

# How to Create the Identity Experience Your Customers Want



Regardless of your organization's location, industry, or size, its success with customer identity and access management (CIAM) depends on one central element: incredible customer experience (CX) backed by bulletproof security.

Vanity user experience (UX) projects that gloss over technical problems at the login won't do. We're talking about seamless, secure, modern identity experiences that act as portals to profitability.

Why is CX so important for CIAM? Because it's the minimum customers expect from organizations today. Whether you're a digital-first business or you intend to master omni-channel services, your customers anticipate a simple, effortless login experience with impeccable security. But this isn't always their reality.

Customers get spooked when they need to resurrect long-forgotten login credentials to access your services. Attempting this feat can involve convoluted password reset processes, endless security questions, and calls to the help desk. Left frustrated, these customers are lost—never to return, never to recommend.

## This report explores:

- How businesses are not meeting their customers' expectations and demands through their current CIAM strategies.
- How consumers are currently using logins, and what they expect from future identity experiences.
- Why CIAM technologies and processes minimize consumer frustrations.
- How to pair authentication with the right level of security for exceptional CX.

# It's Time to Take Back Control

First impressions are critical: they build credibility and set expectations for users. Logging in is often the first interaction a user has with your organization, and it's imperative that you make this experience seamless and secure.

This is why identity management can no longer be overlooked by organizations in favor of other digital transformation initiatives. Your login is an incredibly valuable asset with the potential to drive success, and it needs your investment.

To help you create the identity experiences that your customers want, this report presents strategies for transforming their login experience. It investigates how modern identity management can unlock new business opportunities—without compromising on security.

Plus, with exclusive insight from more than 17,000 global IT and marketing decision makers and consumers, it gives you a clear picture of the tactics your peers and competitors use to deliver exceptional identity experiences.

US organizations' progress rolling out biometric logins is ahead of organizations in APAC, EMEA, and LATAM, and the US is ahead of EMEA and LATAM in implementing multi-factor authentication (MFA).

- **86% of consumers** admit to reusing passwords.
- **87% of developers** see productivity improve when they are able to use the software-as-a-service (SaaS) components they want and need.
- **58% of development teams** expect to add new third-party SaaS components to their application strategy over the next year.

## The value of authentication:

Before we dive into the power and value of authentication, it's important that we break down these key modern identity management terms.



### **Identity and access management (IAM):**

This is the umbrella discipline that allows the right person (or entity) to access the right resources, at the right time.



**CIAM:** This is a system that sits under the IAM umbrella, and is how companies give their end users access to their digital properties as well as how they govern, collect, analyze, and securely store data for those users. CIAM sits at the intersection of security, customer experience, and analytics.



**Identity as a services (IDaaS):** This is a cloud-based solution for IAM functions that allows all users (customers, employees, and third parties) to more securely access sensitive information both on and off-premises. IDaaS also means collecting intelligence to better understand, monitor, and improve their behaviors.



**Identity experiences:** This describes the entire journey your customers take from the first time they log in to your business, to the time they deactivate their account.

# Today's Authentication Landscape

In the past, consumer authentication was often overlooked by busy IT leaders. Some viewed it mostly as a way to manage customer information. Then came the CX juggernauts. Brands like Netflix, Amazon, Uber, and Apple transformed the way we use, engage with, and choose digital authentication experiences.

They forced other brands to compete in the realm of digital identity. Logins went from functional necessities to opportunities for driving engagement and strengthening brand loyalty.

Then, the global pandemic hit, accelerating the use of digital services across every demographic and changing the authentication market forever.

Faced with these fluctuating pressures and responsibilities, businesses are now leveraging their IAM strategies and CIAM solutions to achieve their goals:

- 1. Meet ever changing consumer behaviors and demands:** As we've seen, the way we use digital services can shift overnight—particularly for sectors like banking, healthcare, and e-commerce. CIAM has helped many brands meet the demand for more personalized, streamlined offerings.
- 2. Keep up with competitors and innovators:** Whether you're B2B, B2C, or B2E, individuals expect the same flawless login experience from your business as they receive from their phone, their apps, and even their streaming services. Your rivals aren't just competitor brands—they're any brand with a digital offering.
- 3. Protect customers (and employees) from cyber threats and data breaches:** All business data has incredible value—especially when organizations can apply that data to personalize services—for example, by recommending products. To be a good steward of data and steer clear of penalties for non-compliance, your organization must protect customer identity. From the moment a user first logs in until they delete their account, you are responsible for keeping their data safe from cyber threats.
- 4. Improve operational efficiency:** Data silos, Frankenstein architectures, slow systems, and poor visibility are just some of the challenges IT and operational teams battle on a daily basis. When you're developing new services and streamlining

# 92%

of consumers expect businesses to keep their personal information safe.

processes, your IAM strategy must be robust enough to improve the productivity and efficiency of your workforce.

- 5. Build recurring revenue:** Customer data has the potential to open new revenue streams. Businesses can leverage it to design new loyalty programs, target specific groups like super-users or dormant accounts, and create personalized offerings.

By establishing flexible, responsive authentication solutions, leading organizations have been able to navigate these fluctuating changes and respond to consumer demand through seamless CX. But not all businesses have deciphered what their customers want in an identity experience.

# “

Identity has become more important since COVID has made physical boundaries irrelevant.

Andras Cser  
VP and Principal Analyst, Forrester Research

# The Identity Experiences Your Customers Want

The login experience consumers want most is MFA, followed closely by SSO.

As an IT leader, how confidently can you answer these three questions?

1. How are your customers currently using your login solutions?
2. What are their preferred methods for authentication?
3. Are you prepared to give them what they want?

We surveyed more than 14,700 global consumers to help you understand the authentication experiences they hope for. Explore the survey insights to inform how you tailor your strategies and find the right solutions for your organization and for the customer experience.

## Multi-factor authentication (MFA)

**Definition:** *MFA is a method of verification that requires the user to provide more than one piece of identification—often signing in with a password and a one-time code or confirmation on your phone.*

### ? Did you know?

MFA, with one-time codes and SMS verification, can block 99.9% of account hacking attacks.

Expected to grow, on average, 16.2% annually through 2026, MFA is one of the most commonly used authentication solutions for global consumers. In Singapore, it's the most popular: 52% of consumers report using MFA "frequently/all the time." The same goes for 42% of Americans. Dutch IT and marketing leaders and decision makers surveyed are more likely than their French, German, and Belgian counterparts to say their companies currently offer customers the ability to log in with multi-factor authentication.

## Biometrics

**Definition:** *A cyber security process that verifies a user's identity using their unique biological characteristics, such as fingerprints, voice, or face, instead of a password.*

### ? Did you know?

44% of consumers admit they are more likely to sign up to an app or online service if a company offers biometric authentication

UK businesses are falling especially short when it comes to biometrics—only 14% offer it.

While it may take some consumers a little more time to get used to the idea of biometrics, it's definitely an area to watch.

## Single-sign on (SSO)

**Definition:** *A single ID and password consumers can use for multiple related services.*

### ? Did you know?

48% of consumers are likely to sign up to an app or service if they can use SSO. This is especially the case for Argentinian (63%), Mexican (62%), Brazilian (59%), and Singaporean (56%) consumers.

One of the things that makes SSO so popular is that it helps to eliminate the need for multiple passwords (and for resetting those passwords).



## Social logins

**Definition:** An option for users to sign in to an app or web page using social media credentials, such as their login for Facebook, Twitter, Apple, or Google.

### ? Did you know?

Implementing social logins can increase conversion rates 20–40%.

Social logins are growing in popularity with consumers. Many Brazilian (52%), Argentinian (50%), Mexican (47%), and Singaporean (41%) consumers use social logins all the time or frequently. However, social logins are less popular in Japan (22%), the UK (28%), and Germany (21%). Latin American consumers are more likely to sign up for an app or online service if they are able to use social logins compared to consumers in all other markets.

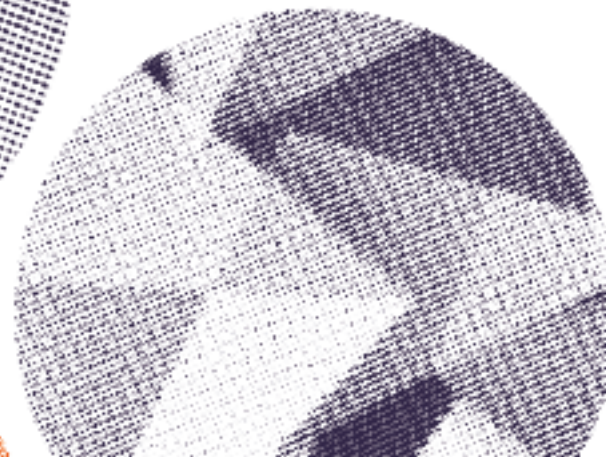
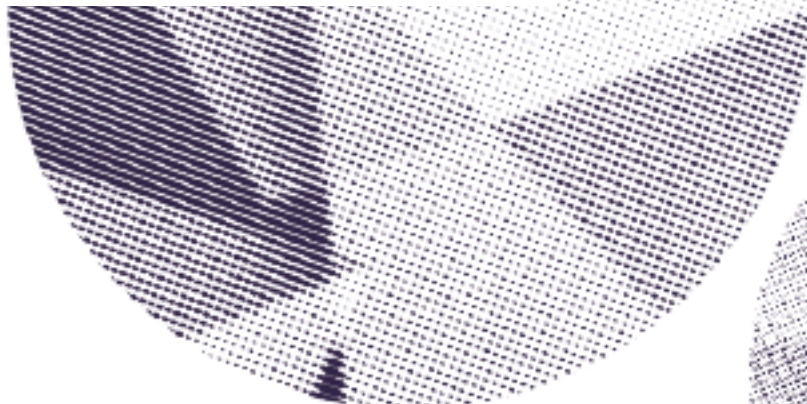
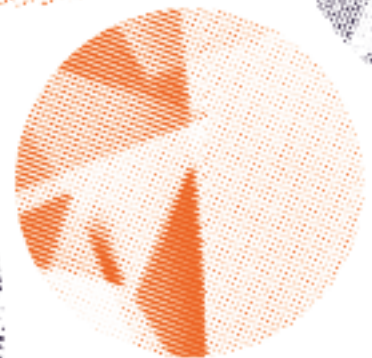
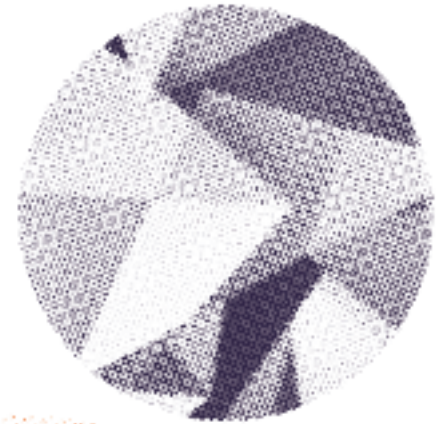
## Passwordless authentication

**Definition:** An authentication method that doesn't use passwords. Users are sent a one-time link or code to enter, or they can verify their identity using a biometric trait, like their face or fingerprint.

### ? Did you know?

80% of consumers admit to reusing passwords for more than one account when using online services.

Along with biometrics, passwordless authentication is one of the newest forms of authentication. 26% of US consumers reported using passwordless authentication all the time or frequently.



# Log In or Log Out: Customer Expectations vs. Reality

Convenience, security, and speed: the three things consumers want from your login.

**First impressions matter.** That's why your organization invests in branding, marketing, and PR. But what about your authentication process?







After all, your customers have high expectations. When they arrive at your login, they want convenience and control: they want to choose which CIAM solution to use—whether it's MFA, SSO, or biometrics. They want a brand experience that resembles a concierge desk: a 24/7 service where no demand is too big. To top it off, they don't want to see any technical glitches or have to re-sign up on another device. Consumers want seamless omni-channel experiences—not to be left out in the cold.

But when your CIAM solutions are outdated, or they don't yet exist, you can't deliver this experience.

## Passwordless authentication

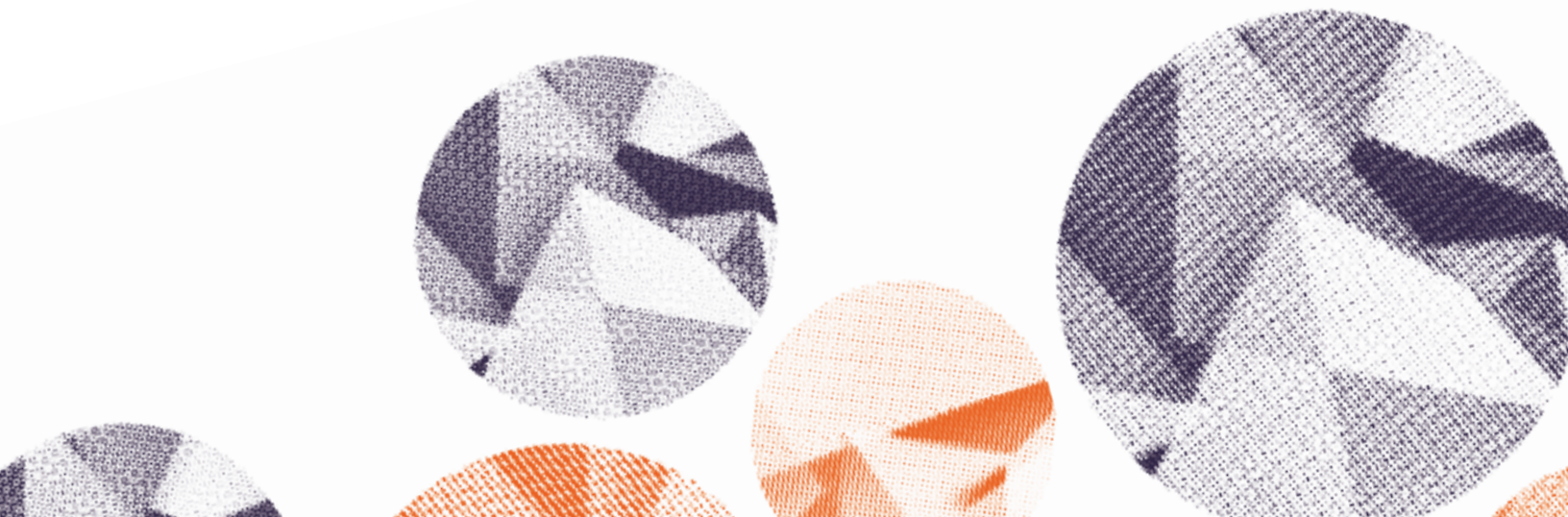
We found consumers rank passwords among their top frustrations with the sign-up process.

When we asked more than 2,400 IT and marketing decision makers what kind of authentication services their business offers, the results were striking:

-  47% offer SSO capabilities
-  35% offer social logins
-  29% offer MFA
-  25% offer biometrics
-  20% offer passwordless
-  8% offer none of these

The numbers don't lie. One in ten companies with online services neglect to offer any of these login options. British (21%) and Japanese (19%) organizations are more likely than those in all other countries surveyed to say that they don't offer any of these online login services to their customers.

Organizations just aren't meeting their customers' demands for the latest login technology. And consumers are fed up, particularly with passwords. The UK is the slowest adopter of social logins: only 19% of businesses offer it compared to 35% of US organizations. SSO fares better with adoption, particularly in Argentina (59%), Mexico (56%), Australia (53%), and France (53%).



Consumers in Asia-Pacific and Latin America are more likely than those in EMEA and the US to find having to fill in long login or sign-up forms frustrating (APAC 55% and LATAM 51% compared to EMEA 46% and the US 36%).

## Consumer frustration

Another top consideration for consumers today is being able to identify apps and online services that will keep their personal information safe. Japanese (50%) and German (48%) consumers are more likely than those in all other markets surveyed to say they find it difficult to identify apps and online services that will keep their personal information safe. Overall, less than 3 in 10 (28%) find these offerings easy to identify.

Today's consumers express these top frustrations:



**48%** Having to fill in long login or sign-up forms



**47%** Creating a password that has to meet certain requirements (e.g. number of digits, symbols)



**40%** Entering private information (e.g., passport number, tax file number)



**43%** Having to create a new ID/password for every app or online service



**23%** Verifying accounts via a one-time password sent to a phone/email



**14%** None/don't know or not applicable

## Lost conversions = lost revenue

Bad customer experiences cost businesses more than their reputation. An overly arduous login process has caused 83% of consumers to abandon their cart or sign-up attempt.

IT and marketing decision makers in Latin America are more likely than those in EMEA to attribute these abandonments to both sign-up processes (LATAM 56% vs. EMEA 46%) and login processes (LATAM 46% vs. EMEA 37%). They are, however, less likely (56%) than their Asia-Pacific peers (63%) to attribute these abandonments to sign-up processes.

E-commerce stores lose \$18 billion in sales per year from cart abandonment alone.

## CIAM could be your lifeboat

Repairing the damage caused by login friction is vital for every organization. That's why it's critical that organizations put customer experience and security at the forefront of their authentication strategy. Leading decision makers are already taking action, using CIAM to facilitate change and meet evolving customer expectations.

SaaS solutions like CIAM are purposefully designed to help organizations deliver scalable identity experiences—whether through MFA, biometrics, or SSO.

Because these solutions work across apps and web pages, they help businesses unlock omni-channel opportunities by breaking down siloed user data, thereby boosting revenue, customer loyalty, and competitiveness. Plus, they provide additional layers of security to make your organization less vulnerable to cyber attacks, data breaches, and identity fraud.



# Your CIAM Checklist for Delivering Exceptional Identity Experiences

To help your organization prevent future roadblocks when implementing your CIAM strategy, we've designed this CIAM checklist. Not only will it help you unite the rest of your team, but it will also help encourage collaboration with developers and strengthen buy-in support.

## 1 Set up a CIAM HQ

Familiarize yourself with the quantifiable benefits of CIAM and share them with your wider team. In this early stage of the decision-making, you're likely to be the in-house CIAM expert in your business. So, make sure to get to know the benefits. Why CIAM?

- Delivers a secure and frictionless login experience
- Guides compliance with data privacy laws, such as the CCPA and the GDPR
- Protects data assets against malicious intrusion
- Derives more specific, meaningful insights from customer data

## 2 Bring together developers, IT teams, and marketers

Create a meeting point where wider teams can come together and align on how to choose, implement, and manage CIAM solutions, as well as how to allocate roles and responsibilities. It's vital to include your development team as early on in this process as you can.

Our research shows that 87% of developers see productivity improve when they are able to use the SaaS components they want and need, and 88% say it improves their overall job satisfaction.

Getting to choose SaaS components matters to 91% of developers.

## 3 Visit the ROI consultants

Speak to vendors, peers, and authentication experts so that you can build a business case for the C-suite. They'll want to see how this investment will generate a return, so come prepared with an estimated figure at that point. Don't forget, quantifiable results don't just include revenue: they can also include increased employee happiness, productivity, and satisfaction.

## 4 Choose your pilot (program)

Before you make a final decision on whether to build vs. buy your CIAM solutions, it's important to establish with your developers and engineers how you plan on testing it.

Our research shows that trials and proof of concepts (POCs) are the preferred methods of testing SaaS components by fast-moving organizations. Plus, statistics show that companies that listen to developer feedback early on in the purchase cycle are more likely to avoid technical obstacles later on.

Gartner predicts the SaaS market segment could grow to \$141 billion in 2022.

# Lost Customers? CIAM Can Get Them Back

It's never too late to take control of your customers' experience. CIAM has the power to transform customer interactions, fix security risks, and even to deliver 24/7 service—and it all starts at login. Find out how Okta can help your organization along the path to modern identity and better CX.

If you'd like to find out more about how CIAM can help your business, visit <https://www.okta.com/customer-identity/>

## Methodology

The study was conducted online by Auth0 (a product unit of Okta) and YouGov from February to August 2021. The research consisted of two surveys, questioning more than 14,700 consumers and 2,400 IT and marketing decision-makers who work for businesses that offer an app/online service to customers (excluding sole-traders) across 12 global markets: The United States, United Kingdom, Belgium, France, Germany, the Netherlands, Australia, Singapore, Japan, Argentina, Brazil, and Mexico. The data for the consumer study was post-weighted by age, gender, and region to reflect the latest population estimates in each market.



## 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 14,000 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. To learn more, visit [okta.com](https://www.okta.com).