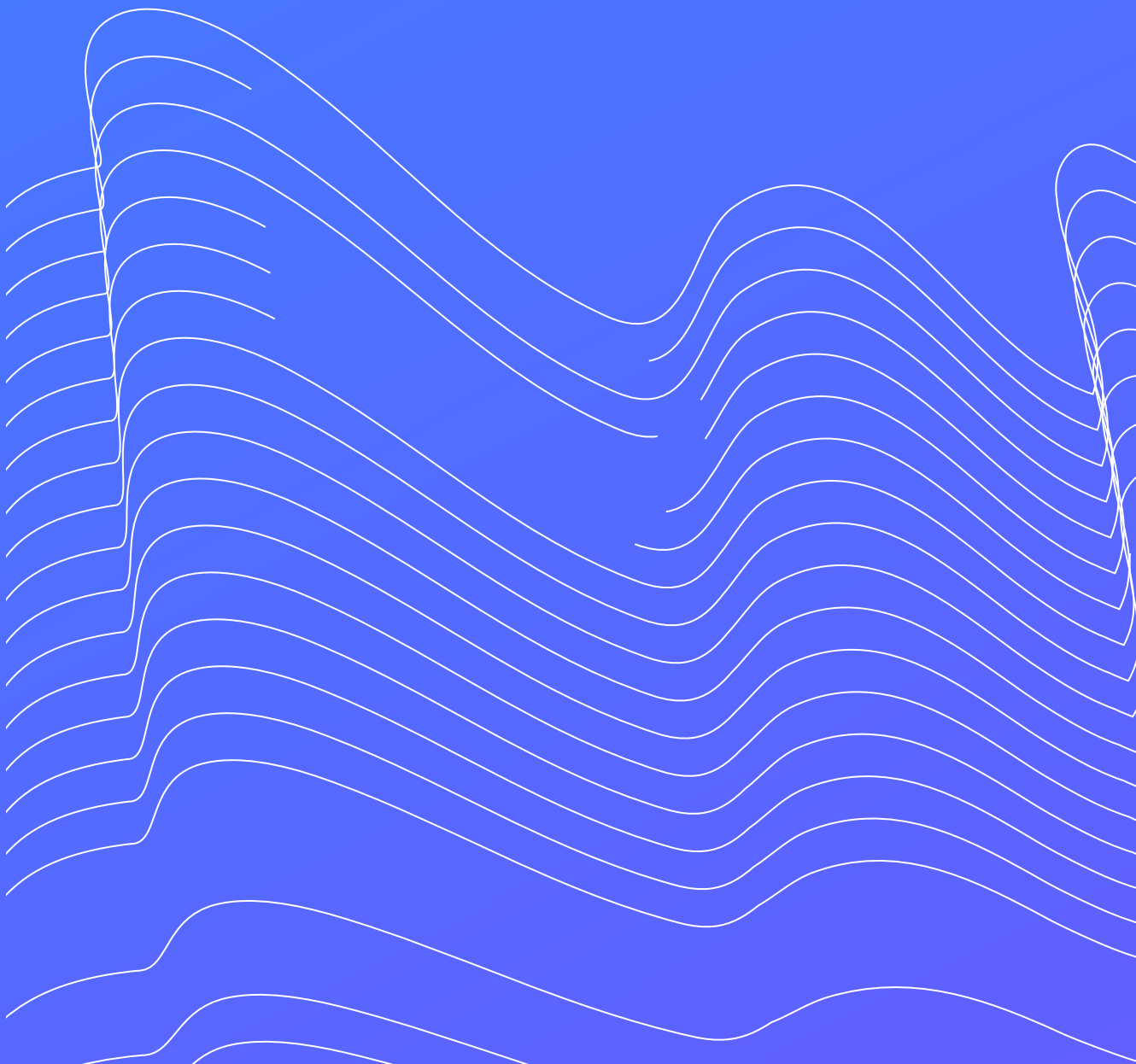
auth0

Authentication After Passwords

Maximizing conversions (and enhancing security) in the age of convenience



EBOOK

auth0.com

Contents

Contents

Contents

Introduction

Identity exists at the intersection of:

- **Convenience:** Conscious selection and subconscious preference both favor convenient experiences, and every new experience is compared against the most convenient one.
- **Security:** Businesses can be ruined, or at a minimum suffer severe brand and valuation damage from a single breach, so ensuring that the applications they build meet the highest levels of security is critical.
- **Privacy:** From both a financial and brand reputation perspective, businesses need to be sure that they meet the ever-changing and demanding requirements of privacy and compliance.

From improving customer experience through seamless single sign-on (SSO) to making multi-factor authentication (MFA) quick and easy, your login box must find the right balance between user convenience, security, and privacy.

In fact, we believe that the companies that will succeed in the next five years will be the ones best-equipped to meet the ever-growing consumer expectations for these three attributes.

But what will that future look like, and by what path can today's companies become tomorrow's leaders?

In this ebook, we'll answer those questions and more.

Misconception #1: It's impossible to simultaneously satisfy convenience, security, and privacy

For the designers, developers, and IT professionals who build digital experiences, there's a constant tension between securing information and protecting private data while also making things convenient for users.

Historically, companies have been forced to prioritize and compromise between these priorities—but in our view, this tension only exists because of the way infrastructure and systems have historically been designed.

As we will see, innovative solutions can satisfy all three areas simultaneously.

The Future of Identity

In the near future—perhaps even this decade—traditional login will become extinct. Replacing today's ubiquitous login boxes, with their user ID and password fields, will be user-centric systems that favor convenience (without sacrificing security or privacy) and that are built on trust.

The world is moving toward a loginless future

Today's authentication systems are unintelligent; as a result, they treat legitimate users and attackers the same way.

Tomorrow will be different: the burden of proof will shift from the user to the business. In this loginless paradigm, users establish trust in the lowest-friction manner possible; once established, more contextual signals and intelligence are used to maintain and increase trust, rather than requiring the user to repeatedly sign in.

How might this loginless future manifest?

Alex wakes up to the alarm from their smartphone; after briefly reviewing their personalized news feed and checking how the international markets are performing, they head into the spare room for a morning workout.

The smart cardio equipment recognizes Alex from a range of factors—the time of day, the pressure on the touchscreen, their weight—and automatically loads the correct user account.

After a quick HIT program (Alex's preferred morning pick-me-up), Alex heads to the bathroom and steps into the shower. Like the fitness equipment, the shower's intelligent system recognizes the occupant and delivers a comfortable experience.

Ready for the day, Alex opens a laptop. The integrated camera and biometrics authenticates Alex in an instant, without any intervention; while Alex isn't consciously aware, this same biometric identity is the reason why accessing online applications—both professional resources and personal services—is so seamless. The one exception was an online doctor's appointment that required Alex to verbally answer a few questions posed by a virtual assistant before being authorized to meet with the physician.

Meanwhile, on the other side of the world, an attacker is trying to access Alex's online trading account. Behind the scenes, the system recognizes that not enough time has passed to enable the change in location from when Alex checked the markets this morning to now. Detecting an "impossible travel" scenario, the system presents the attacker with an MFA challenge—and the attack is stopped.

Key to the secure and convenient operation of such a system is a foundation of trust.

Trust forms the foundation

The future of the Internet will be based on trusted digital relationships, with trust flowing in two directions:

- The trust a user places in a business.
- The intelligent trust a business bestows upon a user.

We'll return to the first point later, but for now let's examine the second.

While it's true that loginless is built upon a foundation of trust, it's important to understand that the trust is not blind; rather, tomorrow's customer identity and access management (CIAM) systems will employ a number of technologies and approaches to deliver a secure, convenient experience. At the core, such systems need to consider, with every user interaction:

- What functions, data, resources, etc. a user is trying to access or use.
- The trustworthiness of the user at that time.

By continuously monitoring signals (e.g., the user's location, device, apps, consumption patterns, time of day, input behavior, etc.), the authentication system simply checks, whenever needed, to see if the trust is sufficiently high to allow the user unchallenged access to a particular resource.

This "continuous authentication" is extraordinarily powerful, as it enhances both security and the user experience—and the trust that it delivers extends far beyond anything a password by itself can provide.[1]

Now that we've seen a glimpse of the future's *what*, let's look at the why.

1. Continuous authentication can be viewed as an intrinsic element of the strategic approach Gartner refers to as Continuous Adaptive Risk and Trust Assessment (CARTA).

   Gartner ®, "Secure Application Access by Applying the Imperatives of CARTA to Access Management", Michael Kelley, Abhyuday Data, Henrique Teixeira, Refreshed 12 August 2021, Published 25 February 2020. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Misconception #2: Loginless is insecure

Without knowing the details of how such systems are implemented, it's almost natural to look at the term "loginless" and conclude that this approach sacrifices security for convenience. However, loginless systems don't sacrifice security for convenience—methods with lower friction can still be safe against the most common attack vectors.

The Frictionless Imperative

In the physical world, friction is the force that resists the relative motion of solid surfaces, fluid layers, and material elements sliding against each other.

In a consumer business, **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
- recovering lost account information
- checking out a purchase

While *some amount* of friction during these interactions is necessary both to establish trust and to provide security controls that protect a user's sensitive information and combat fraud, the more friction involved (e.g., more steps, more information required, etc.), the greater the user's frustration—and the more likely they are to abandon the experience.

Friction is revenue's natural enemy (that's the tweet)

For consumer businesses, friction is a major obstacle to conversions and, by extension, to revenue. The more friction there is—in any and every consumer interaction—the lower your conversion rates and the less revenue you get over both the short and long term:

- Does your account creation process ask for too much information or require too many steps to complete? You get fewer customers signing up.
- Is signing in too inconvenient? Fewer customers will use your service.[2]
- Is resetting the password too cumbersome? In the short term, customers who encounter this issue during checkout may abandon their purchases;[3] over the long term, difficult password reset flows may cause customers to stop using your service altogether.
- Is checkout too complicated? Items will sit in the cart, unpurchased—possibly forever.

Too few businesses understand this fundamental truth, so it's worth repeating: **for consumer businesses, the more friction there is, the lower your conversion and revenue.**

Lowering friction provides a competitive advantage

Another way lowering friction contributes to healthier outcomes, meaning higher conversion and revenues, is by providing a competitive advantage over less user-friendly alternatives.

2. FICO's 2020 **Digital Banking Study** [FICO] revealed that 28% of Americans reported abandoning an online purchase because they forgot login information.

3. A study conducted jointly by MasterCard and the University of Oxford (**Mobile Biometrics in Financial Services: A Five Factor Framework**) [University of Oxford] reported that, "About a third of online purchases are abandoned at checkout because consumers cannot remember their passwords."

Many service industries and e-commerce sites already understand this reality and have introduced convenience as a key differentiator.

While the digital world has features like one-click purchasing and “same order as last time,” the physical world has plenty of its own examples.

For instance, a hotel’s mobile app was rarely anything more than a way to manage bookings and reward points—until Marriott and Hilton used the app to transform a phone into both the check-in desk and room key. Business travelers—a lucrative segment in the hospitality industry—embraced the ability to fly by the check-in lines and appreciated that they no longer have to deal with the annoyance that follows losing a room key.

Or consider National Car Rental’s emphasis on the “Choose any car in the aisle and go” convenience available to Emerald Club members.

Delivering a uniquely great experience can elevate your brand above all others, while raising customer expectations in the market as a whole and forcing the competition to play catchup.

And until they do? More customers—and higher conversions—for you.

Friction impedes accessibility

While friction is an inconvenience for many users, for others it can present significant impediments that prevent them from accessing your services.

Unfortunately, accessibility (when it’s even considered at all) is often prioritized far below other factors, resulting in designs that look slick—but that some consumers struggle to use. The COVID-19 pandemic highlighted many of these usability deficiencies, as it forced far more interactions to go online.

Consider disabilities like vision or cognitive impairment, or limited motor function, and imagine trying to navigate a cumbersome authentication flow that requires the user to remember and then enter a long, complex password.

Or give thought to how a user uncomfortable or unfamiliar with technology would respond to a message asking them to download an app and configure push notifications.

When designers and developers—who themselves are tech-savvy—design experiences, there can be a tendency to disproportionately focus on similarly leading-edge users ("What, doesn't everyone use a password manager these days?!"[4]), but care must be taken to ensure others aren't left behind.

Not only is there a moral obligation to consider accessibility during the design and development process, there is also a considerable financial incentive—by building applications that can be used by everyone, you maximize your market reach.

Identity Flows are Fundamental Elements of the Customer Journey

Once you recognize the dangers of friction and how it manifests, it becomes clear that:

- For online consumer businesses, identity flows (shown in blue in Figure 1) are fundamental parts of the customer journey.
- Friction can mean the difference between making or missing your conversion (and revenue) goals.

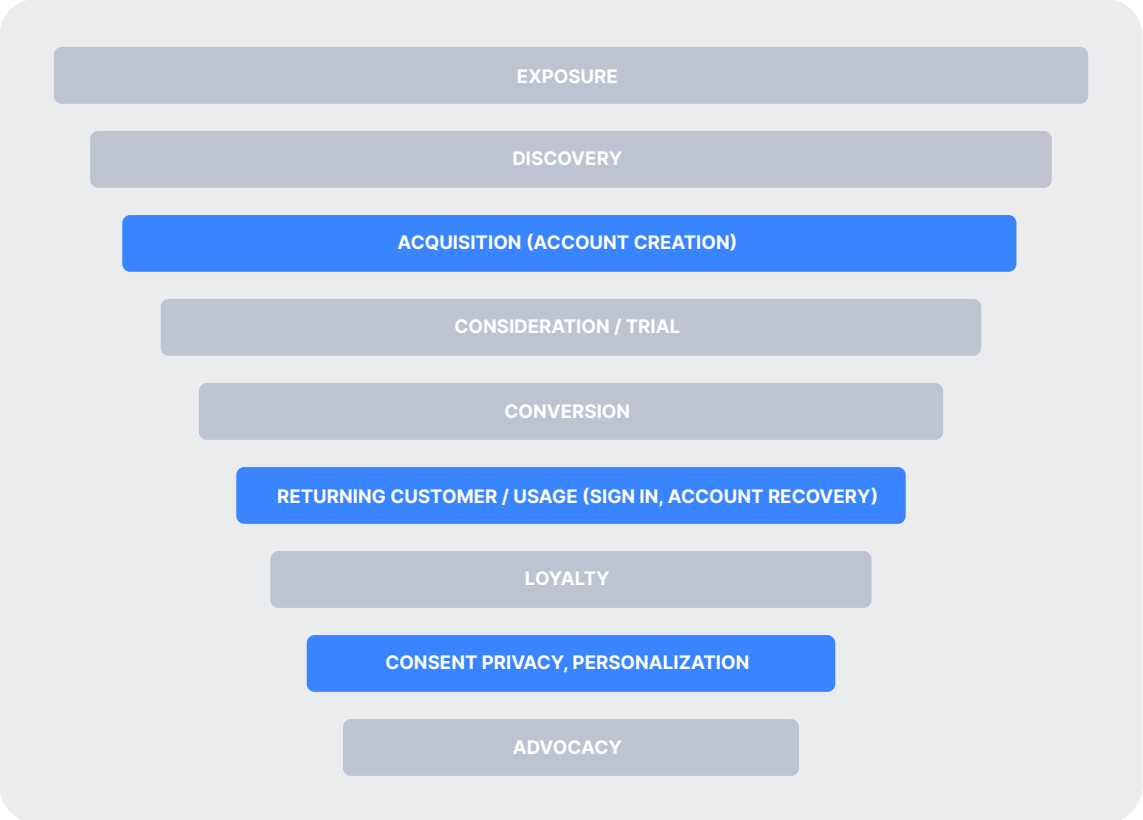
4. The same FICO study cited earlier found that fewer than 23% of Americans use a password manager.

Viewed through this new lens, the cost of friction within identity flows becomes much clearer. For example, an abandoned account creation might equate to $1,000 in missed lifetime revenue, and every failed login might cost $100 in lost sales.

Plug in your own numbers and multiply by your customer base, and you'll start to approximate the cost of friction to your business.

So now that the impact of friction is becoming clear, how can you minimize it?

Figure 1: Identity flows are fundamental elements of the customer journey and strongly influence conversion rates



Misconception #3: Friction is a technical issue, not a business imperative

If more companies understood the connection between identity management and real business outcomes, the alarm bells would be ringing: if you fail to deliver a low-friction experience, then you are literally missing out on customers and revenue.

Unfortunately, too many companies view friction within identity flows as technical issues.

How do we know? Because most of our conversations with companies involve identity and security personnel; it's comparatively rare for finance, product management, product marketing, customer experience, or other customer-oriented roles to be involved—and when they are, it's a clear signal that the company understands what's truly at stake.

First Things First: Passwordless Authentication

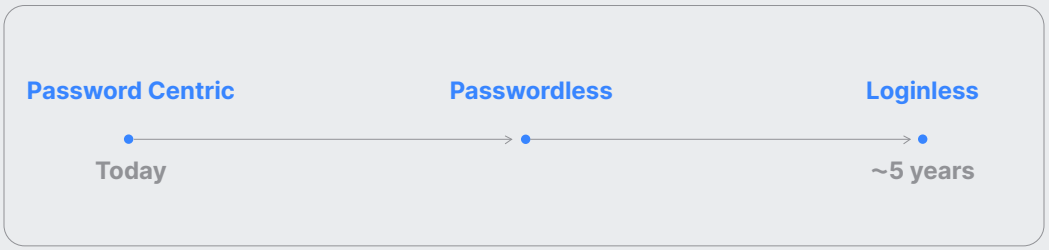
It's no secret that passwords are a comparatively poor solution to the problem of authenticating a user. Among other deficiencies, they're cumbersome for users to create and remember (one reason why password reuse is so common) and they're vulnerable to a range of cyberattacks.[5]

Fortunately, there are stronger alternatives.

Passwordless authentication (often just shortened to "passwordless") refers to any mechanism—and there are several, as we'll see—that authenticates a user without requiring them to enter their password.

5. Our own **State of Secure Identity** report examines the latest threats, including credential stuffing, injection attacks, fake account creation, MFA bypass attacks, as well as the defensive measures available to combat these attacks.

Figure 2: The three authentication paradigms—passwordless is the intermediate step on the way to loginless



However, while most of us wouldn't miss passwords, the word "passwordless" is a bit of a misnomer because passwords will continue to exist—at least for the foreseeable future—even when passwordless authentication has widespread adoption.

The major difference is that, in the passwordless paradigm, other authentication methods will take precedence—with passwords likely serving as the factor of last resort.[6]

So if eliminating passwords isn't the driver behind going passwordless, then what is?

As you may have already guessed, it comes down to reducing friction.

Misconception #4: You don't already have a passwordless flow

Would you believe us if we told you that, today, almost every online company already has a passwordless flow? Well, it's true!

But this misconception arises because the existing flow isn't called "passwordless"—instead, it's called "reset password."

Think about it: in the typical account recovery flow the user clicks on a "reset password" button, which triggers an email that includes a "reset password" link. The user clicks on this link and arrives at a page that asks them to enter a new password. After doing so, they're logged into their account—all without entering the original password.

6. Perhaps "passwordlast" would be more accurate, but we don't see that term catching on.

Passwordless can minimize friction while enhancing security

While different organizations use identity and access management (IAM) systems for similar purposes, their exact needs vary. **Technologies that are effective in consumer applications must balance security and usability,** and one way to assess the quality of user experience is by examining two measurements:

- The **passing rate** of an authentication challenge: the higher the passing rates, the better the user experience.
- The **time to complete** an authentication challenge: the shorter the time to complete, the better the user experience.

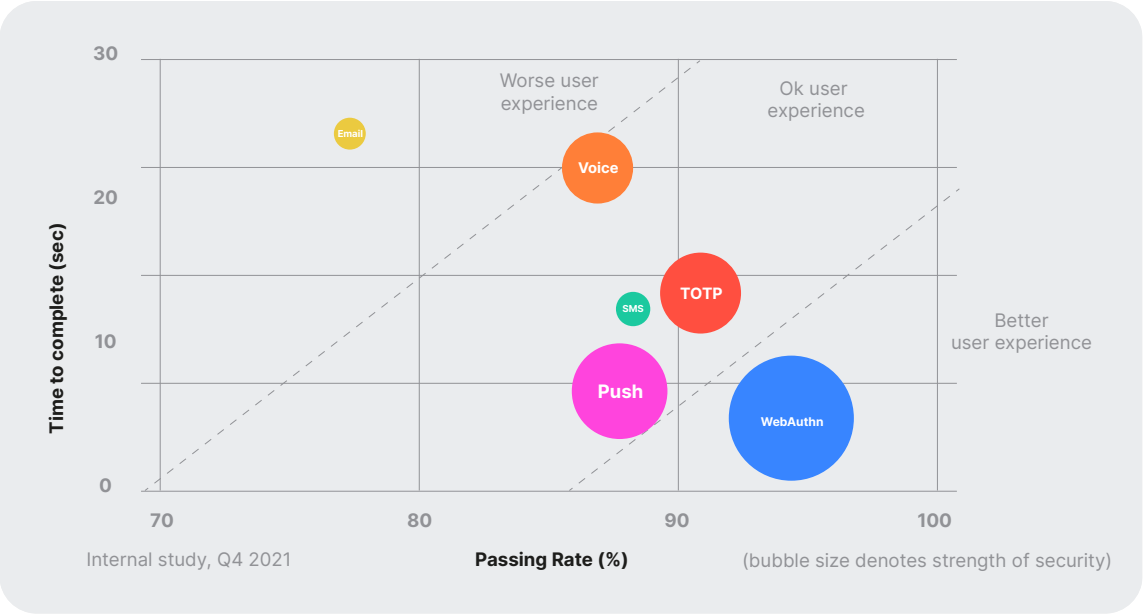
Combining these two measures and comparing across passwordless authentication challenges shows that the user experience varies significantly. Visually examining Figure 3 reveals that:

- Voice and email authentication provide a poor user experience: passing rates are low (82% and 84%, respectively) and the time to pass is high—around 25 seconds on average for each.
- Push via a proprietary application (Push), pushing a one-time password (OTP), and using SMS as an multi-factor authentication channel deliver a middle-of-the-pack experience, with passing rates from 87-90% and an average time of around 10 seconds.
- Using a proprietary application to send an OTP (MFA-OTP) and leveraging device biometrics (WebAuthn) deliver the best user experience—both exhibit high passing rates and low time to complete the challenge.

Interestingly—and importantly—we can also see a high degree of correlation between those authentication challenges that deliver a convenient user experience and those that provide the best security.

In fact, **biometrics like WebAuthn are a great example of how IAM systems can simultaneously deliver a convenient, private, and secure experience.**

Figure 3: Internal Auth0 data shows that passwordless authentication challenges minimize friction and enhance security



The Loginless Roadmap

It may seem like an enormous undertaking to get from today's password-centric paradigm to the intermediate step of the passwordless paradigm, but the journey becomes much more manageable if you break it down into smaller initiatives.

Plus, there are many reasons why you should start right away—from the immediate conversion gains, to the relative ease of incremental change now (as compared against massive upheaval in the future), to the reality that the trust which is so essential to the transition needs to be built up over time, to the fact that different users will move at their own pace.

Misconception #5: We can't make meaningful progress today (so we'll wait)

There's a fairly common perception—even among those who recognize the inevitability of a loginless future—that there isn't much that can be done today to move in that direction. This misconception leads to missed opportunities and magical thinking, as organizations wait for some perfect solution to appear before moving forward with the necessary intermediate steps.

But the truth is that you can get started today on your journey to loginless—by embracing passwordless authentication.

Elevate your mindset about identity flows and authentication

The first and most critical step is to change your mindset about identity flows. Stop regarding them as some behind-the-scenes technical component and start seeing them for what they are: make-or-break elements of your customer journey.

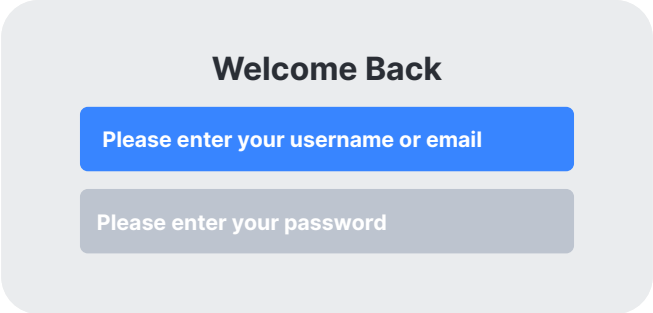
Changing your mindset should lead to carefully considering many voices in any discussion about identity flows, going beyond the developers and security engineers to also include product management, customer success, marketing, user experience (including accessibility), and revenue owners. Collectively, the group should be able to discuss convenience, security, and privacy, as they relate to authentication.

Don't default to passwords

While the login box didn't become a familiar sight until GUIs emerged, logging in with a user ID and password was established with the time sharing systems of the 1960s and, later, the Bulletin Board Systems (BBS) in the 1970s.

Since then, the user ID and password combination has been synonymous with authentication, and passwords have remained the default challenge embedded in login screens.

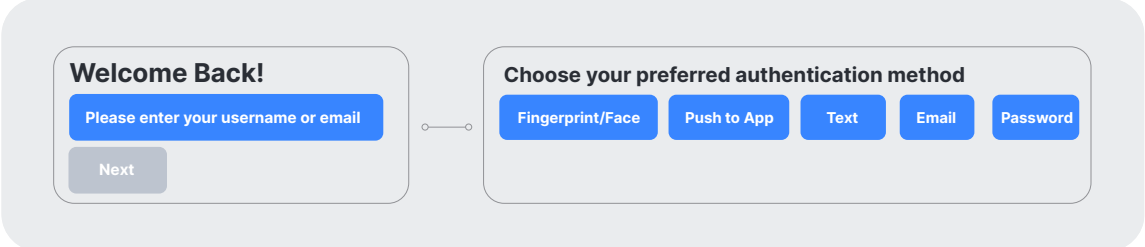
Figure 4: The password-centric login experience typically prompts for the username and password by default



Admittedly, for a while there weren't better alternatives, but this is no longer the case: a password is simply one way to 'prove' an identity—and not nearly the best one.

The first step in going passwordless is to avoid defaulting to the password as the identity challenge. In this new paradigm, the login flow starts by asking the user for an identifier (e.g., user ID, email address, etc.); then, when it comes time to challenge, it treats passwords as just one of many available options—including biometrics, OTPs, magic links, etc.—most of which offer stronger security and more convenience.

Figure 5: The passwordless paradigm decouples the login flow and allows the user to choose their preferred authentication method



Setting aside the artificial complication that many authentication flows have been 'hardwired' around passwords, there is nothing stopping you from adopting this identifier-first paradigm; in fact, many familiar Internet giants have already begun to implement this approach, as they long ago recognized the value of going passwordless.[7]

Start earning trust

Companies are already realizing that their success depends upon consumer trust and that this trust must be earned.

Additionally, as is the case with relationships in real life, trust in the digital world is earned over time—through safe, convenient, respectful, and delightful interactions—and consumers get to choose what information they share, with what companies.

The burden of earning that trust now falls upon companies; those that succeed will reap considerable rewards, while those that fail to establish trust—or, worse, that violate it—will suffer consequences.

Two proven ways to earn trust are to show value before you ask for something from the user and to only ask for the minimum information you need. These approaches manifest in a few forms, including:

- **Anonymous checkout** (also referred to as guest checkout), in which a user can use a service without creating an account; billing and delivery information is collected to facilitate the transaction, but is not stored within an account.
- **Progressive profiling**, which gradually asks the user for information (and introduces them to new authentication options) as they experience more value from the service—while allowing them to get started very quickly.[8]

7. The WSO2 Open Banking Documentation site includes a resource page for **Identifier-first Authentication.**
8. Learn more about progressive profiling in **Progressive Profiling: Vital Info from Happy Customers.**

Misconception #6: Personal information is worth more than trust

Marketers, especially, are addicted to user information; after all, it helps power the retargeting and personalization so important to many services. Consequently, giving the user more control over what information they share is a scary proposition!

However, this thinking is rooted in the short term; long-term thinking recognizes that trust is essential to loyal—and yes, highly profitable—relationships. Plus, there are very real short-term benefits to trusting your customers: for example, reducing the number of fields required during registration can dramatically increase conversions.[9]

Plus, there's another reason to overcome the discomfort and start giving consumers more control: the big players are already doing it. Companies like Apple and Facebook,[10] as well as financial institutions like Fidelity Investments[11], recognize the growing importance of trust—whether to create a competitive advantage or to address a perceived deficiency—and not only do they see the trust-centric future, but they're working to make it happen as quickly as possible.

Start trusting

While you may find it uncomfortable to build more trust into your customer interactions, it's important to note that trust exists on a spectrum—it's not a binary thing where you do or do not trust a user absolutely—and it is a function of confidence and risk. In fact, it's already possible to consider many factors and calculate a "trust score" or "risk profile" that influences authentication flows and the user experience. For example:

- **Adaptive MFA** is a technique that only engages MFA when a user interaction is deemed risky based on behavioral data.[12]

9. In an example shared by Unbounce, cutting the number of fields required from 11 to 4 led directly to a 120% increase in conversion rate; see **How To Optimize Contact Forms For Conversions.**
10. See the Facebook-sponsored video **Consumers Want Control. To Compete, Your Brand Needs to Give It to Them** [Harvard Business Review].
11. See **Financial industry to give consumers more control over their data** [Akoya].
12. Learn more in **Auth0 Launches Adaptive MFA to Increase Security and Reduce Friction for End Users.**

- **Step-up authentication** is a technique that adapts identity requests to the importance of the resource and the risk level if it were to be exposed.[13]

Misconception #7: Passwords are secure; other authentication challenges aren't

The traditional login box, with its username and password combination, has poisoned popular thought about trust by creating:

1. A false sense of security based upon the flawed premise that passwords are secure
2. A perception that anything lacking a password is intrinsically insecure

As a result, companies are understandably wary of going passwordless. Plus, the threat of brand damage and regulatory fines stemming from breaches is enough to give any reasonable security or product leader pause about placing too much trust in users.

In fact, the combination of their vulnerability to a number of attacks (e.g., brute force, password spraying) and poor user habits arguably makes passwords a security liability; moreover, many other options (e.g., MFA, OTP, magic link, push notifications, etc.) offer superior security.

Recognizing the many misconceptions around passwords is essential, because doing so changes your perception of the risks and rewards of trust, nudging you forward.

Introduce—and encourage—biometric authentication

Enabling users to authenticate using their device biometrics has two benefits:

- It greatly reduces friction during the authentication challenge, boosting user retention and revenue.
- It increases security since the flow is not 'phishable' by bad actors.

13. Learn more in **What Is Step-Up Authentication, and When Should You Use It?.**

In the last few years, the FIDO Alliance has been working relentlessly toward the vision of helping users authenticate with maximum security and minimum friction. The resulting WebAuthn standard provides the foundation for that to happen.

WebAuthn is the only standard-based authentication method that makes phishing impossible, as it binds the public/private key to a specific web domain—which makes it impossible for a user to mistakenly authenticate into a phishing website.[14]

By using device biometrics for MFA, WebAuthn makes the security and convenience of WebAuthn-powered flows available to anybody who has a device and browser who can support the biometric challenge.[15]

However, simply offering users WebAuthn-enabled identity flows isn't enough; while tech-savvy users may have been eagerly awaiting the option, the majority of your users likely don't pay particularly close attention to the latest advances in authentication. To drive adoption, you should promote WebAuthn device biometrics for what it is—the easiest and most secure authentication mechanism—and provide resources that show users how to enrol (we promise it will be worth the effort!).

14. See WebAuthn: **Beyond the Password** [W3].
15. Security Keys are another great WebAuthn-enabled way to secure access, but their adoption is mostly limited to tech-savvy users or corporate environments with relatively high-security requirements.

Misconception #8: Biometric authentication introduces privacy concerns

There are two major misconceptions regarding biometrics and privacy:

1. User concerns that their personal biometric data is being handed over to a business.
2. Business concerns about handling (e.g., storing, securing) biometric data.

In reality, the WebAuthn specification forces all biometric data to be contained within (and remain within) the device. Some device manufacturers even go a step further, employing dedicated subsystems that further segregate sensitive data.[16]

The result of such measures is that neither users nor businesses need to worry about privacy concerns when it comes to biometrics.

Prioritize accessibility

As noted earlier, building accessible authentication flows reduces friction and maximizes your market reach. Historically, design processes often considered accessibility only as an afterthought, rather than an intrinsic requirement, but one lasting impact of the COVID-19 pandemic is the heightened understanding of the importance of accessible digital experiences and their dependence upon inclusive design processes. Excerpting from Level Access' 2021 State of Digital Accessibility report:

> *When it comes to being human, we have three simple needs: to earn, to learn, and to belong. If we can support ourselves, grow and develop our talents, and be a part of something bigger, we'll have a good base from which to build a fulfilling life.*

16. For example, Apple's Secure Enclave is isolated from the main processor to provide an extra layer of security and is designed to keep sensitive user data secure even when the Application Processor kernel becomes compromised.

> *Last year, we lost physical access to many of our earning, learning, and belonging opportunities during the pandemic. Technology had to bridge the gap—immediately—whether organizations were ready or not. Paradigms typically take generations to shift, but the shift to virtual work happened over a weekend.*
>
> *Organizations are taking a real and deliberate look at digital access for their employees as well as their end users.*

Fortunately, you aren't on your own when it comes to designing accessible experiences. For instance, the World Wide Web Consortium (W3) hosts a page dedicated to Accessible Authentication.[17] Drawing upon the Web Content Accessibility Guidelines (WCAG),[18] the page provides explanations, links to resources, and examples of accessible design, including:

- Supporting WebAuthn so the user can authenticate with their device instead of username/password.
- Offering the ability to login with a third-party provider using OAuth.
- When two-factor authentication is used, allowing for multiple options for the second factor, including a USB-based method where the user simply presses a button to enter a time-based token.

As some pre-pandemic normality returns, we all have the chance to contribute to a newly accessible world. In the words of Level Access' CEO:

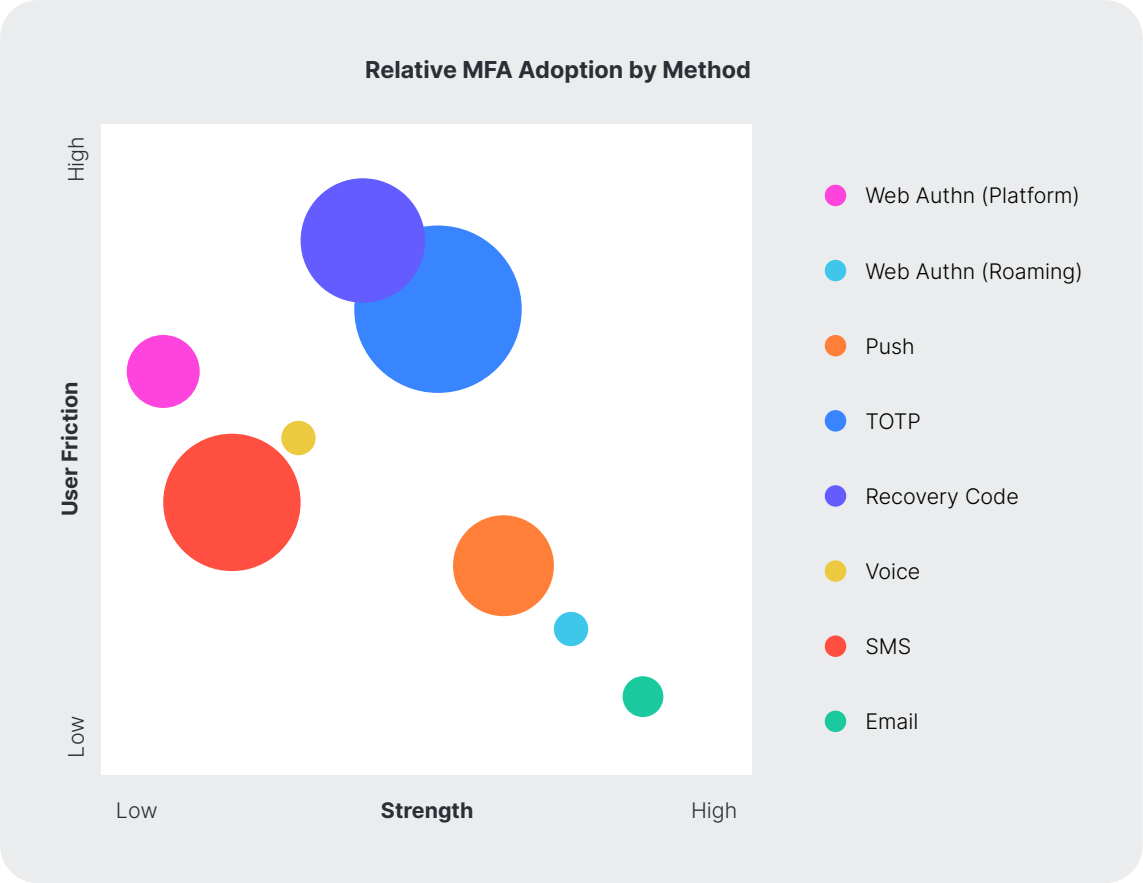
> *Hopefully it's a mix of the best parts of life before 2020 and life now—with technology as an empowering source of earning, learning, and belonging.*

17. See **Understanding Success Criterion 3.3.7: Accessible Authentication** [W3].
18. See **Web Content Accessibility Guidelines (WCAG) 2.2** [GitHub].

Start using progressive enrollment

Today, there are many authentication options available. However, adoption varies enormously (Figure 6).

Figure 6: New MFA methods based on WebAuthn offer a great combination of strength and low user friction, but adoption typically lags what is possible



19

A number of factors influence the relative adoption rates of different authentication methods, including:

19. Learn more about MFA in **The State of Secure Identity.**

- IAM provider offerings.
- Application provider introduction.
- Device support (e.g., WebAuthn).
- User awareness.
- Perceived user benefit.
- User preferences.

As an application provider, delivering the best user experience for the majority of users means not only supporting leading-edge authentication methods, but also the more widely established, older mechanisms.

Of course, it remains in your best interest—and your customers'—to up-level your users to the more-secure and lower-friction options. An effective way to do so is to combine incentives with progressive enrollment.

Similar to progressive profiling, which spreads your requests for information over multiple interactions to build trust, **progressive enrollment is an intelligent way to spread out when you encourage users to enroll in a stronger authentication mechanism.** For example, users relying on voice, SMS, or email can be prompted to enroll in an alternative like push notifications or biometrics. Additionally, users can progressively enroll biometric-capable devices one at a time, as they use them, giving them the flexibility of having multiple passwordless authentication options.

Progressive enrollment can even be combined with device awareness, so that only users with WebAuthn-compatible devices are targeted with an enrollment promotion or only users on the mobile app are asked to enable push notifications.

Misconception #9: Simply offering a particular authentication method means 'job done!'

Simply making a particular method available isn't enough; while tech-savvy users may have been eagerly awaiting the newest option, the majority of your customer base likely isn't paying particularly close attention to the latest advances in authentication.

To drive adoption, you should:

- Make enrolment as easy as possible by asking for a minimum amount of information across only a few steps
- Educate about the benefits of enrolling (e.g., "WebAuthn biometric authentication is the easiest and most secure way to protect your account") and instructions for enrolling
- Promote the option (leverage progressive enrollment) and provide incentives

In combination, these techniques will help move your users to the most convenient and most secure authentication methods.

Summing Up

Traditional authentication is a digital barrier that suffers from many well-known flaws:

- Most login and account creation flows put too much burden and friction on the end user.
- Today's most widely adopted methods are far too easy for attackers to exploit.
- Traditional systems are unintelligent—as a result, they treat legitimate users and attackers the same way.

Because unnecessary friction in account creation and login is now recognized as a major deterrent to customer acquisition, conversion, and brand loyalty, in the coming years traditional authentication systems will be replaced by passwordless and—ultimately—loginless systems that simultaneously deliver convenient user experiences while preserving privacy and enhancing security.

In this loginless future:

- Identification systems will use continuous authentication to allow access when you are you and deny access when "you" are not you.
- Digital experiences will be safe, effortless, and delightful.
- Digital relationships will be formed and will progress in the same way they do in real life—over time.
- Consumers will choose what they share, how they get access, and what companies they trust with their data.
- The burden of establishing a trusted digital relationship will be on the business.
- Trust must always be earned, respected, and protected.

The path to the loginless future goes through passwordless, an IAM paradigm in which a user is authenticated without entering a password.

While biometric authentication using WebAuthn is the shining example of passwordless, it is not alone: other methods also offer more convenience and stronger security than passwords, with fewer device dependencies than leading-edge biometrics.

Misconception #10: It's too hard to go passwordless

Admittedly, this misconception has an element of truth: CIAM is complex, developers are already working hard to maintain and extend existing solutions, and resource constraints may impede your ability to take on grand new initiatives.

However, Auth0 exists because CIAM is so complex. By building identity solutions that are easy for developers to use, we take on that burden. Plus, moving to passwordless isn't an all-or-nothing endeavor; rather, incremental adjustments can be made, right now.

With a disciplined approach and the right IAM partner, there's no reason why you can't become a passwordless leader. Auth0 can help your development team get started and quickly gain some passwordless wins.

What You Can Do Now

While the future is loginless, there is plenty that companies can do in the interim. While preparing for that eventuality, companies can start to take advantage of the building blocks to loginless and be ahead of the game. Here are some things that you can do:

- **Implement Passwordless with WebAuthn Biometric**
  Allows users to authenticate using their device biometrics with minimal friction and increased security.

- **Measure and benchmark conversion funnel metrics**
  Authentication is a key component of conversion metrics and can greatly impact their efficacy. Tracking these metrics before and after implementing Passwordless with WebAuthn Biometrics will help you understand your customers' journey and provide clear opportunities for optimization.

- **Establish usable security practices**
  It is no longer necessary to sacrifice convenience for security. Usable security practices such as Adaptive MFA, Bot Detection, and Step-Up Authentication maintain a strong security posture while minimizing the disruption to users.

- **Start using progressive enrollment**
  The best security is the one that is actually used. Encouraging your users to enroll in a stronger authentication mechanism via progressive enrollment protects them and their personal information and also strengthens the security apparatus for your business as a whole.

- **Think about accessibility**
  While friction is an inconvenience for many users, for others it can present a significant challenge. While considering accessibility as a key variable while designing identity systems is simply the right thing to do, building applications that can be used by everyone also maximizes your market reach.

By following the map, consumer companies can increase conversions and grow revenue by decreasing friction, expanding their market reach, and improving accessibility—all while enhancing security.

Learn More About Identity Management with Auth0

Identity is vital to enabling online applications and will become even more important as the zero trust paradigm gains wider adoption.

Identity is also difficult—even seasoned pros find creating effective and efficient implementations to be challenging.

Auth0 takes on the burden of identity and access management, so you can focus effort and energy on delivering core business value.

Auth0 is an easy-to-implement, adaptable, and secure authentication and authorization platform. Built on a set of composable building blocks exposed through APIs and protocols, the Auth0 Identity Platform provides multiple solutions to address any identity use case without forcing a compromise between convenience, privacy, or security.

Learn more at **auth0.com/identity-platform.**

Auth0 provides a platform to authenticate, authorize, and secure access for applications, devices, and users. Security and development teams rely on Auth0's simplicity, extensibility, and expertise to make identity work for everyone. Safeguarding more than 4.5 billion login transactions each month, Auth0 secures identities so innovators can innovate, and empowers global enterprises to deliver trusted, superior digital experiences to their customers around the world.

For more information, visit **https://auth0.com** or follow **@auth0** on Twitter.