Whitepaper

Move beyond passwords

Get started with passwordless authentication.

Contents

Introduction

Traditional authentication using a username and password has been the foundation of digital Identity and security for over 50 years. But with the ever-growing number of user accounts, there are a number of new issues: the burden on end users to remember multiple passwords, support costs, and most importantly, the security risks posed by compromised credentials. These new challenges are now outweighing the usefulness of passwords. The case for eliminating passwords from the authentication experience is getting more compelling every day.

Emerging passwordless security standards, elevated consumer and consumer-like experience expectations, and ballooning costs have moved eliminating passwords from a theoretical concept to a real possibility. In this whitepaper, we will explore the case for going passwordless for both customer and employee authentication, and map out steps that organizations can take on their journey to true passwordless authentication.

The quest to move beyond passwords

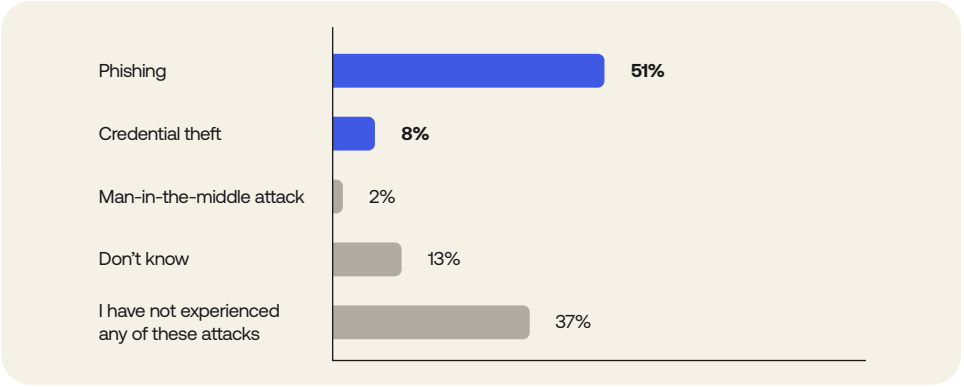
Understanding the need for passwordless authentication starts with understanding the challenges presented by passwords. The core challenges with passwords can be broken down into the following areas:

Poor account security

Passwords have spawned a whole category of security/Identity-driven attacks — compromised passwords due to credential breaches, phishing, password spraying attacks, or poor password hygiene can result in account takeover attacks (ATO). In order to combat these attacks, organizations can start by leveraging an additional authentication layer, i.e., multi-factor authentication (MFA).

59%

of respondents have experienced credential theft or phishing.



But MFA isn't a perfect solution. The challenge with this technology lies with the fact that low assurance second factors, such as SMS, are widely used but have well-documented weaknesses that are exploited by hackers.

> "81% of hacking related breaches used either weak or stolen passwords."
>
> **Gus Shahin**
> CIO, Flex

Source: Ponemon Authentication Report 2019

Poor user experience

Passwords are frustrating. Best practices on password choice vary, but at the very least, we know they should be unique and hard to guess but easy to remember. A survey by the University of Oxford predicted that roughly a third of online purchases are abandoned at checkout because people cannot remember their passwords.

Increased costs

The costs associated with passwords outweigh any benefits of using passwords. Password management is one of the top reasons why people call call centers. Reducing the support burden imposed by passwords is mission-critical for organizations.

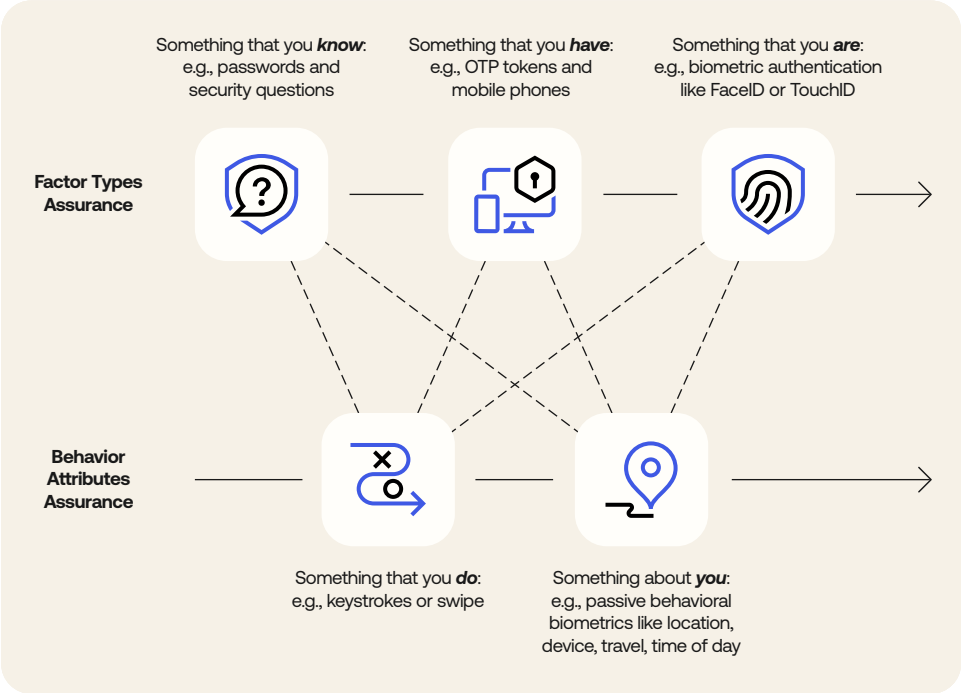
12.6 min/wk Average time per week spent entering or resetting passwords

$5,217,456 Annual cost of productivity and labor loss per company on average

Source: Ponemon Authentication Report 2019

Evaluation of current authentication methods

Current authentication methods use factors such as knowledge, possession, or biometric authenticators. Organizations frequently combine one or more factors and behavioral attributes to drive access decisions. The belief is that by having additional layers of security, you lower the odds that an attacker can gain access to a user's account.



Two key evaluation attributes

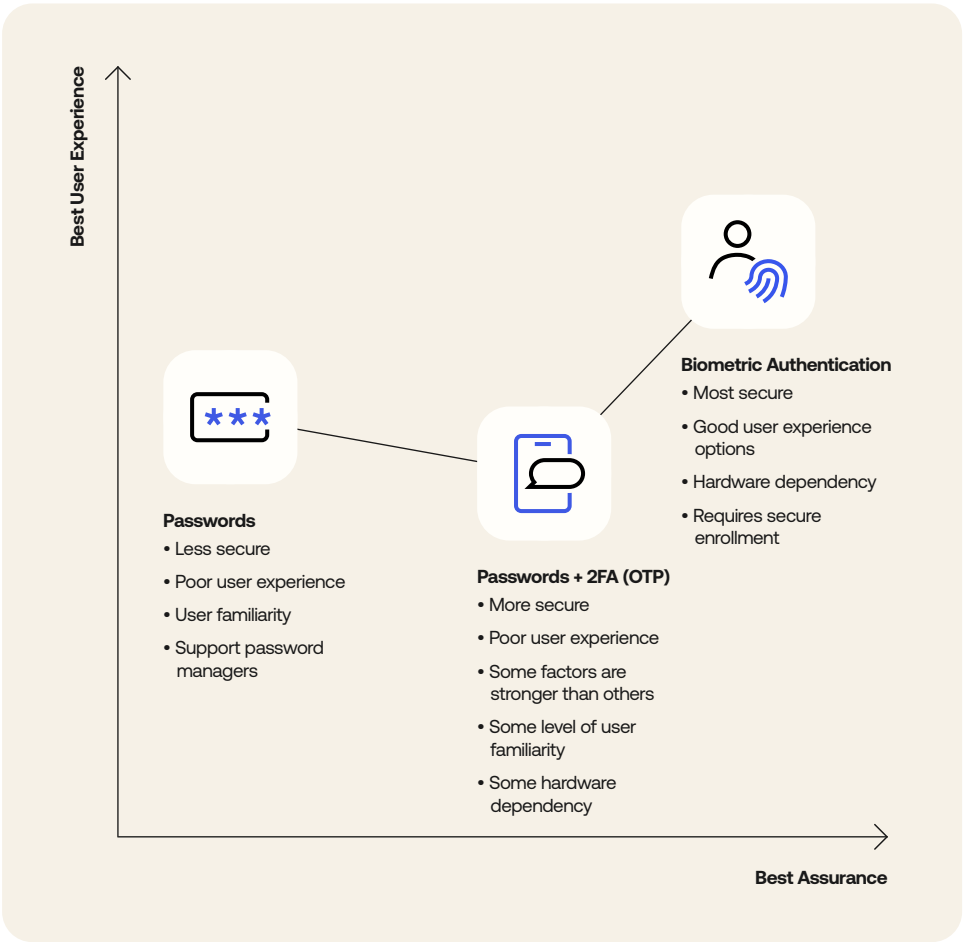
When evaluating authentication methods, we broadly need to look at two key attributes:

Assurance / security

- Can the authentication mechanism ensure only the authorized user gets access to the account?

User experience

- Can the authentication mechanism provide a seamless registration, authentication, and recovery journey?
- Does the authenticator support all authentication for all user groups, device types, and software platforms?



Getting started with passwordless authentication

Moving beyond passwords requires some deep thought. Before organizations decide to eliminate passwords, we recommend a gradual approach by looking at threats, technology, user journeys, costs, adoption friction, and implementation.

Threats

- Credential breaches
- Man-in-the-middle
- Man-in-the-browser
- Password spraying
- Brute-force attacks

Technology

- Browser support
- Technology approach
- Platform authenticators vs. external authenticators

User journey

- Registration flow
- Authentication flow
- Recovery flow

Business considerations

- Support
- Integration
- Device adoption
- Compliance requirements

Adoption friction

- Passwords are common
- Password managers are also common
- Passwords are easy to provision

Implementation

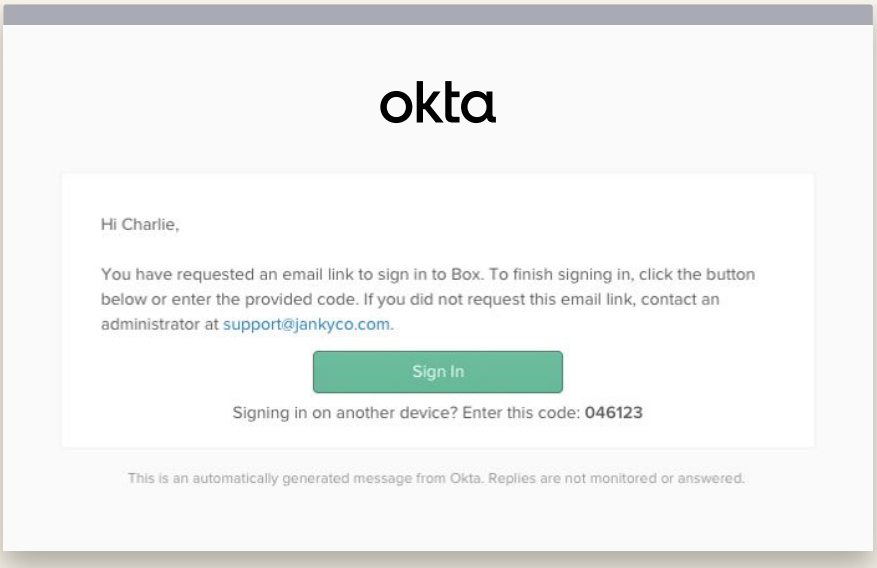
- Security and compliance requirements
- Website support

Common approaches to going passwordless

Eliminating passwords and going passwordless can be accomplished using a number of different technologies. Approaches such as email magic links leave an encoded OTP token or live link in the body of a secure email, while approaches like WebAuthn leverage public-private key-based cryptography to ensure secure authentication.

Okta offers a number of passwordless approaches. In this section we will look into some of the major approaches to going passwordless.

Email magic links

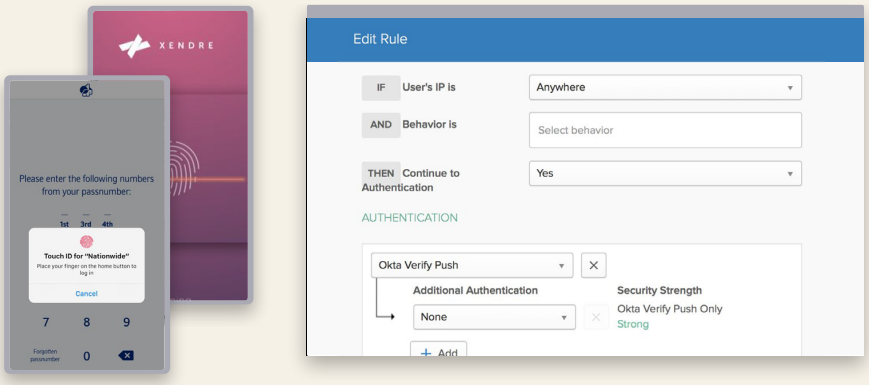


Email-based passwordless authentication has become very common. This method is, at its core, a password reset flow; a secret link is sent to the user that allows them to bypass their password and set a new one. It's familiar to most users because they've utilized it dozens or hundreds of times. This method of authentication has been popularized by apps like Slack and Medium. True passwordless authentication takes the password reset flow a step further. App designers remove the password (and its associated resetting ceremonies) and simply send a secret, time-limited or user life-cycle limited, single-use link to the user's email address. Clicking that link authenticates the user and sets a cookie with a long lifetime to keep them logged in. The user never needs to set, save, or type any

passwords at all, which is a very appealing feature, particularly on mobile devices. This method of passwordless authentication requires no hardware dependencies and is very attractive to consumer applications.

Use cases	Benefits	Challenges
• Infrequent login patterns • Alternative passwordless authentication method for WebAuthn • Stop password-based attacks	• Easy to deploy and use • Seamless onboarding • No hardware dependency • Acceptable and familiar user experience • Consistent experience on desktop and mobile	• Security outsourced to the email account security • No control or visibility into link (email) sharing • Susceptible to man-in-the-middle attacks if the email is not encrypted

Factor sequencing

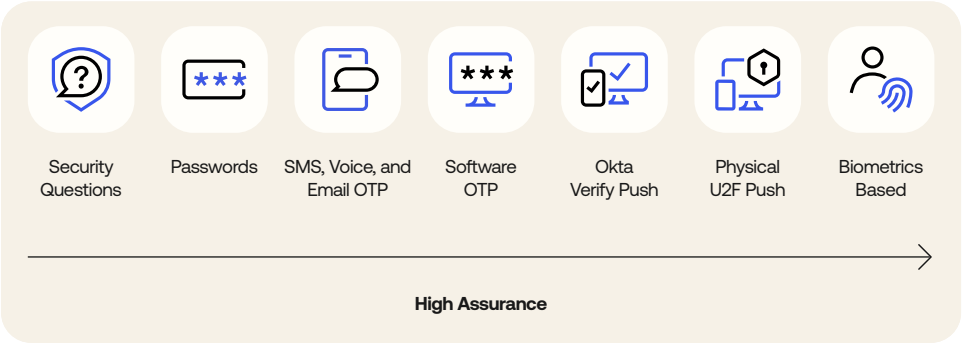


The combination of Okta Adaptive MFA's contextual awareness and the intelligence of ThreatInsight means organizations can securely configure a passwordless solution utilizing a variety of authentication factors. When threat levels are low, the login experience can be streamlined and users can be offered a simpler path to the data and apps they need. However, when the risk level associated with a login is high, additional authentication

factors will be required. For example, an administrator might set the Okta Verify mobile app as the primary authentication factor. If the user logs in from a known location and device, Okta sends an authentication request via the app that the user accepts in order to gain access.

However, if Adaptive MFA detects an anomaly that raises the risk level of the login request, Okta can prompt the user to also make use of a second authentication factor such as WebAuthn.

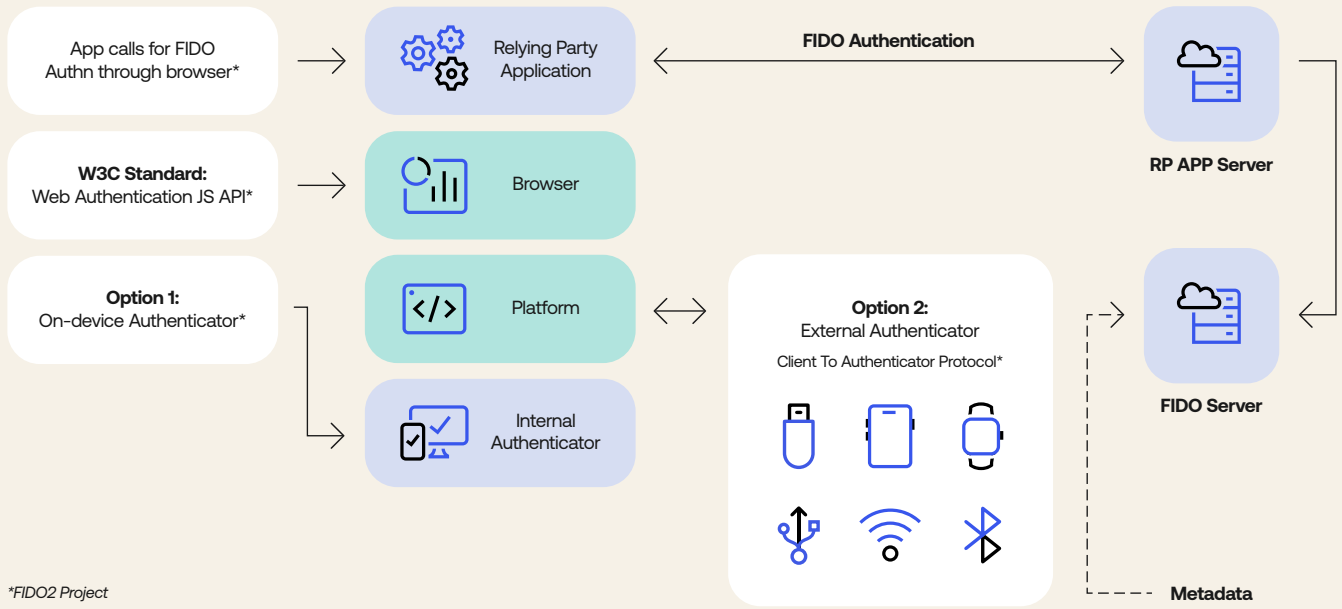
It's important for administrators to take the sliding scale of assurance into consideration when it comes to selecting a method of authentication and choosing factors. User context should be the guide, allowing for simpler login and improved usability whenever the situation allows for it. A knowledge factor, like a security question, is easy to use, but also less secure than a possession factor like U2F. With this in mind, it makes sense to opt for a simple possession factor when a user signs in from their usual network and location at the head office, and reserve more secure factors for instances where a device, network, or location increases the risk level.



Naturally, administrators also need to select factors in a way that makes sense given the company's available technology. Using Okta Verify wouldn't work unless everyone in the organization has access to a smartphone, for example, so it might be better in some instances to use another factor like an SMS OTP.

Use cases	Benefits	Challenges
• Alter the login experience based on session risk • Chain higher assurance factors into the authentication experience	• High assurance login • Consistent experience on desktop and mobile	• Potential hardware dependencies

WebAuthn



WebAuthn is a standards-based passwordless authentication framework that allows web applications to simplify and secure user authentication by using registered devices (phones, laptops, etc.) as factors. With this new standard, any web application running in a browser that supports WebAuthn can now take advantage of these authenticators to securely authenticate users. Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari, Opera and the rapid adoption by platforms (e.g. MSFT Edge with Windows Hello, Google Android) means there's a practical way to

deploy FIDO2/WebAuthn. Now, organizations can deploy with roaming authenticators like YubiKeys or through supported platforms since the device itself is used for WebAuthn.

Use cases	Benefits	Challenges
• Standards-driven passwordless authentication • Scalable authentication experience	• Account takeover to stop Identity-driven attacks like phishing, credential stuffing, password spray attacks • No credential management required • Improved user authentication experience • Reduced organizational support for password management	• Requires hardware and browser support • Needs a secure user boot-strap and recovery flow • Requires pairing with other passwordless authentication methods like email credential links for alternative authentication

Planning for a passwordless future

The adoption of password-less authentication is one of the most impactful steps that can help organizations and services manage a range of security risks and deliver a seamless customer experience. Organizations are now moving towards the adoption of passwordless authentication. Going passwordless is not a revolutionary process, but more of an evolutionary process. Therefore as organizations embark on this journey, we leave you with a roadmap with a few simple options before moving towards true passwordless authentication. Going passwordless requires careful thought and planning. Organizations need to think about the entire authentication lifecycle from secure enrollment, migration from passwords, deployability, recovery, and off-boarding. Organizations that understand all aspects and needs will be well positioned to build a passwordless journey to eliminate Identity attacks, deliver delightful experiences, and grow their business.

Build your passwordless journey with Okta