



Whitepaper

Security from the first click to the long haul

Contents

2	How modern customer identity can help you build trust and loyalty before, at, and after login
3	Three ways innovative powerhouses have reinvented the customer experience
4	Welcome to the era of no trade-offs
5	Secure and seamless experiences begin with getting identity right
6	Customer identity cheatsheet
7	Delivering secure experiences across the customer journey with CIAM (Before, at, and after login)
8	Before login: How to protect your customers (when you haven't even met them yet)
12	At login: How to secure your digital front door (and ruin a hacker's day)
17	After login: How to remain everyone's favorite app (forever and ever)
22	How Auth0 helps secure CIAM



How modern customer identity can help you build trust and loyalty before, at, and after login

Consumers expect more from every organization, every purchase, and every experience. Your customers tap their phone and, in seconds, they've booked a ride, ordered a coffee, or generated a bespoke playlist tailored to their mood. No logins. No waiting. No thinking twice.

The explosion of GenAI has only raised this already-high bar, especially when it comes to tailored experiences and instant gratification.

Whether online, in-app, or in person, consumers today want brands to know them, anticipate their needs, and remove friction — and they want all this ***without compromising security.***

Three ways innovative powerhouses have reinvented the customer experience

1



Instant gratification

Instant access and seamless experiences, such as one-click checkouts



DEAL-BREAKERS:

- CAPTCHA after CAPTCHA
- Clunky password resets

2



Consistency

Interactions continue seamlessly across channels, devices, products, and services



DEAL-BREAKERS:

- Re-entering info
- Re-logging in
- Losing progress between platforms

3



Hyper-personalization

Individualized experiences and recommendations based on preferences and behaviors



DEAL-BREAKERS:

- Generic experiences
- Irrelevant communications
- Delayed support

Welcome to the era of no trade-offs

When a customer makes a purchase, creates an account, or logs in, they are placing trust in your brand. That means secure digital experiences are table stakes for winning and retaining customers.

But here's the challenge: That level of security can't add friction that drives customers away.

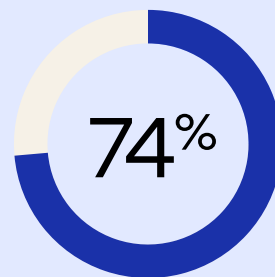
Like it or not, your business is operating in the era of no trade-offs, where security and seamless customer experience (CX) must coexist.

Living up to this no-trade-off standard requires Customer Identity and Access Management (CIAM) — also known interchangeably as “customer identity.” When done right, CIAM builds security directly into the seamless experiences your customers love. It protects interactions across the entire customer journey — before, at, and after login — while enabling the speed, personalization, and seamless access today's customers have come to expect.

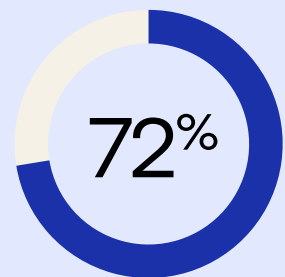
Digital trust is a core concern across generations

When creating a new account, more users consider a company's reputation and security measures more important than the overall quality or value of the product itself.

These numbers are even higher among older and more tech-inclined users. As a respondent's age or tech affinity rises, so does their likelihood to consider trustworthiness, transparency, and security important factors when deciding to create a personal account.



**Reputation/
trustworthiness**



**Security
measures**

% of respondents listing the above qualities as “important factors” when deciding whether to create an account

[SOURCE](#)

Secure and seamless experiences begin with getting identity right

Identity is the connective tissue between every person and every technology. By defining the “who” in each interaction and determining who can access what, when, and under what permissions at the resource level — through, for example, fine-grained authorization (FGA) — it serves as the foundation of the digital world. This centrality carries a lot of significance: To deliver the secure, elevated experiences customers expect, you have to get identity right.

Scream it from the rooftops: Identity is security

Because identity underpins every digital interaction, it should come as no surprise that it’s a prime target for attackers. Identity remains the top initial access vector in breaches, with around 60% of cybersecurity incidents involving the human element — namely, compromised credentials or social engineering like phishing.¹ For organizations with customer-facing apps, these threats don’t stop at the login screen. They appear in fake registrations, abused promo codes, and stolen session cookies that let attackers hijack legitimate sessions — no password required. This means that “getting identity right” is not limited to the moment of authentication; identity security should also extend to the pre-authentication and post-authentication risks that can compromise security and undermine your business.

To stay ahead of evolving threats, you need proactive, built-in identity security. That means detecting and responding to risky behavior in real time, protecting exposed surfaces, and limiting access if an attacker gets in. Security should be embedded into the entire customer journey, not bolted on after the fact.

It’s time to ditch dated identity and excessive friction

Protecting customers from account takeover and other malicious actions is crucial. But when dated protections create frustrating stumbling blocks for customers (for example, difficult-to-remember passwords, frequent CAPTCHAs, or a flood of multi-factor authentication (MFA) requests), your business is at risk.

These good-faith security efforts often create excessive customer friction, leading to abandoned journeys, lower conversion rates, and lost business. Even worse, this burden on customers doesn’t necessarily mean better security. For example, the common MFA method of combining traditional usernames and passwords with SMS is highly vulnerable to social engineering and SIM-swapping attacks.

Time has run out for outdated identity solutions. It’s time to move beyond treating identity as just single sign-on (SSO) and MFA checkboxes and, instead, reimagine it as the foundational backbone of your security posture and business strategy, deeply woven into every customer touchpoint.

To prevail, you need modern customer identity. Let’s dive into exactly why.

^[1] Verizon Data Breach Investigation Report 2025

Customer identity cheatsheet

At its core, CIAM includes:



User registration:
Creating user records.



User authentication:
Verifying user identity.



User authorization:
Managing access levels.



Identity management:
Enabling user and admin control over data and access.



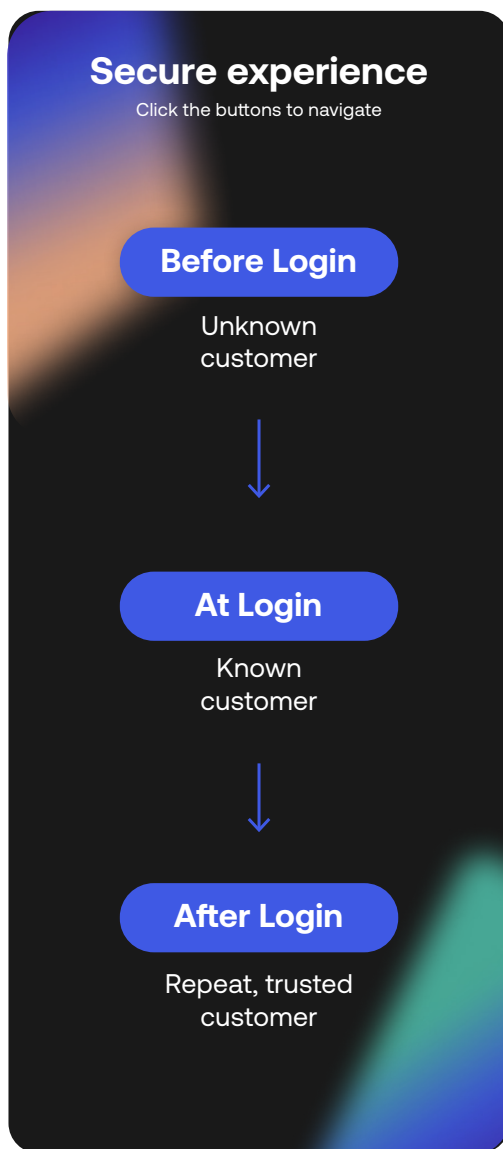
Developer tooling:
Building identity for custom flows.

Effectively implemented, modern CIAM empowers businesses to:

- ☐ **Secure every identity, every experience:**
Built-in protection for all users — human and non-human (e.g., AI agents) — across every platform, every interaction.
- ☐ **Streamline access:**
Improve conversion with fast sign-ups, passwordless login, and connected experiences across channels.
- ☐ **Personalize experiences:**
Drive loyalty and growth with a 360° view using progressive profiling and consented first-party data for tailored experiences and cross-selling.
- ☐ **Accelerate innovation at scale:**
Free up developer time with an extensible platform that's fast to integrate, easy to maintain, and built to grow.
- ☐ **Simplify compliance:**
Meet evolving standards like GDPR and HIPAA with out-of-the-box features that avoid costly gaps.

Bottom Line: Customer identity extends far beyond the login box. It's about enabling secure, convenient, and personalized experiences throughout the entire customer journey — **before, at, and after login.**

Delivering secure experiences across the customer journey with CIAM **(Before, at, and after login)**



Exceptional customer experiences demand security that extends well beyond the login box. Building trust and driving loyalty requires optimizing every touchpoint: from facilitating guest checkout and loyalty program sign-ups to managing sensitive personal or payment data. Each interaction in the customer journey is an opportunity to both bolster security and elevate the user experience. Striking this crucial balance begins with customer identity.

In this section, we'll examine how modern CIAM addresses inherent risks and threats across the journey — before, at, and after login — and crucially, how it transforms security measures into seamless, experience-enhancing interactions.

Before Login

At Login

After Login



Before login:

How to protect your customers (when you haven't even met them yet)

The customer journey doesn't start at login; in fact, it starts long before customers ever reach the login box. First impressions are made in milliseconds, and any friction in those early moments can drive potential customers away before you even learn their name. Whether they're browsing, shopping, or signing up, your identity strategy needs to work behind the scenes to reduce drop-off, protect against threats (think: automated, bot attacks), and make it effortless for unknown visitors to become known, trusted customers.

Before Login

At Login

After Login



Using modern identity to make account creation easier than ever

One of the most common reasons customers abandon purchases is a difficult, tiring sign-up process. To reduce abandonment, account creation must be as effortless as possible, while still allowing for secure identity verification. The good news is, you have options.

62%

of users cite filling out long sign-up or login forms as a source of frustration. It's the #1 source of sign-up or login frustration²

Social login

One popular option for reducing abandoned sign-ups is social login. It lets customers sign up with credentials they already trust — from Google, Apple, and Facebook accounts, for example — and complete the process in seconds. This not only accelerates account creation, but also enables you to take advantage of the fact that their identity has already been verified. And, social login means one less account where they may be reusing a password, which makes their account more difficult to hack.

But what if customers forget how they originally signed up? Was it with email and password, or a social login like Google or Facebook? If they guess wrong, they may unintentionally create a duplicate account. Modern CIAM solves this with intelligent account linking. When a returning customer uses a different login method, the system detects the existing account and offers to link it to that login method. Even if a duplicate gets created, a secure, consent-based flow can merge the records later — preserving data, preferences, and history.

Guest accounts

Guest accounts offer another powerful option, especially for commerce. With modern CIAM, you can generate an anonymous customer ID as soon as someone adds an item to their cart — even before they've shared any personal data. This ID lets the site remember what's in the cart across pages and devices, calculate taxes, show real-time inventory, and even enable one-click checkout, all without forcing account creation. Later, when the customer is ready, you can prompt them to add a small piece of identity information — an email or phone number — to upgrade that guest session into a persistent profile.

From there, **progressive profiling** takes over. Rather than asking for a mountain of personal information up front, you can gather data gradually as the customer continues to engage. For example, you can ask for a shipping address at checkout, a phone number for delivery updates, or a preferred store when location services are enabled. Each new data point improves personalization, auto-fills future forms, and routes support more efficiently. Progressive profiling asks only what's needed, when it's needed, and always with consent. It builds trust, strengthens security, and keeps the journey seamless from the very first interaction.

Before Login

At Login

After Login



Using modern identity to keep fake sign-ups from draining your marketing budget

Before a legitimate customer even reaches your login screen, attackers are already at work — often in the form of bots. Automated traffic now makes up nearly half of all internet activity.³ Some bots are harmless. Many are not. GenAI is making it easier and cheaper to carry out malicious bot attacks that are harder to detect.⁴ They exploit your sign-up flows, test stolen credentials, and drain your acquisition budget by creating fake accounts at scale. Without the right defenses, bots can flood your system, wasting resources and opening the door to larger attacks.

And these fake sign-ups don't just pollute your database. They cost you money — real money. Welcome offers and loyalty programs meant for new customers become easy targets. A free \$50 checking bonus, 20% off a first order, or loyalty points with sign-up? Bots are all over it. In fact, bot-driven ad fraud is estimated to have cost businesses over **\$71 billion** in 2024 alone — a 33% jump from 2022.⁵ And the threat is escalating: generative AI is making it easier than ever to launch sophisticated, automated attacks that bypass legacy defenses like picture-based CAPTCHAs.



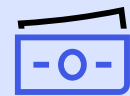
~50%

Of all internet traffic is made up of bots⁷



120x

During sustained attacks, fake accounts outnumber real ones 120 to 1⁸



\$2.9M

Is the average cost of a major bot attack⁹



44.5%

Of registration attempts on the Auth0 platform were flagged as sign-up attacks last year. This number is even higher in Financial Services (65%) and Retail (70%)⁶

[3] 2024 Bad Bot Report, Imperva, 2024

[4] "How Cybercriminals Are Using Gen AI to Scale Their Scams" – Okta Newsroom

[5] Bot clicks and fake traffic set to cost advertisers over \$71bn in 2024, MarketingTech, 2024

[6] Auth0 Customer Identity Trends Report 2025

[7] 2024 Bad Bot Report, Imperva, 2024

[8] Auth0 Customer Identity Trends Report 2025

[9] Bot Wars: How Bad Bots are Hurting Businesses Survey, Fastly, 2024

Before Login

At Login

After Login



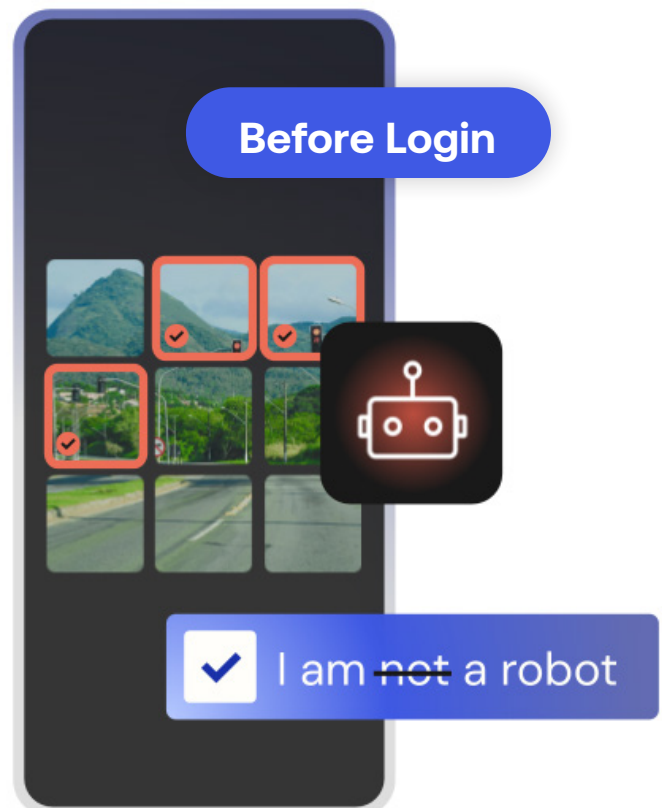
Using modern identity to stop bots without slowing down real customers

If your identity security only kicks in at the login box, you're already too late. Bots often strike before a customer gets that far, flooding sign-up flows, testing stolen credentials, and abusing promotional offers at scale. Traditional bot defenses (like puzzle CAPTCHAs) aren't enough to stop sophisticated bots, which now solve many challenges faster than humans. The worst part? In addition to falling short at bot detection, these defenses frustrate real users, driving down abandonment and trust. It's the definition of a lose-lose.

A modern CIAM solution can stop bad bots in their tracks — without making real customers jump through hoops. With the right CIAM in place, **bot detection** provides continuous, real-time monitoring of identity-related signals (like IP reputation, ASN data, and user agent behavior) to spot suspicious traffic early. When risk is detected, the system responds with low-friction challenges designed for humans, not bots. Advanced solutions also leverage AI models tailored to specific attack types, like fake sign-ups or credential stuffing, boosting accuracy and minimizing false positives so most real users never even see a challenge.

The best CIAM solutions also offer out-of-box integrations with third-party **bot challenges** for greater flexibility, preventing reliance on outdated CAPTCHAs. This is particularly vital in high-risk industries like finance, travel, and social media that demand advanced bot controls.

And for higher-risk traffic, the ability to **proactively and automatically block known malicious traffic** (like IPs or CIDRs) or entire geographies where you don't do business creates another crucial first line of defense, filtering threats *before* they interact with your sign-up or login box.



Before Login

At Login

After Login



At login:

How to secure your digital front door (and ruin a hacker's day)

The login box is more than just a username and password — it's your digital front door. Often, it's the first impression customers have of your brand, and just as often, it's the first target for attackers. One look at your login box gives sophisticated bad actors an understanding of what protections you have (or don't have) in place across the organization. When they spot low-hanging fruit, they're inclined to act — at scale.

The stakes are high: large-scale breaches risk catastrophic damage to brand and revenue. Luckily, modern CIAM can help organizations strengthen their defenses without compromising on customer experience.

**64%**

Of users are concerned about identity fraud, while only 10% express little or no concern¹⁰

**~1 in 4**

Consumers either always (6%) or often (17%) abandon an online purchase due to issues with sign-up or login processes¹¹

[10] Auth0 Customer Identity Trends Report 2025

[11] Auth0 Customer Identity Trends Report 2025

Before Login

At Login

After Login



Using modern identity to reduce friction without sacrificing security

Friction kills experiences. Even minor barriers — forced sign-ups, confusing flows, redundant MFA prompts — can cause customers to walk away.

Modern CIAM allows you to centralize customer identity across all products, services, and brands, solving key friction points.

Prevent login abandonment

Login abandonment means a bad experience and a lost chance to interact with an identified customer. With **single sign-on (SSO)**, you can significantly reduce login fatigue and improve security by minimizing password reuse and reducing the number of abandoned accounts.

Offer seamless experiences between channels

Imagine checking in for a flight in an airline app, only to be redirected to log in again on the website to claim upgrade credits. **Mobile-to-web SSO** eliminates this extra step, ensuring a seamless and secure experience with one login — backed by safeguards like device binding, app attestation, and Demonstration of Proof-of-Possession (DPoP) — for a smooth, consistent brand experience.

Reduce drop-off during password resets

A frustrating reset flow can lead to abandoned sessions or even duplicate accounts. Low-friction password reset solutions keep customers from abandoning their user journey for something as simple as a forgotten password while still enforcing strong security through features like **breached password detection, strong password enforcement, and reuse prevention**.



Using modern identity to smash credential-based threats

Attackers today don't break in, they log in. Passwords are the weakest link in most login flows and the most common cause of account compromise.^[12] Once inside, attackers can drain funds, steal identities, and erode trust in your brand.

~1 in 4 

Consumers were a victim of account takeover in 2024, up from 18% in 2023^[13]

68% 

Of users report reusing passwords across multiple accounts, largely because remembering unique passwords is hard^[14]

[12] Verizon Data Breach Investigation Report, 2024

[13] Sift's Q3 2024 Digital Trust Index

[14] Auth0 Customer Identity Trends Report 2025

Before Login

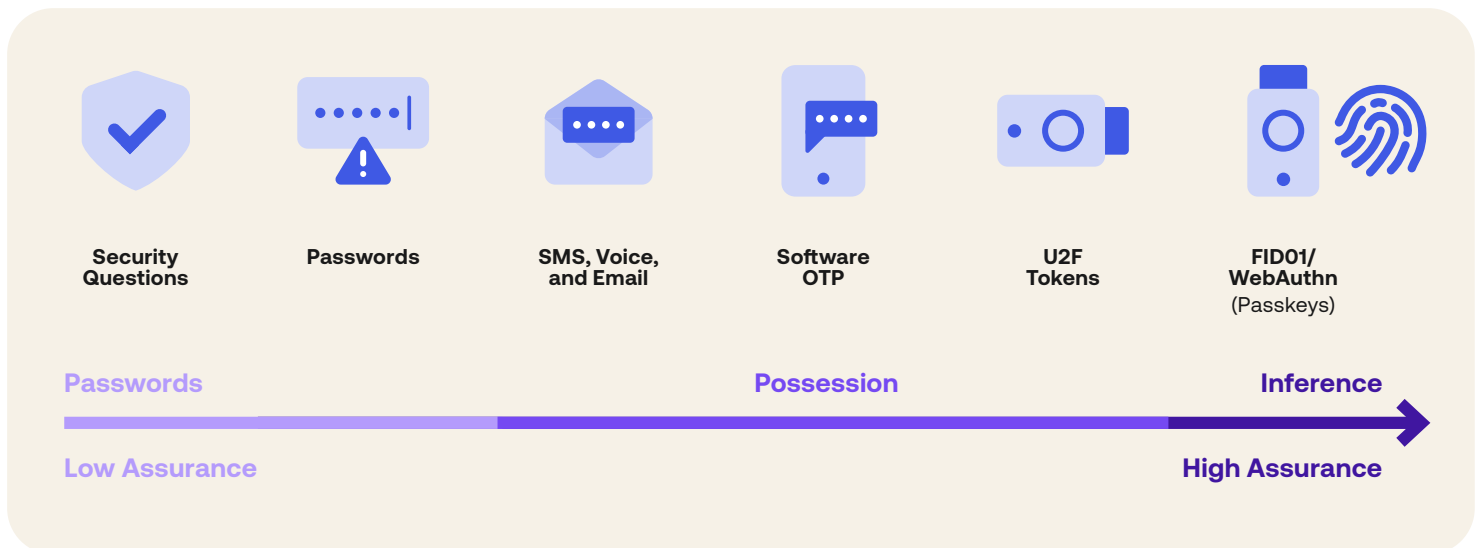
At Login

After Login

Modern CIAM uses layered, context-aware defenses to detect credential threats early, respond in real time, and keep friction low for trusted users.

Multi-factor authentication (MFA) is widely endorsed by security authorities like [NIST](#) and [OWASP](#) as a way to increase defenses at login. But when applied too often, it can frustrate users and drive up abandonment. Adaptive MFA offsets the potential frustration of MFA by offering a smarter, context-aware approach. It evaluates risk signals like device, network, location, and behavior to decide when an extra verification step is truly needed. If a customer logs in from their usual device at home, Adaptive MFA knows to let them breeze through. But if the same credentials are used from a new device in another country, Adaptive MFA steps in with additional verification. The ideal CIAM solution will further enhance decision-making and security responsiveness through integrations with additional third-party risk engines.

Passkeys are one of the most effective phishing-resistant authenticators available. They store cryptographic credentials on a customer's device and use biometrics or a device PIN to authenticate. Nothing is typed, nothing is shared, and nothing can be phished. Not all authenticators have the stamp of true phishing resistance. A truly phishing-resistant authenticator stops attackers from stealing your login info even if you fall for a fake website. It works by using unique digital "keys" stored securely on your device that are cryptographically bound to the real website, blocking phishers from intercepting your credentials.



Before Login

At Login

After Login

In addition to layering context-aware defenses that the user can see, modern solutions work behind the scenes to recognize abuse patterns, flag risky behavior, and enforce better authentication hygiene. The right solution should be able to:

- Detect repeated failed logins targeting one or multiple users and automatically block access (and notify the end-user).
- Detect suspected bot activity at login and introduce bot challenges.
- Proactively block traffic from known malicious IPs, CIDRs, or regions where you don't do business.
- Detect breached passwords at login, sign-up, or password reset.
- Prevent weak or common passwords through configurable password policies and dictionary checks.
- Discourage password reuse with history controls and reset policies.
- Offer integrations with your security stack like risk engines, SeCops tools like SIEMs, and preferred bot challenges.

Why phishing is getting harder to prevent

Phishing is no longer limited to suspicious emails. With the rise of generative AI, attackers can mimic brands, voices, emails, and entire login experiences with alarming realism. Phishing kits (collections of tools, resources, and scripts that facilitate the deployment of phishing attacks) make it even easier for bad actors to initiate a breach through phishing. These kits are easily purchased online or assembled using AI-generated code, making the barrier for entry in cybercrime extraordinarily low.

While the customer may be the entry point in a phishing scenario, it's your brand that carries the consequences.

Imagine this: A customer receives a call from someone claiming to be their telecom provider. The caller knows their name, phone number, email, account number and last statement balance. They mention a new promotion and ask the customer to confirm a code just sent via email. The email is real — it's from the provider's domain. Trusting the context, the customer reads the code aloud. What they don't realize is that the attacker has just initiated a password reset. With that code, the attacker takes over the account, locks the customer out, and orders a new cell phone — charged to the customer's account.

Customer phishing training is highly unlikely to stop that attack. But the sudden password reset request and login from an unknown device and location? A big red flag for a modern CIAM risk engine, which could have kept the customer (and the telecom provider brand) safe.

94%

Of organizations reported falling victim to phishing in 2024^[15]

**<5
minutes**

Average time to generate a convincing phishing lure using GenAI (down from 2 days)^[16]

**703%
surge**

In credential phishing attacks in the second half of 2024 alone^[17]

[15] Email Security Risk Report 2024, Egress

[16] X-Force Threat Intelligence Index 2024, IBM

[17] The 2024 Phishing Intelligence Report, SlashNext

Before Login

At Login

After Login

Using modern identity to test and optimize (before your users run to the comments section)



Security shouldn't be a black box — CIAM should give you full observability and control before customer experience is impacted. And you shouldn't have to wait until go-live to assess the efficacy of your CIAM solution's security or CX performance.

Poorly implemented new security measures like too-frequent CAPTCHAs for real users or excessively rigid MFA policies can leave customers frustrated and drive up abandonment rates. That's why it's important to choose a CIAM solution that offers a **monitoring mode**. These tools let you observe how identity security features would affect real application traffic *without actually impacting it*, which allows you to fine-tune policies like bot detection in a risk-free environment. You can evaluate their impact, optimize configurations, and roll out protections with confidence, without disrupting the user experience.

Using modern identity to honor the customer bill of rights



On top of its CX and security balancing prowess, centralized customer identity makes it easier to **meet regulations like GDPR and CCPA**, which require companies to provide users' data and information about its use upon request. And since this extends to partner systems and data, CIAM provides the easy access you need to allow compliance, keeping your customers happy in the process.



Before Login

At Login

After Login



After login:

How to remain everyone's favorite app (forever and ever)

In a security landscape where attackers can employ **post-authentication attack methods** to access users' sensitive information, it's crucial that your defenses not only protect users before and at login, but after login as well.

Using modern identity to get (really) clear on who can access what



To protect sensitive data without slowing users down, modern CIAM solutions must support least-privilege access. That means giving each user the exact permissions they need — and nothing more. Traditional role-based permissions (which are based on broad, static roles) can no longer meet the granular and dynamic demands of modern systems, and they can fall short of security and compliance standards like SOC 2 and PCI-DSS. To bring access in line with modern technology and security environments, permissions must be fine-grained and dynamic, adapting in real time to contextual information like user role, group, resource ownership, or session details. Modern CIAM solutions make this level of granularity and dynamism possible with tools like **fine-grained authorization (FGA)** that are capable of managing complex access decisions at scale with low latency and strong security.

Before Login

At Login

After Login



Example: CIAM defends against session hijacking

Imagine a trusted customer is logged into your application from Toronto. Ten minutes later, their session appears to be in Brisbane from a different device.

Major red flag.

Without post-login attack protection measures, this attacker could be free to take over the session from a real user for fraudulent activity. With post-login attack protection, CIAM can trigger additional security, like immediately requiring reauthentication.

Using modern identity to suss out suspicious behavior



Logging in does not guarantee that a session will remain secure, as evidenced by attack methods like **session hijacking**. Attackers accomplish this through methods like social engineering and stealing **session cookies** used by websites to keep users logged in as they navigate pages. If the stolen session cookie is still valid, the attacker can act as an already authenticated user without ever touching the login screen.

To provide protections after login. The ideal CIAM solution will have **session management** capabilities, which let you:

- Continuously monitor user sessions and detect anomalies like sudden IP and device changes.
- Customize responses in the event of suspicious activity by prompting reauthentication, logging the user out, or triggering additional security measures.
- Set custom session and refresh token timeouts to meet compliance or security policies.



17.3 B

Stolen session cookies from malware-infected devices in 2024¹⁸

Before Login

At Login

After Login

Using modern identity to make call center operations surprisingly delightful



Imagine you're calling customer support to resolve something urgent — maybe a flagged bank transaction, a lost package, or a billing issue. Before the agent can assist, they need to verify your identity. You're asked for a security passcode (which you've forgotten), then a series of questions: your birthday, the amount of your last transaction, your best friend's name. It's frustrating. More importantly, it's not secure: these answers are often easy to guess or find online.

Some organizations try to improve security in these out-of-band channels by sending a one-time passcode via SMS or email. But these traditional methods aren't foolproof either. SMS is vulnerable to SIM swapping. Email assumes your inbox is secure. And both rely on knowledge-based authentication — the kind that phishing and social engineering attacks are built to exploit. They also lack stronger, device-based protections like biometrics.

That's where asynchronous authentication with **CIBA (Client-Initiated Backchannel Authentication)** changes the game.

CIBA is a decoupled authentication protocol designed for scenarios like call centers, POS systems, and even AI-powered support agents. Instead of relying on security questions or one-time passcodes (OTPs), the agent — human or AI — initiates an authentication request that's sent directly as a push notification to your device or to your email inbox. You can then review the request and confirm using your fingerprint, face scan, or device PIN. One tap later, you're verified, and the support agent can take action securely. No sensitive data is sent over the push notification or the email. It's seamless for the customer, secure for the business, and critically, keeps a human in the loop for high-trust interactions, even when AI is involved.

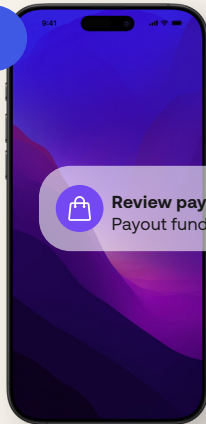
Before Login

At Login

After Login

Example: CIBA (Client-Initiated Backchannel Authentication)

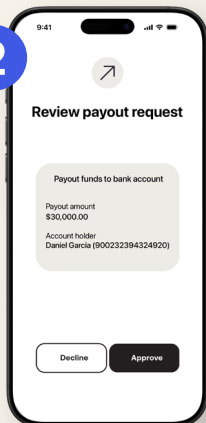
1



Step 1: Authentication request sent

The client (e.g., an app or service) sends an authentication request to the authorization server with the user's ID and required scopes. This triggers a push notification or backchannel prompt to the user—without requiring direct interaction on the client device.

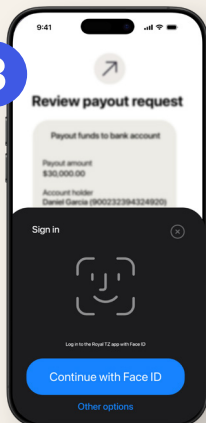
2



Step 2: User verification via backchannel

The user receives a prompt on a trusted device (via app, push notification, etc.) to review the request and confirm it using their fingerprint, face scan, or device PIN.

3



Step 3: Token issuance

One tap later, the user approves the request, and the authorization server notifies the client. The client then retrieves the access token to complete the process.

Before Login

At Login

After Login

Using modern identity to secure the really sensitive stuff



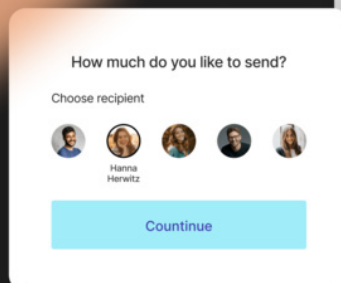
Too often, organizations rely on outdated security methods: MFA bombing that overwhelms users with low-risk prompts; auto-declined transactions with no explanation; or generic “New login. Was this you?” emails sent after the fact when damage may already be done. These tactics frustrate legitimate users and leave exploitable gaps for attackers.

Because they faced this challenge earlier than other industries, the financial services industry raised the bar on combining strong security with seamless CX. Now, organizations across industries are **adopting financial-grade identity practices** as tablestakes to strengthen security, protect privacy, and improve the user experience during sensitive interactions. The ideal CIAM solution will come equipped with these practices so your organization can benefit from financial-grade protections, regardless of industry or use case.

One of the most effective approaches is **Contextual Strong Customer Authentication (SCA)** — adaptive MFA designed specifically for high-risk actions that also require consent. When a sensitive action is detected (a large transaction or account change, for example) your CIAM platform can use SCA to trigger contextual step-up authentication using push notifications, WebAuthn, SMS, or email.

This capability extends beyond verifying identity. **Dynamic Linking** embeds transaction details — like amount, recipient, or purpose — directly into the approval request. With **Rich Authorization Requests (RAR)**, users see clear, actionable prompts.

“Do you approve a person-to-person payment to Hanna Herwitz for \$500?”



They can confirm or deny with a single tap.

Behind the scenes, implementing **Financial-grade API (FAPI)** protocols helps secure communication channels and protect sensitive data end-to-end. These hardened standards, designed for the financial industry, prevent tampering or interception throughout the user journey.

By adopting financial-grade identity for sensitive interactions, organizations can reduce fraud and deliver the transparency, control, and confidence users expect. Modern CIAM puts this power in their hands.

Before Login

At Login

After Login

How Auth0 helps secure CIAM

The world's most innovative companies, from AI start-ups to Fortune 500s, trust Auth0 to deliver convenient, trustworthy experiences to their customers. Designed for both simplicity and scalability, Auth0 enables a modern, developer-first approach to customer identity that empowers your teams to leverage the full power of identity across every aspect of the customer journey. The result? **Better customer outcomes**, stronger security, and a streamlined path towards growth.

Auth0 Platform brings this to life

Secure experience

Before login Unknown customer

Bot Detection

Breached Password Detection

SCIM

At login Known customer

Passwordless

Universal Login

Adaptive MFA

Social Login

Progressive Profiling

Organizations

After login Repeat, trusted customer

Fine-Grained
AuthorizationHighly Regulated
IdentityContinuous Session
Protection

Secure APIs

Universal Logout

Orchestration and Extensibility

Developer Tooling

APIs

SDKs

Quickstarts

Custom Authentication Flows

Forms and Actions

Security Operations

Security Center

Log Streaming

Event Streaming

Ecosystem



Data Platforms

CDPs and CRMs

Analytics Tools



Applications and APIs

Cloud Apps

Public and Private APIs



Devices

Web and Mobile

IoT



Identities

Human

AI Agents

10B+ Monthly Authentications. 99.99% Uptime. <90 Days to Average Go-Live.



Interested in learning more about how modern CIAM secures and streamlines customer journeys before, at, and after login?

Connect with our team and take Auth0 for a test drive. Also, check out our latest Auth0 Customer Identity Trends Report for insights on customer expectations surrounding convenience, security, and privacy — and how to meet them.

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

About Auth0

Auth0® takes a modern approach to identity and enables organizations to provide secure access to any application, for any user. Auth0 is a highly customizable product that is as simple as development teams want, and as flexible as they need. Safeguarding billions of login transactions each month, Auth0 delivers convenience, privacy, and security so customers can focus on innovation. Auth0 is a part of Okta, Inc., The World's Identity Company™.