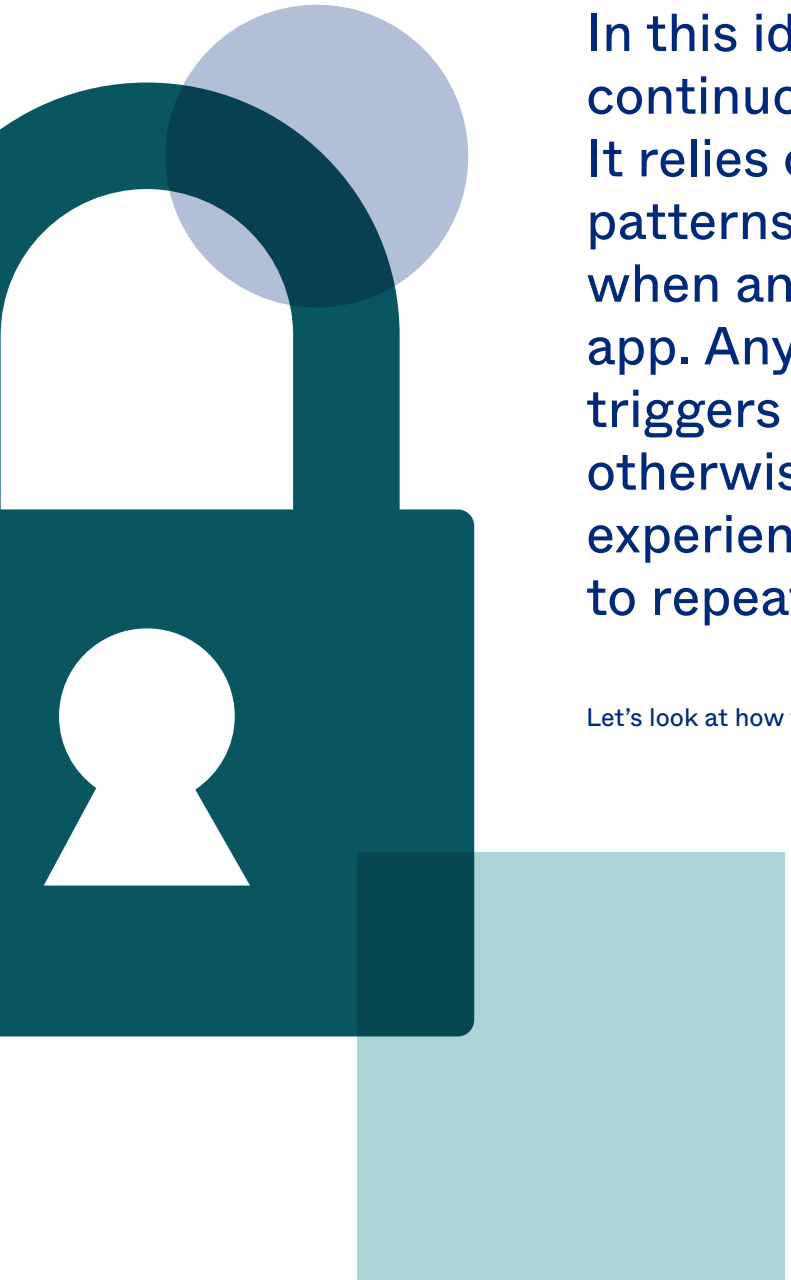
Build trust, not barriers: that's the loginless future

Okta, Inc.
100 First Street, 6th Floor
San Francisco, CA 94105
info@okta.com
1-888-722-7871

okta

The future is frictionless

The world is moving towards a loginless future. Perhaps as soon as the end of this decade, the traditional login box will be replaced by convenient authentication methods that deliver frictionless access to trusted users, without sacrificing security or privacy.



In this ideal, authentication is continuous, contextual and intelligent. It relies on monitoring customers' patterns of behavior, such as where, when and how they interact with your app. Any change to their usual behavior triggers a security response—otherwise, they can enter the experience freely, with no need to repeatedly sign in.

Let's look at how this could transform tomorrow's customer experience.

Robin wakes up and, after a quick check of messages on her phone, hits the treadmill for a workout. The machine knows it's her: it can tell by her weight, her fingertip pressure on the touch screen, and the fact Robin usually uses the treadmill at this time of day. It automatically loads her profile and starts her preferred training program.

Thirty minutes later, Robin steps into the shower. She likes it cool, but her partner likes it hot; thanks to the intelligent sensor, it recognizes Robin and automatically adjusts the temperature to 22C.

Robin leaves the house and gets in the car: the music, navigation system and contacts are all tailored to her history and tastes. She stops for gas on the way to the office and pays cashless from the car. It's simple, as the vehicle is connected to a payment system that uses biometric authentication.

Arriving at work, Robin opens her laptop. The integrated camera authenticates her, giving her instant access to all her professional and personal apps without any further need for verification. The only app that stops Robin to re-verify is the doctor's virtual booking assistant, which asks a few questions before allowing her to proceed.

While Robin's getting on with work, an attacker is trying to access her personal email account from the other side of the world. The system recognizes Robin cannot possibly have travelled thousands of miles since this morning and issues an MFA prompt, stopping the attack from going any further.

This loginless utopia isn't here yet—but many of the technologies that will pave the way there, like passwordless authentication, are available for your organization to implement now.

In this whitepaper, we show how rising customer expectations make preparing for loginless essential and explain six changes you can make now to start your journey.

Customer experience matters

How you treat your customers is as important as what you're offering, and just one bad experience could lose their trust forever: according to PWC, **32% of customers globally have stopped doing business with a company after one poor customer experience**. Speed and convenience are the most important elements of a positive experience, cited by **80% of US consumers**.

Fast, fluid user journeys are a business imperative and it's driving innovation among companies as they strive to minimize friction for their customers. For instance:

- Amazon Go, which allows customers to shop in its cashierless stores without queueing to pay
- Disney's MagicBand wristbands, which act as room keys, tickets, and money all in one at the company's resorts
- Starbucks, whose new pickup-only stores allow customers to order their drinks ahead from the app, then come to store to collect them
- Belgian bank KBC, which allows customers to link their car numberplate to their account, so payment is automatically taken when they use Q-Park car parks

Friction starts at the login box

Your login box is your digital front door. It's one of the most important parts of your digital experience, and it's critical to get it right.

Current authentication methods—the standard username and password combination—often create frustration for customers, as we'll see later in this report. But concerns about privacy and security can also stop customers from completing their journey.

Here are four barriers that may be stopping your customers from converting.

Barrier 1 – logging in

Customers are fed up with passwords, according to Okta + Auth0's latest research, **Expectation vs Reality at the Log Inn**. Top frustrations with the sign-up process are: filling in long login or sign-up forms (48%), creating a password that meets certain requirements, for example number of digits or symbols (47%), entering private information such as passport or tax numbers (46%), and creating a password for every new online service (43%).

This frustration is bad for business: 83% of consumers have abandoned their cart or sign-up due to an arduous login process. Many businesses themselves realize the problem, even if they're unwilling or unable to do much about it. Over half (54%) of businesses attribute abandonments to the sign-up process for new customers.

Barrier 2 – desire for security

While customers want a fast-flowing login experience, they also expect their personal data to be protected at all times.

Barely a week goes by without a high-profile data breach hitting the headlines. This can have a damaging impact on a company's revenue and reputation, with a PWC study finding **87% of customers would take their business to a competitor if they didn't trust a company to handle their data responsibly**. Expectations for security and privacy have never been higher, but for customers the onus is firmly on organizations to protect their data even if their own password hygiene is relaxed: **86% admit to reusing passwords**, but **92% expect businesses to keep their personal information safe**.

Additional layers of security are also reassuring. **Nearly half (49%) of consumers are more likely to sign up to an app or online service if they can use multi-factor authentication**, followed by **48% for Single Sign-On**.

Barrier 3 – concerns about privacy

Allied to these security concerns is the growing awareness of how companies are using our information, with **40% of users concerned about their data being sold to third parties and used without their consent**. These fears have driven up usage of ad blockers, with **37% of internet users aged 16-64 now using ad blocking tools for at least some of their online activities**, and privacy search engines such as DuckDuckGo, which saw its **average daily search volume increase by 73% in 2020**, although this growth slowed in 2021. Customers are more aware than ever of the value of their data and distrustful of organizations who seem to be asking for unnecessary amounts of it.

At the same time, compliance requirements are increasing around the world, due to data privacy legislation such as the EU and UK General Data Protection Regulations (GDPR), California Consumer Privacy Act (CCPA), and Payment Service Directive 2 (PSD2) regulations.

Correctly requesting, storing, and managing personal data is critical to build customer trust and adhere to the latest regulations.

Barrier 4 – inaccessible authentication

Friction that is an inconvenience for some can be a total blocker for others. For instance, inputting passwords can be a challenge for people with cognitive disabilities, dyslexia, memory issues, and perception-processing disabilities.

A more accessible alternative is Web Authentication (WebAuthn), which allows people to authenticate with their devices, without needing to enter a username or password. It identifies a user's device and allows a range of authentication options, such as facial or fingerprint scanning, or entering a PIN number. These alternative authentication methods are not only more inclusive, they're more secure, and create a better user experience to drive your business.

Loginless: building trust, not barriers

The future of authentication is barrier-free and loginless. In this ideal, authentication is continuous and contextual. It relies on monitoring signals such as your user's location, device, apps, consumption patterns, time of day, or input behavior, checking dynamically to see if trust is sufficiently high to allow the user unchallenged access to a particular resource. Any change in their pattern of behavior triggers a proportionate security response.

This continuous authentication is powerful, as it enhances both security and the user experience. Because it doesn't rely on usernames and passwords, there are no credentials for cybercriminals to target. It transcends the simplistic notion that people can be identified by their passwords and utilizes something far more human and intelligent: trust.

In the loginless future, people will be able to prove who they are simply by being who they are. Trusted relationships will be formed online and will progress in the same way they do in real life—over time.

6 changes to make now

Here are six changes you can make now to start removing friction from your customers' experience and get ready for the loginless future.

1. Understand your identity gaps

How do you currently authenticate identity and authorize access for your customers? How much friction does your identity solution add to your customer experience? How well does it protect their data? Understand where the deficiencies are in your identity architecture that are creating frustration for your customers, so you can take the first step to removing those barriers. Your identity audit should encompass the entire authentication flow, scrutinizing all points of friction, security controls, and where and how customer identities are stored.

Identity is a make-or-break element of your customer experience and as such, impacts stakeholders across the business. Now is the time to get everyone together—product management, security, developers, marketing—to make their voices heard as you plan your identity strategy.

2. Go passwordless

Passwords have been synonymous with user identification since the 1960s, but are neither the best nor safest authentication option: the 2021 Verizon Data Breach Report found passwords were responsible for **89% of web application breaches, either through stolen credentials or brute force attacks**.

However, new streamlined login options are now gaining popularity. Passwordless authentication solutions are not just liked for their convenience, but trusted for their security. In fact, the **top three preferred methods of authentication globally are now physical biometrics, pin codes sent to mobile devices, and behavioral analytics**.

Passwordless technologies such as biometrics, email magic links and one-time codes help to streamline the login flow and win trust among your customers. They eliminate security vulnerabilities based on password reuse and deliver a more frictionless user experience that drives conversion. Passwordless could be one of several authentication options you offer to your customers.

3. Build trust into your UX

Many of us would be put on guard if someone we'd just met asked us lots of personal questions. Your digital experience is no different. Asking for copious details to create an account is not only irritating, it raises suspicions: what are they doing with all this data? In a survey of consumer trust, **35% of customers said that being asked for too much personal information was their top reason to distrust a brand**. There may be legitimate reasons for asking for the data, but if your customer is unaware of them, their trust is lost from the very beginning of your interaction.

Far better is to gather data incrementally from your users through progressive profiling. Rather than overwhelming people upfront, customers are asked only for minimal information at the first interaction. More data is gathered as your relationship builds, and the customer engages with your brand, perhaps in exchange for a discount or loyalty program membership. You get the valuable context you need to unlock insights about your customer, but only when they're ready to give it. In return, they also get something of value.

4. Use intelligent security controls

Your identity solution doesn't need to treat every customer like a potential hacker. Heavy security controls could deter returning customers if they have to interact with them every time they visit your UX.

Instead, technology can be used to differentiate genuine customers from bad actors. For instance, adaptive MFA factors in trust scores and applies security only when appropriate. It relies on changes in patterns of behavior—such as a login attempt from a new device or location—to trigger additional security measures, based on risk.

Bot detection can mitigate scripted attacks by detecting when a request is likely to be from a bot. If an attack is detected, an extra security step—such as a CAPTCHA request—is displayed. The triggers are designed only to happen for bad actors, based on data and statistical models, and genuine users pass through with minimal friction.

5. Automate consent management

Data privacy legislation is constantly changing, creating a challenge for IT and security teams in staying compliant. Customer consents must be correctly requested, stored, offered to customers for periodic review, and updated when necessary to ensure users' privacy is respected.

A CIAM solution allows you to automate the consent management process, making compliance seamless. It creates a single source of truth that links data to identity across your systems, providing you with the visibility and record keeping you need to address your compliance requirements, and alleviating users' concerns around their information being misused.

6. Design in accessibility

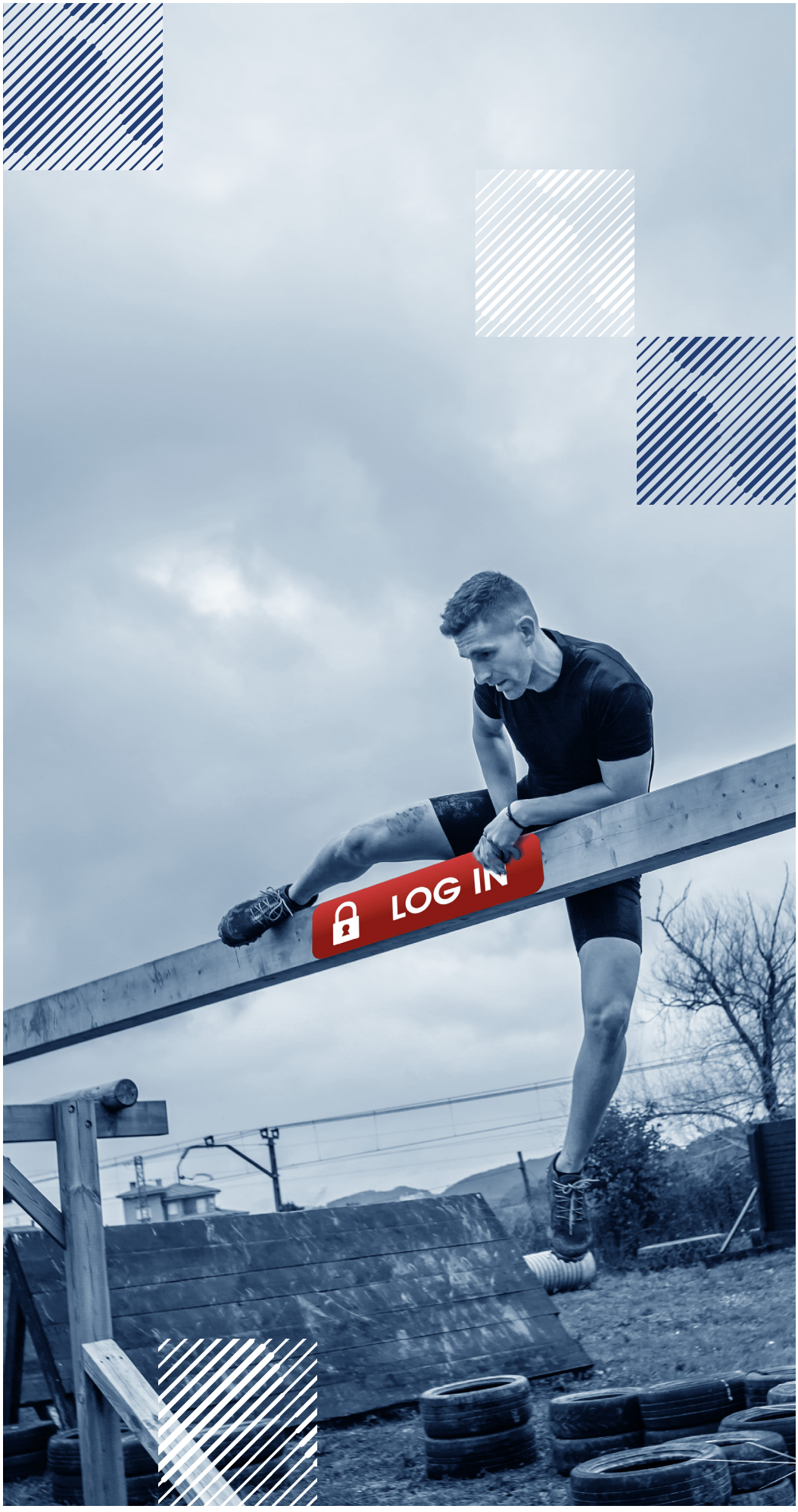
A login experience can't be barrier-free until it's inclusive for all users. The World Wide Web Consortium (W3C) has produced new proposals for designing accessible authentication flows, with a range of considerations to keep in mind. One option is supporting WebAuthn, so users can authenticate with devices instead of passwords. Another is Open Authorization (OAuth), which allows login with third-party providers such as Google or Apple, offering an alternate option to password. Organizations can also enable multiple options for the second factor in MFA, for example by simply pressing a button to enter a time-based token.

Start your journey to loginless with Okta + Auth0

At Okta + Auth0, we're helping companies move towards the seamless, loginless ideal, one step at a time. This approach makes the transition more manageable, helping businesses to gradually win the trust and buy-in of customers and stakeholders across the organization.

With Okta + Auth0's CIAM solutions, you can remove barriers from your UX with benefits for your customers and your bottom line.

To start your journey, **reach out to our team** today.



okta