehensive understanding of detailed legal language and the skills to implement compliant data management processes.

Through a combination of attributes and capabilities—including centralized management, built-in interoperability, user-friendly identity management features, and cutting-edge security measures—CIAM solutions lift this burden, dramatically reducing the costs associated with regulatory compliance (and the consequences of a failure to comply).

Identity is in the crosshairs

Securing identity has taken on even more importance in recent years because as security perimeters dissolve, attackers are focusing efforts on gaining access to accounts (and their rights, privileges, and information) for direct use or resale.

This focus has major consequences for the businesses being targeted, who incur costs to investigate and remediate abuse and who face severe regulatory penalties and reputational damage should a data breach occur.

CIAM solutions with an agile, secure-by-design, defense-in-depth approach can stop attacks entirely or dissuade threat actors by disrupting their business models. Because of the domain expertise behind their development, these best-of-breed solutions are far better equipped to do so than identity stacks built in-house by non-experts.

Learn more about identity threats in our 2021 State of Secure Identity Report

Customer Identity in Action

Traditionally, CIAM was primarily a tool for managing business-to-consumer (B2C) relationships. However, as companies have undergone digital transformation and lines between users have blurred, CIAM has shown its utility and value for other types of customers.

Serving consumers

In a consumer context, "friction" refers to anything that slows down a person's interactions with your service. These interactions may include (but are not limited to) a user:

- Signing up for your service
- Logging in to their existing account
- Updating their information and preferences
- Recovering lost account data
- Checking out (I.E., completing a purchase)

For consumer businesses, friction is an obstacle to conversions and, by extension, to revenue. The more friction there is, the lower your conversion rates and the less revenue over both the short and long term. For example, 17% of US online shoppers have abandoned an order solely due to a "too long / complicated checkout process".

An effective CIAM implementation enables you to offer highly personalized promotions and recommendations that drive additional revenue and create more value for your customers, while at the same time acting as a way to minimize the friction your customers experience when engaging with your digital channels.

Lush leverages customer identity to deliver seamless customer experiences

Lush is a giant in the world of cosmetics, the result of an "ethics-over-profit" approach that applies to all areas of the business and resonates with the digital consumer generation.

Customer identity has been a core enabler of Lush's consumer-oriented initiatives, powering a range of features including single sign-on (SSO) and guest checkout, as well as the centralization of the point-of-sale (POS) system for the entire business—all with a limited developer team and while ensuring the pace of transformation doesn't compromise customer privacy or system security.

Learn more about how Lush is using CIAM to drive growth.

Empowering business customers

Countless organizations rely on business-to-business (B2B) SaaS applications as essential enablers. However, different users within each organization need different levels of access to different resources, and creating a convenient and secure experience requires precise management of identity and access privileges.

For a B2B SaaS provider, administering this multitude of identities within each customer, across the customer base, is complex. CIAM provides the answer—and benefits both parties—by empowering B2B SaaS customers to self-manage identity.

For example, CIAM allows administrators within each customer to:

- Provide a simple login experience to their user base
- Build out key identity features like multifactor authentication (MFA), Security Assertion Markup Language (SAML) support, and OAuth
- Evolve their third-party ecosystem and address security and privacy needs among its customer base
- Manage access privileges through seamless integration with their existing identity services (e.g., Azure Active Directory)

Through this, the B2B SaaS provider enables each customer to create a highly customized experience that aligns with their unique needs without directing excessive resources to its creation, maintenance, and extension.

Atlassian empowers businesses to self-manage their identities

Atlassian is a leading provider of collaboration and productivity software that helps businesses—including Walmart Labs, Merrill Lynch, Bank of America, and Verizon—to organize, discuss, and complete shared work.

Atlassian relies on CIAM to enable customers to easily and securely self-manage their identities across a wide range of products (e.g., Jira, Confluence, Trello, Opsgenie, and more).

Learn more about how their CIAM solution enables Atlassian to focus on product innovation

Enabling constituents, partners, and other known third parties

In consumer and SaaS applications, customers manage their own identities, but there are many scenarios where identity must be managed by the organization providing the service. For example:

- A healthcare provider needs to create a patient's account before that patient can book an appointment or access their health records.
- An education provider needs to define a new student within their identity system before that student can use the course sign-up portal.
- A company needs to provision vendors, suppliers, and partners before those third parties can access protected resources.

To fulfill these use cases—where customer identities are known to, and provisioned by, the service provider, CIAM provides all the tools organizations need to manage customer account creation, maintenance, and end of life. At the same time, CIAM ensures seamless and convenient experiences for those customers.

TCSG simplifies student experiences and protects their privacy

With 22 colleges, 88 campuses, and ~150,000 students annually, the Technical College System of Georgia (TCSG) oversees the state's technical colleges, adult literacy programs, and a host of economic and workforce development programs.

TCSG used CIAM to implement shareable, universal identities that connect to individuals like a fingerprint, staying with them throughout their educational and professional careers. In addition to improving the student experience, centralizing identity management eliminated the need for workarounds and strengthened the protections safeguarding students' personal data.

Learn more about how TCSG uses CIAM to continually extend a student-obsessed solution

Summing Up

To 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 also need to comply with strict regulations governing data privacy, customer control, and interoperability—a task made all the more challenging when identity data is involved or when a company operates in multiple jurisdictions.

Existing at the intersection of customer experience, analytics, and security, and providing the essential tools needed to manage customer identity through the entire lifecycle, CIAM provides the answer.

What to look for in a customer identity solution

With so many solutions available today, shopping for a CIAM solution can seem overwhelming. Here are a few things to look for as you make your short list:

- **Independent and neutral:** Your CIAM solution should enable you, not restrict you. It should integrate with your existing solutions, leverage open standards to avoid vendor lock-in, and work with your preferred cloud provider.
- **Comprehensive and customizable:** Every customer is unique with complex needs. Thus, your CIAM solution should help you build seamless, consistent, and trustworthy experiences for every type of user
- **Easy to build with, maintain, and use:** For virtually every piece of technology, engineering teams aim to reduce effort and time that it takes to deploy, configure, and operate it—and your CIAM solution should support this mission.
- **Trusted:** Having a serious security breach, failing to meet compliance requirements, or experiencing an unavailable or degraded service can result in significant brand, legal, and financial consequences. Your CIAM solution should relieve these worries.

The Okta Customer Identity Cloud: A Modern Approach to Customer Identity

Okta is the modern identity foundation for organizations that need to deliver secure digital experiences.

With Okta your product development, security and IT resources can focus on building the best possible digital services for your customers while we take care of identity. With a full suite of packaged, production-ready identity management solutions, and more than 7,000 pre-built integrations to applications and infrastructure providers, Okta's solutions allow your teams to launch quickly, secure user identities, and scale online through massive growth.

To learn more about the four key phases on the path to customer identity maturity, download our free ebook: A Comprehensive Guide for Your Customer Identity Maturity Journey.

Whitepaper

Why Customer Identity?

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 16,400 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, and Teach for America, trust Okta to help protect the identities of their workforces and customers. To learn more visit okta.com. okta.com

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871