Gartner Research

# Take 3 Steps Toward Passwordless Authentication

Ant Allan

19 October 2021

Gartner®

# Take 3 Steps Toward Passwordless Authentication

Published 19 October 2021 - ID G00745034 - 19 min read

By Analyst(s): Ant Allan

Initiatives: Identity and Access Management and Fraud Detection

Eliminating login passwords can improve both UX and security, but passwordless authentication is not a discrete technology or a distinct market. SRM leaders responsible for IAM must carefully identify their objectives and options to prioritize time to value along the path to a passwordless future.

**Additional Perspectives**

- Summary Translation: Take 3 Steps Toward Passwordless Authentication (08 November 2021)

## Overview

### Key Findings

- Identity and access management (IAM) leaders seeking to eliminate passwords are often uncertain of what passwordless authentication should actually look like.
- IAM leaders are often put off by the prospect of investing in novel technologies — unaware of the passwordless methods and flows that are available in incumbent tools —or by the lack of a universal approach.
- While passwordless methods, especially those based on FIDO2, are widely available, they are not yet universally supported or adopted. Thus, universal passwordless authentication remains tantalizingly on the horizon.

### Recommendations

Security and risk management (SRM) leaders responsible for IAM ("IAM leaders") should take the following steps toward passwordless authentication:

- Identify drivers and define objectives by collaborating with stakeholders to agree on priorities for UX and security improvements, and preferences among different methods and flows.

- Minimize time to value by fully exploiting the capabilities of incumbent tools, even if the scope is limited to one or a few use cases (such as Windows and SaaS login).
- Prepare for universal adoption by shifting investments to tools and methods that simplify the migration path. Make net new investments, if needed, in specific use cases.

## Strategic Planning Assumptions

By 2025, more than 50% of the workforce and more than 20% of customer authentication transactions will be passwordless, up from less than 10% today.

By 2025, more than 25% of multifactor authentication (MFA) transactions using a token will be based on FIDO authentication protocols, up from less than 5% today.

## Introduction

Passwords remain ubiquitous in user authentication but are vulnerable to many attacks. Thus, they do little to bring account takeover (ATO) and other digital-identity risks within an organization's risk tolerance. Compromised passwords account for more than 60% of breaches due to hacking. [1]

Multifactor authentication, [2] typically achieved by adding some kind of token to a legacy password, [3] can significantly reduce risks. [4] But the password remains extremely vulnerable, putting a significant burden on the additional factor.

With or without additional factors, passwords can be a significant source of friction and frustration for users and administrators. They degrade user experience (UX) for both employees and customers, and create a significant volume of service desk or contact center calls. Thus, Gartner clients are increasingly seeking passwordless authentication methods.

However, even though many vendors explicitly offer "passwordless authentication" methods, "passwordless" doesn't specify what an authentication method is, only what it is not. The term doesn't define a new market or a new innovation (although some innovations are inherently passwordless).

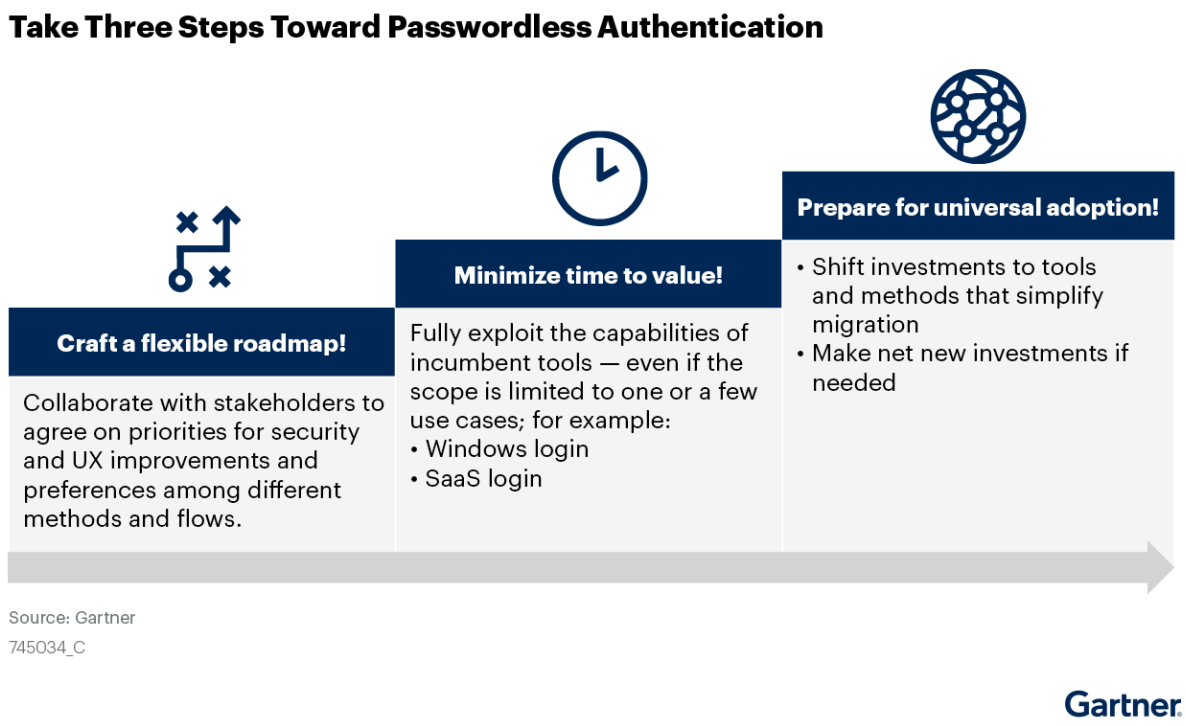
While IAM leaders often have a very clear idea of the need to stop using passwords, and why, they might be less certain of which way of achieving passwordless authentication best meets their needs. Or, seduced by fashionable vendors' marketing, IAM leaders might overlook options that are readily available and don't demand new investment.

**Passwordless authentication is an aspiration, not a destination.**

How, then, should IAM leaders approach a "passwordless authentication" initiative to define a destination that maximizes effectiveness (reducing risks or improving UX) and minimizes costs?

Follow the three steps outlined in this research to identify drivers and define objectives, to minimize time to value, and to prepare for universal adoption in the next few years (see Figure 1).

Figure 1. Take Three Steps Toward Passwordless Authentication




# Analysis

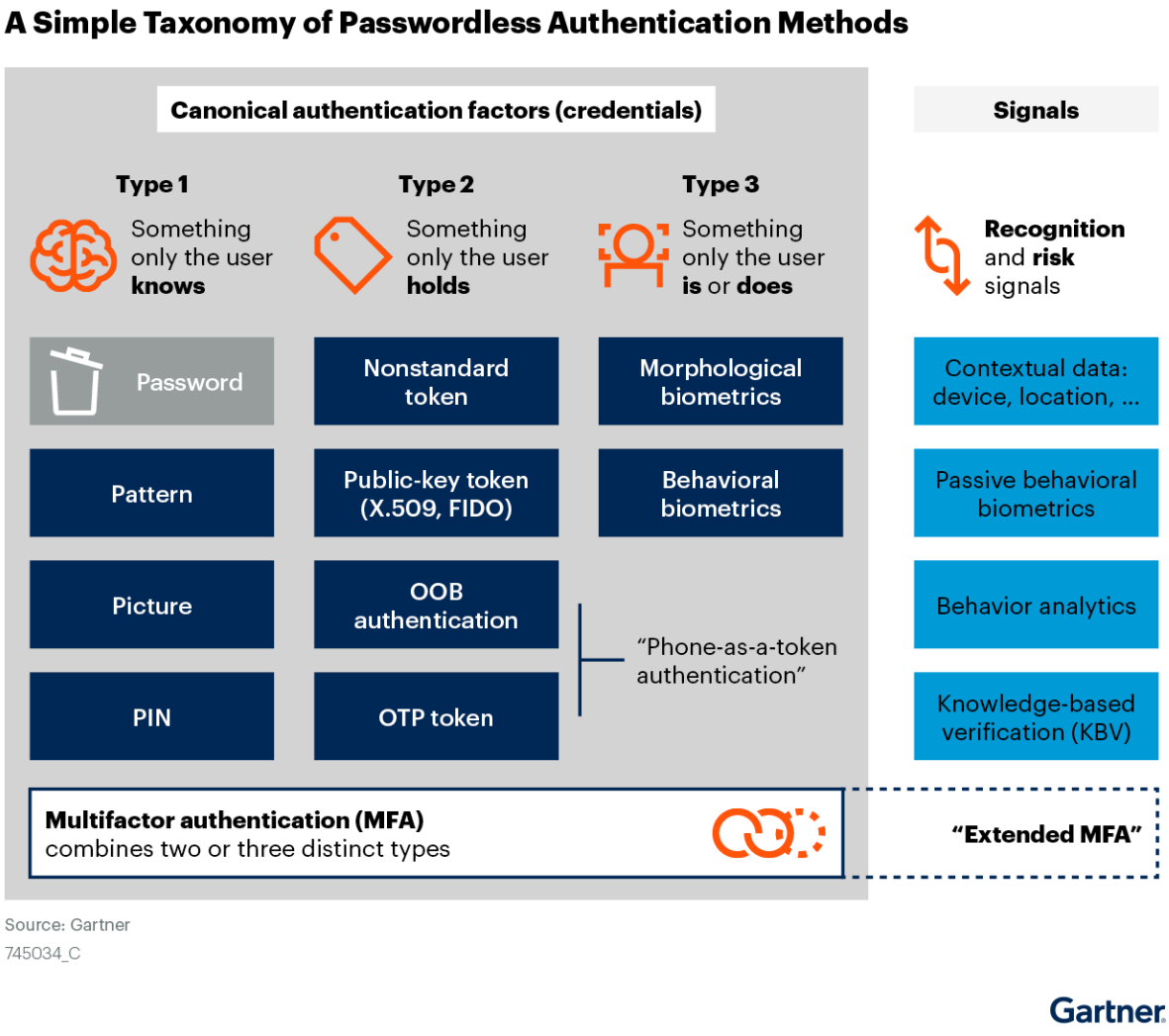
## Step 1: Identify Drivers and Define Objectives

*Collaborate with stakeholders to agree on priorities for UX and security improvements, and preferences among different methods and flows.*

As noted above, “passwordless authentication” doesn’t define a new market or a new innovation. User authentication can be based on one or more credentials of three different types, with or without the addition of recognition and risk signals.

A passwordless authentication method is simply one that uses any credential or combination of credentials and signals that isn’t, or doesn’t include, a password (see Figure 2).

Figure 2. A Simple Taxonomy of Passwordless Authentication Methods




Source: Gartner
745034_C

Gartner

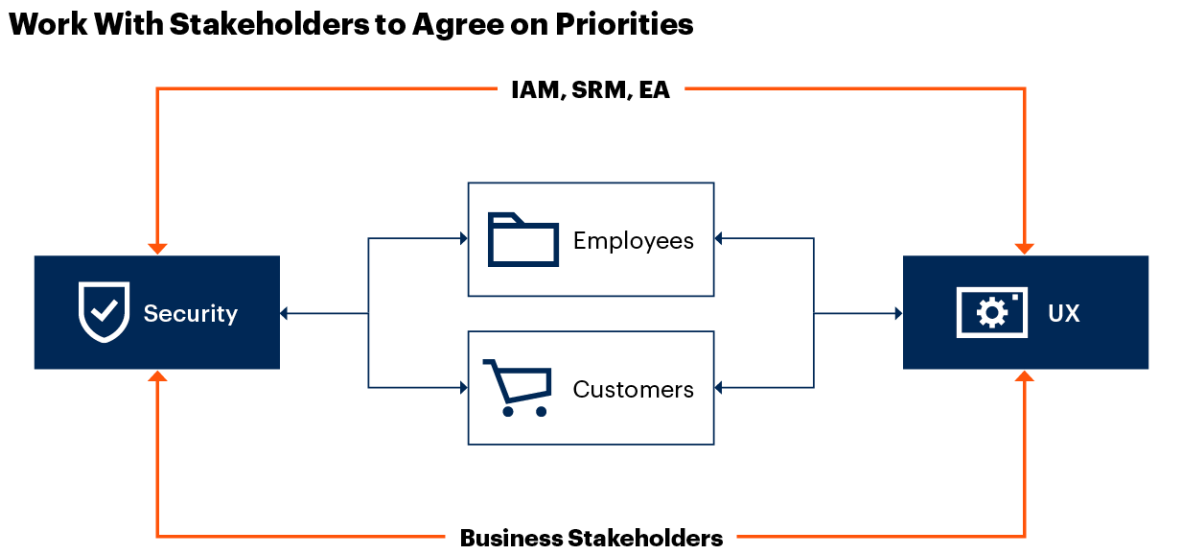
PINs can be contentious. In this research, we make the distinction that PINs are wholly local to devices (e.g., smart cards, smartphones) and used to “unlock” credentials stored therein, in contrast to passwords that are centrally stored (e.g., in Active Directory), creating a honey pot for an attacker. [5]

For example, a PIN-protected smart card or FIDO2 security key provides a robust passwordless authentication method. However, some Gartner clients deprecate PINs, as they have the same "look and feel" as passwords, with similarly poor UX, and are also vulnerable to, for example, "shoulder surfing."

Here, and across the board, IAM leaders must have a clear notion of what their destination will look like, based on security and UX needs. They must determine which approaches can most effectively meet their criteria.

They cannot do this alone and must work with SRM colleagues, enterprise architects and representatives from various lines of business (see Figure 3). [6]

## Figure 3. Work With Stakeholders to Agree on Priorities




Source: Gartner
IAM = identity and access management; SRM = security and risk management; EA = enterprise architecture; UX = user experience
745034_C

Gartner

The key security-first goals are to:

- Eliminate centralized password stores, removing passwords completely from the infrastructure.
- Reduce ATO and other digital-identity risks.

The key UX-first goals are to:

- Remove passwords from the user journey.
- Avoid adding more friction.

The key questions that will shape the passwordless authentication roadmap are:

- What passwordless methods are already owned?
- Can existing user authentication flows be modified to avoid passwords?
- Can planned investments be exploited to ease migration?
- Are there urgent needs that demand net new investments?

These questions are fleshed out in the following sections (the second and third steps). All stakeholders must be familiar with the possible next steps to answer these questions and to agree on priorities for the roadmap in this first step.

## Step 2: Minimize Time to Value

*Fully exploit the capabilities of incumbent tools, even if the scope is limited to one or a few use cases.*

While there is significant hype in the market about newer vendors with novel passwordless authentication options, some well-established and widely available methods might meet an organization's needs across different employee and customer use cases.

Here, we outline four options:

- Windows Hello for Business (WHfB)
- Phone-as-a-token and mobile MFA
- "Magic links"
- Signals-first authentication flows

### Windows Hello for Business (WHfB)

Many organizations have fully migrated to Windows 10, offering the possibility of using WHfB where other hardware and infrastructure prerequisites can be met. [7]
WHfB is based on FIDO2 (which we discuss in some detail later). It combines local authentication, typically using a fingerprint or, more often, face recognition, or a PIN, [8] with embedded public-key credentials for passwordless MFA to Windows networks and downstream applications.

When used from an Azure-AD-joined PC or tablet, WHfB login can be "consumed" by Azure AD Conditional Access to "skip" a need to use Azure MFA or an alternative. However, to enroll, users need to use Azure MFA, for example, using out-of-band (OOB) SMS, as well as their AD passwords.

### Phone-as-a-Token Authentication and Mobile MFA

Phone-as-a-token authentication [9] is widely used in both employee and customer use cases and is readily available in access management (AM) tools as well as stand-alone user authentication tools.

A phone-as-a-token method can be used as a direct replacement for a password (see Figure 4). OOB SMS modes, ubiquitous in the market, are used for passwordless customer authentication to online banking and other services in China, India and Russia. [10] Other variants may require new investments. [11]

Figure 4. Adopt Passwordless Phone-as-a-Token Authentication

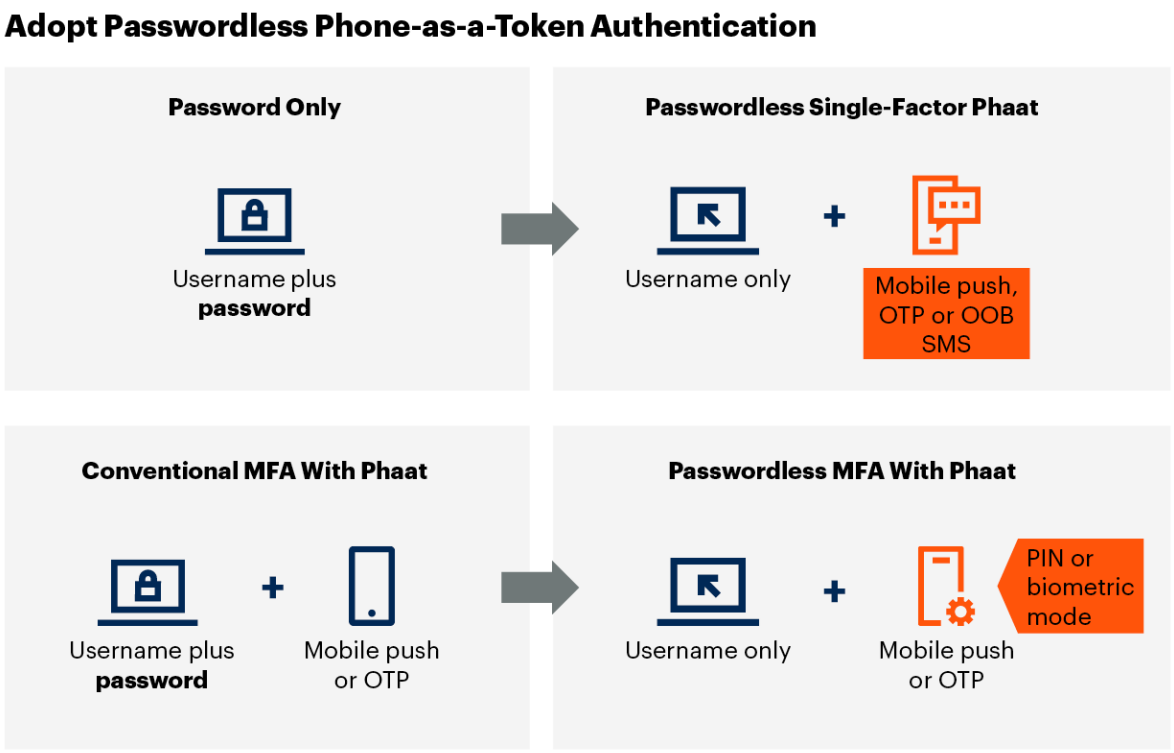



Figure 4 also shows an MFA variant. In this case, the password is replaced by an additional factor in the mobile push or OTP app on the phone, either a PIN or a biometric mode (e.g., Apple Touch ID or Face ID). This is an example of "mobile MFA." [12]

One of the challenges of passwordless authentication in general is that it might not be possible to eliminate the password from existing flows (e.g., a legacy VPN using RADIUS). This limits where mobile MFA can be usefully deployed, but it is well-suited to use cases where an AM tool can manage the flow.

This option is available in several tools that organizations might already have deployed, including AM tools from CyberArk, ForgeRock and Microsoft, and authentication tools from Entersekt, KOBIL and SecurID. Newer vendors with obligate mobile MFA approaches likely require new investments.

Another challenge, shared with conventional phone-as-a-token methods, is that not everyone can or will use a phone, especially if they're asked to use a personal device. OTP hardware tokens are the normal alternative, but PIN-protected versions that mirror mobile MFA are uncommon.

### "Magic Links"

Some vendors (e.g., Auth0, LoginRadius, Okta) offer "magic links," a kind of out-of-band authentication using email or an SMS message. However, rather than an OTP, the message embeds a link that the user simply clicks on to authenticate and continue the login process.

There are two cautions. First, if using email, this method is no stronger than the authentication to the email account, which may be a password outside the organization's control. Second, if using SMS (which is stronger, but still quite weak), it doesn't readily support access from a PC, eroding UX. [13]

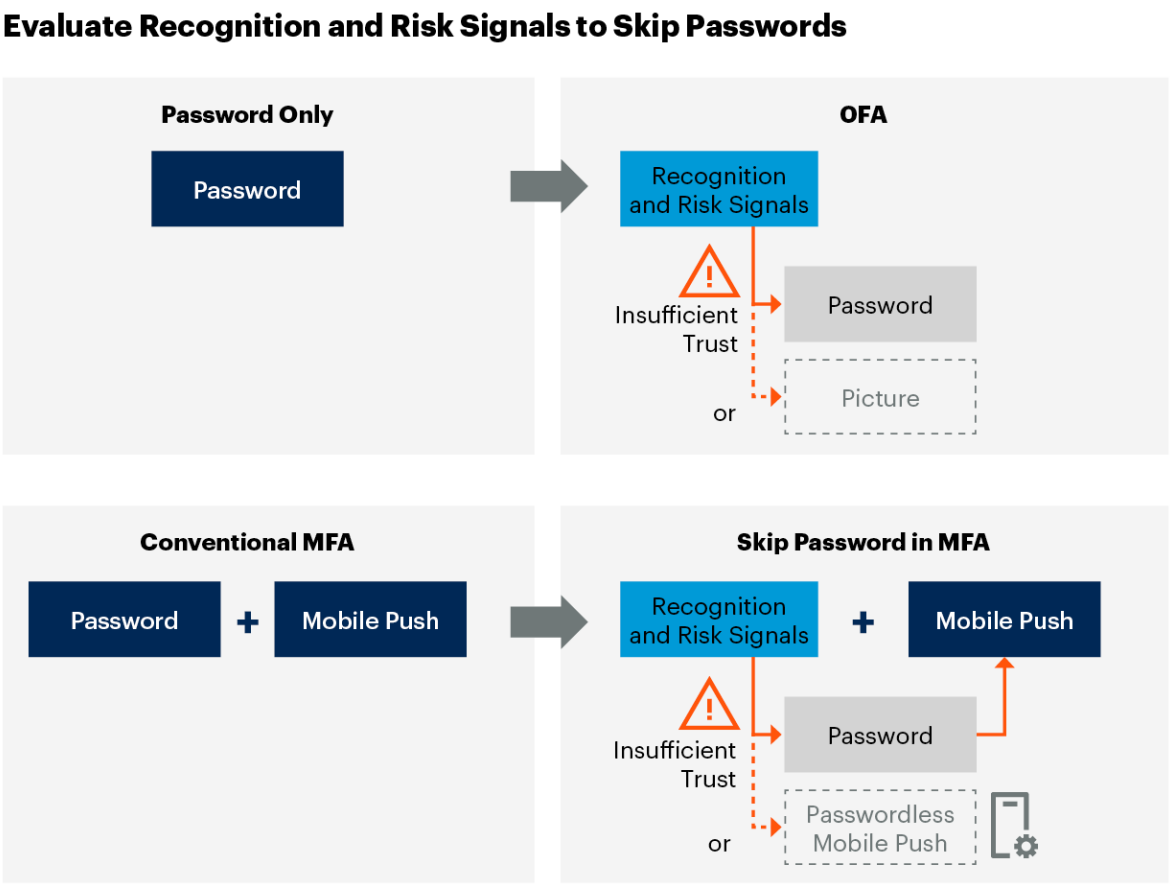
This method might be appropriate for infrequent access to lower-risk applications or as a replacement for a password as part of MFA.

### Signals-First Authentication Flows

Recognition and risk signals (see Figure 2) are quite commonly used with conventional MFA use cases to support "risk-based authentication" or "conditional access." If the signals meet certain criteria, a user can log in with a password and not have to use, say, mobile push as well, except maybe every *n*th day.

Where password-only authentication is still appropriate, e.g., in some customer use cases, these signals can be evaluated before the password is entered. If they meet the criteria, the user can enjoy "zero-factor authentication" ("0FA"); if not, the user is prompted to enter the password anyway (see Figure 5).

Figure 5. Evaluate Recognition and Risk Signals to Skip Passwords




Source: Gartner
0FA = zero-factor authentication
745034_C

Gartner

This provides UX benefit by taking the password out of the authentication flow, but doesn't eliminate the passwords at all. However, the password could be replaced with an alternative knowledge method (e.g., a picture-based method), but this would require new investment (see the Pattern and Picture Methods section below).

This approach prompts the following questions:

- Can signals alone provide the same confidence in the claimed identity as a password?
- Does 0FA indicate intent? That is, if there is no friction, is it clear that the user meant to log in?

- Are people completely happy to go passwordless? Again, if there's no friction, people who have been inculcated with the importance of passwords might not feel secure, reducing UX.
- If people can ordinarily skip passwords, are they more likely to forget them and have to endure clunky password reset processes?

Thus, a 0FA approach requires careful evaluation.

In MFA use cases, if the signals meet the criteria, the user skips entering the password and is simply prompted to use mobile push (or whatever the "second" factor is), enhancing UX. [14] Again, if the signals fall short (e.g., login from an unknown device), the user has to enter the password anyway.

Several AM vendors including ForgeRock, Okta and Ping Identity can support signals-first flows, and these can be easily switched in, if "conditional access" type approaches are already in play. [15]

To completely eliminate passwords, mobile MFA can be used. Where the signals meet the criteria, mobile push can be used with a simple tap; otherwise, the user is prompted to use a PIN or biometric method. However, this requires tight integration between the app and authentication flow.

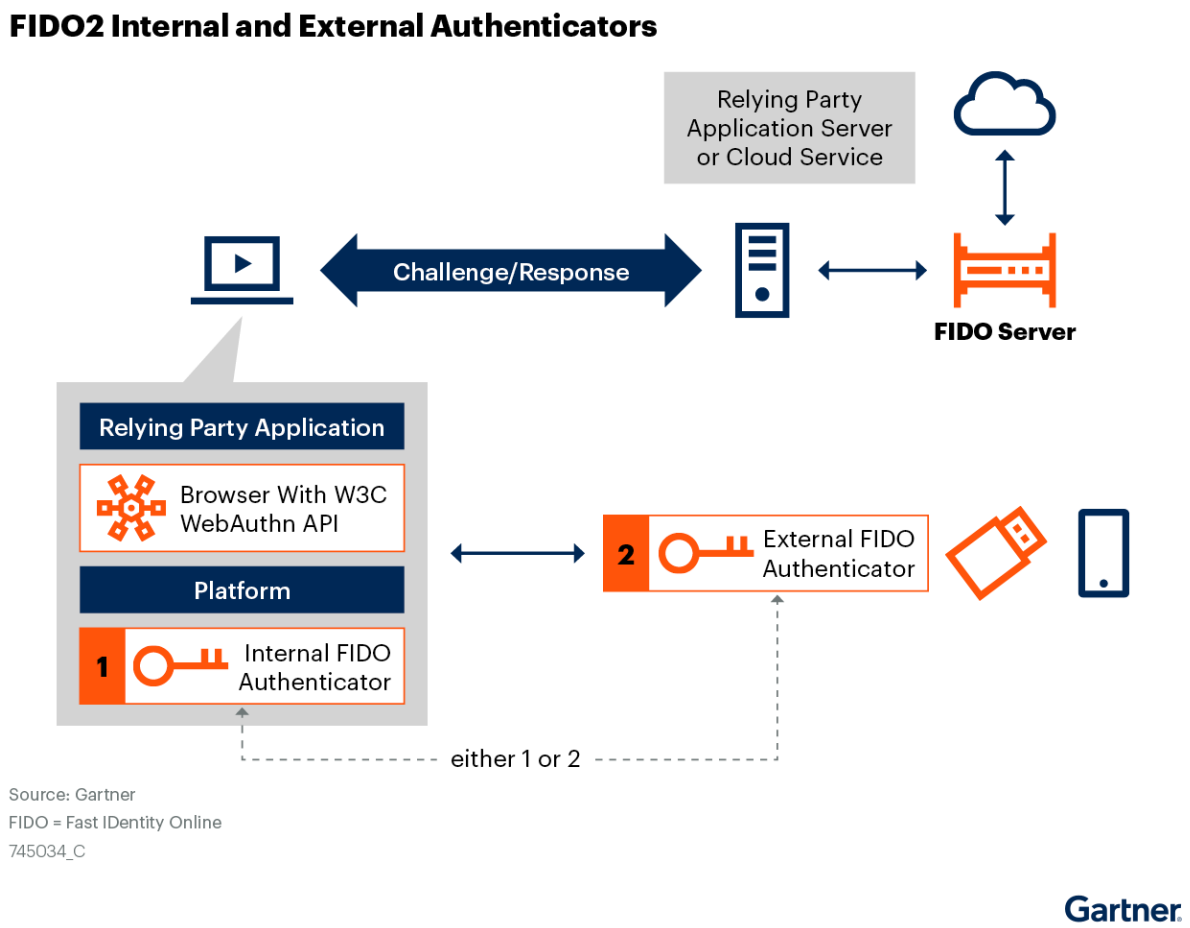
## Step 3: Prepare for Universal Adoption

*Shift investments to tools and methods that simplify the migration path. Make net new investments if needed in specific use cases.*

Gartner projects that FIDO2 will become the dominant flavor of authentication token in the midterm, with more than 25% adoption within the next three years. [16] FIDO2 will likely dominate in workforce use cases, but faces more hurdles in customer use cases.

FIDO2 authenticators can be *internal* to an endpoint device, either natively in the operating system or as third-party software, or *external*, either a dedicated USB or wireless hardware token ("security key") or a "companion" device with an internal authenticator (see Figure 6).

Figure 6. FIDO2 Internal and External Authenticators




FIDO2 authenticators can be used to authenticate to applications via browsers supporting the W3C Web Authentication (WebAuthn) API. AM vendors now commonly offer FIDO2/WebAuthn support, as do specialist vendors like Nok Nok Labs.

Microsoft Windows 10 supports the use of FIDO2 external authenticators as well as WHfB, which is essentially a Windows-native internal authenticator. Thus, in workforce use cases, FIDO2 external authenticators provide a transportable solution for login to desktops as well as to cloud applications.

Most of the hype around FIDO2 has been about the use of FIDO2 security keys. However, few Gartner clients have an appetite for hardware tokens for everyone.

Phone-as-a-token authentication has huge traction in the market, and we project that this will be the more popular option for FIDO2 in the midterm. However, FIDO2 apps for smartphones are still uncommon in the market, offered by specialist vendors (e.g., IDmelon) rather than mainstream vendors. [17]

IAM leaders can simplify the migration path to FIDO2 by shifting procurement to multiprotocol authenticators that are FIDO2 ready, but continue to support incumbent legacy methods:

- PIN-protected or biometric-enabled USB or wireless hardware tokens supporting FIDO2 as well as OTP or X.509 from vendors such as FEITIAN Technologies, Hypersecu Information Systems and Yubico.
- Mobile MFA supporting FIDO2 as well as mobile push, OTP or X.509 in combination with a PIN or biometric method (either device native or third party). These will become readily available over the next one to two years.

The second option can be approximated by discrete FIDO2 and, say, mobile push/OTP apps from different vendors, but that requires new investment. IAM leaders should press incumbent mobile push/OTP app providers for their roadmap for FIDO2 support. WebAuthn support is not enough.

In customer use cases, FIDO2 adoption will be more limited as:

- There is limited and uneven penetration of native FIDO2 support in endpoint devices.
- Many customers are reluctant to download authenticator software.
- Organizations don't want the overheads of hardware tokens.

The second obstacle is potentially removed by vendors such as Transmit Security and Trusona, which have launched "appless" FIDO2 authentication. However, these are nascent, and IAM leaders should carefully review their suitability.

### Other Alternatives to FIDO2

IAM leaders who have needs for passwordless authentication that can't be satisfied by the options discussed in the previous section (Step 2), and cannot wait for FIDO2 or deem FIDO2 unsuitable (e.g., in some customer use cases), might choose among the following options:

- Mobile MFA
- Biometric authentication
- Pattern and picture methods
- Continuous adaptive trust

### Mobile MFA

Vendors such as HYPR, Secret Double Octopus (SDO), Trusona and Veridium offer obligate mobile MFA solutions; that is, they provide passwordless MFA by design, without a "+1FA" option, rather than being an evolution of a conventional mobile push app.

Some of these are FIDO-certified but are highly proprietary. They can typically support PC and network login, via credential provider integration, as well as remote and cloud access use cases.

### Biometric Authentication

Vendors such as Daon, iProov, Keyless, TypingDNA and Veridas (and many others) offer biometric authentication for a variety of use cases.

Biometric authentication has had significant traction in mobile banking apps. Gartner projects that this will become increasingly important in a broader range of customer use cases across multiple channels, especially when it can be integrated with document-centric identity proofing (DCIP). [18]

### Pattern and Picture Methods

Several vendors provide a variety of different ways of using some combination of knowledge and graphical elements as a password replacement. For example:

- Authlogics presents the user with a 6×6 or 8×8 grid of random digits and prompts them to enter an OTP based on a memorized pattern (e.g., partial diagonals, knight's moves).
- PixelPIN presents the user with a chosen image and prompts them to click or tap on four chosen points in order.

Methods of these kinds have been available for decades and often perform well in academic studies of UX (particularly in terms of memorability, compared to passwords), but none has had significant traction in the market. Nevertheless, we think they are worth careful consideration.

### Continuous Adaptive Trust (CAT)

CAT is a model (rather than a product) that can significantly broaden and deepen signals-first authentication flows. It assumes the use of advanced analytics (e.g., machine learning) with a richer set of signals, including passive behavioral biometric methods and behavior analytics (see Figure 2).

CAT is part of a broader adaptive access approach that continuously seeks to balance trust in a claimed identity against the risk of access. Vendors that can at least contribute to CAT approaches to passwordless authentication include Acceptto, Callsign, Prove (incorporating UnifyID) and TruU.

Forward-looking IAM leaders should evaluate this approach, which will be more fully described in forthcoming Gartner research.

### Is Universal Passwordless Authentication Actually Achievable?

The short answer is, "no," unless an organization is in the fortunate position of having:

- All its applications in the cloud.
- On-premises applications that can either:
  - Piggyback on Windows authentication flows.
  - Federate to an AM tool or other identity provider (IdP) supporting passwordless methods or flows.

Applications that obstruct universal adoption are those with one or both of the following "features":

- Passwords "baked" into an authentication flow that cannot be modified by the organization; e.g., a legacy VPN using RADIUS:
  - Some applications might be brought within scope via SSO tools supporting password vaulting and forwarding. However, this is a rather fragile approach.
  - Some passwordless authentication methods (e.g., mobile MFA) can be simply layered on top of an existing password flow as if they were a typical second-factor method, but UX is clearly suboptimal in this case.

- No standards-based way of integrating with the IdP; e.g., no support for Security Assertion Markup Language (SAML) or OpenID Connect federation:
  - Bringing an application within scope then becomes dependent on the IdP or other vendor having a programmatic interface for that application (e.g., an SDK or API).

Nevertheless, such pockets of "passwordless-less" authentication should not derail IAM leaders from planning to migrate to passwordless authentication elsewhere across their application infrastructures and executing on that plan.

However, as long as passwords persist in any login flows, organizations and users still have the burden of managing them, including enforcing and complying with effective password policies (see Quick Answer: What Does a Good Password Policy Look Like?).

## Evidence

[1] 2021 Data Breach Investigation Report, Verizon.

[2] We use the term "MFA" throughout for combinations of two or more factors. MFA using three factors is rare, and the term is very widely used as a synonym for "two-factor authentication" ("2FA").

[3] Thus, most legacy "MFA" tools are really only "+1FA" tools, adding a single extra factor to an existing password. Here, "MFA" has been a convenient shorthand, but it masks an important distinction between legacy approaches and modern passwordless MFA methods that incorporate both factors.

[4] Microsoft noted that 99.9% of ATO attacks can be blocked by MFA.

[5] Of course, plaintext passwords should not be stored. The store should hold only hash values derived from the passwords, with suitable salting and key stretching.

[6] This collegial approach is a top practice for all user authentication decisions and, indeed, for all IAM decisions (see Best Practices for IAM Program Management and Governance).

[7] For the infrastructure requirements, see Windows Hello for Business Deployment Prerequisite Overview.

[8] In WHfB, the PIN must always be available. However, it is possible to set " multi-factor unlock" to require use of, say, the PIN and a biometric method.

[9] Phone-as-a-token authentication encompasses a variety of methods that enable a phone to be used as an authentication token, including: OTP software tokens ("OTP apps"); mobile push via a dedicated app; and OOB SMS and voice modes, making use of generic messaging apps or infrastructure (see Innovation Insight for Many Flavors of Authentication Token).

[10] While we deprecate OOB SMS as a second factor in MFA, it still has more value than a password for single-factor authentication. Some government clients find this approach attractive for low-velocity users who seldom remember their "government gateway" passwords and end up going through clunky password reset processes.

[11] For example, in China, firms such as WeChat, Taobao and JD.com enable passwordless website login by prompting people to scan a quick response (QR) code with their custom smartphone apps.

[12] Hype Cycle for Identity and Access Management Technologies, 2021 provides a full description of mobile MFA variants, including X.509 and FIDO2.

[13] Its utility depends on the availability of a messaging app on the PC. Thus, this would have acceptable UX on an iMac with the macOS Messages app, for example.

[14] This is not necessarily the case. However, against expectations, the author's own experience is that it is easier to use mobile push for login a few times each day than to use a password. Except for the few occasions when he has left his phone charging in another room.

[15] The lower part of Figure 5 shows a typical flow for MFA, in which the password is evaluated first, with mobile push being used as the second factor once the password has been verified. However, AM vendors can also support a "mobile push first" flow, which can protect against brute force attacks against passwords. The same reordering can be used when the password is replaced by recognition and risk signals. The user responds to mobile push first; if the signals provide sufficient trust, login is complete; otherwise, the user is then prompted to enter their password (or use an alternative method).

[16] Innovation Insight for Many Flavors of Authentication Token describes FIDO2 among the other flavors of authentication token.

[17] Android and new iOS phones with native FIDO2 capabilities could be used. However, this gives an organization little control. It is reliant on how FIDO2 has been implemented on the phone and which local gesture (e.g., PIN, biometric method) the user chooses to use. It's also limited to using a device-native biometric method, rather than a third-party method, with everything that entails (see Technology Insight for Biometric Authentication).

[18] Market Guide for Identity Proofing and Affirmation describes DCIP in detail and Technology Insight for Biometric Authentication discusses the contiguous use of DCIP and biometric customer authentication.

## Document Revision History

Passwordless Authentication Is Here and There, but Not Everywhere - 18 December 2019

---

## Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Innovation Insight for Many Flavors of Authentication Token

Technology Insight for Biometric Authentication

Market Guide for User Authentication

Tool: Vendor Identification for User Authentication

IAM Leaders' Guide to User Authentication

---

## Gartner Identity & Access Management Summit

6 – 7 March 2023 | London, U.K.
gartner.com/eu/iam

# Experience Gartner research live

Join Gartner experts and your peers at Gartner Identity & Access Management Summit 2023, 6 – 7 March, London, U.K., to share valuable insights on adopting an identity-first security mindset, putting identity-based controls at the heart of your organization's protection architecture and expanding capabilities around threat detection and response.

Learn more at **gartner.com/eu/iam**



Gartner®