



Your Bridge to Passwordless

Key considerations when building a secure passwordless strategy

What is passwordless?

You will find there are as many definitions of passwordless as there are passwords, but to keep it simple let's start with this basic definition:

Passwordless authentication is any form of authentication that doesn't require the user to provide a password at login.

In a broader sense, passwordless is a journey the enterprise decides to embark upon rather than an overnight destination. To get there every enterprise may have to take a different road depending on factors like their current user environment, their existing authentication processes and whether their IT staff is ready to cross the bridge to passwordless. This whitepaper helps you sift through the key considerations when mapping out your road to passwordless, no matter where you start the journey.

Not all MFA is built equal

There are many examples of passwordless multi-factor (MFA) in use today. However, not all MFA is equal in their strength of security and defense against phishing. The goal of an organization should be to adopt a passwordless MFA solution that offers strong phishing defense. But first let's take a look at the options available today

SMS – SMS verification is one form of passwordless authentication solution because you don't need to remember a password. Usually, you're sent a One-Time-Password (OTP) code valid for a short time to be used for authentication. Many people are getting too used to seeing these text messages sent to their phone, often in the form of a 6-digit numerical code. These are vulnerable to being intercepted so they are considered a weak form of authentication.

Email magic link – This is also a commonly used way to circumvent having to remember a password. A unique link with an embedded token is created and delivered to a verified email address (we hope it's verified!). Clicking the link verifies the user for that particular service, and there may be an expiration time for that link.

You can even use SMS to deliver the magic link, but what you're gaining in usability you may be losing in security. Both of these methods are highly susceptible to phishing. If a user is tricked into typing in a fake OTP or clicking on a "phishing bait" magic link, that user might just give away the store. You can read more about modern phishing techniques [here](#).






Smart cards – A third, and perhaps the most familiar passwordless implementation, uses the trusty smart card. Government employees know these as PIVs (personal identity verification) and CACs (common access card). Smart cards are one of the most effective ways to protect against phishing, and are known to offer a high level of security. The user must insert their smart card into a reader, and validate the smart card with a unique PIN. This is one of the best ways to stop remote

phishing attacks. But traditional smart cards may be somewhat complex for administrators to implement and manage, and involve having a good strategy in place to implement at scale. While the administrative usability leaves room for improvement, the end user usability and security are both top notch and similar to FIDO2. Thus, this approach may be considered as a component of an enterprise passwordless solution as infrastructure and environments evolve to support newer standards.

Biometric readers – Biometric readers use something uniquely biological (a face, a fingerprint, an iris, or other feature) as a credential. As more and more modern devices are available with built in platform authenticators such as TouchID, FaceID and others, the use of biometrics is growing fast. In many cases PINs are necessary to back up a device that fails to read the correct biometric information.

PINs – PINs are often paired with local devices like biometric readers or smart cards. Since a PIN is always tied to a physical device, it is considered more secure than a password because it does not reside on a server that can be breached, nor does it have to be sent over a network.

Not all of these passwordless approaches are created equal. SMS, OTP and certain forms of mobile authentication are considered to be outdated by many and are increasingly known to be highly phishable. Therefore companies that want to accelerate toward passwordless should consider a roadmap to advance those authentication processes in their environment. Modern authentication methods will mitigate risks from increasingly sophisticated threat vectors.

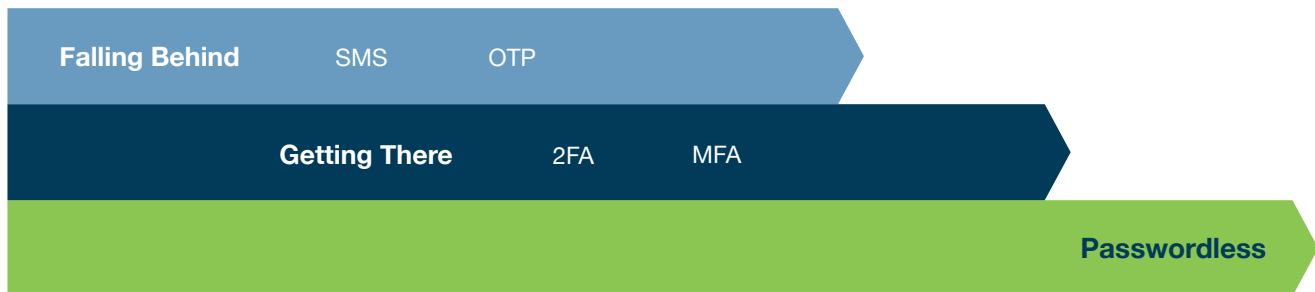
Traditional MFA alternatives	Modern Authentication & the Passwordless future
 <p>SMS/Voice</p>  <p>TOTP</p>	 <p>Smart card</p>  <p>Biometric</p>  <p>PIN</p>

Where are enterprises today on the road to passwordless?

Every company is parked at a different mile marker on the road to passwordless. Knowing where you are parked (i.e. knowing what kind of environment you have) is the first step to creating a passwordless strategy.

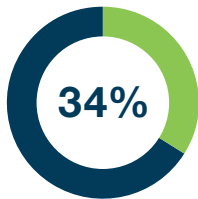
There are two questions worth asking to determine how far you are down the road:

1. Do you operate in the cloud, on-premises, or a hybrid environment? It may be comforting to know that no matter what type of technical environment you have today, you can take advantage of one or more passwordless MFA options available to you.
2. How do you prioritize security levels, user experience and compliance cost? These elements are sometimes in conflict, so it's worth knowing how you will negotiate the trade-offs if you have to make tough choices.

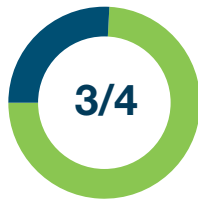


It's clear that the road to passwordless is a long one with a few turns. It's not a "one-and-done" implementation strategy. But a journey has to start somewhere—with a good map you'll get there in due time.

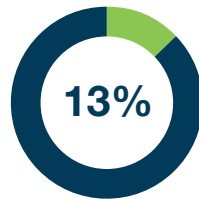
Many companies have already embarked on that journey. In a recent [survey](#) we found:



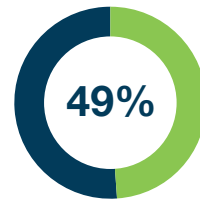
34% of companies have passwordless technology deployed and 27% are in pilot



Nearly three out of four companies plan to increase spending on MFA



13% are planning to deploy in 12 months, 7% in 24 months



MFA/2FA is the top security technology to be adopted (49%) as a response to Covid-19

Choosing your passwordless strategy - Smart card, FIDO2/WebAuthn or Hybrid

Once you've identified where you are on the road, you'll need to choose the best strategy for reaching a passwordless destination. Your choice on where to start may be dictated by whether you want to focus on improved user experience, more robust security measures, or other business drivers like compliance costs and help desk resources. But every move away from passwords, no matter how small, is going to improve security because we know that a password-focused environment will always be more phishable and less safe.

We're going to cover a few different ways an organization can adopt secure passwordless authentication in their organization in order to offer a fast and easy user experience that is safe and enables productivity. First we'll address a smart card passwordless approach, and next discuss how FIDO2/WebAuthn passwordless can be adopted in the organization while working with an existing Identity Access Management (IAM) solution. And, finally we'll look at hybrid passwordless implementations where

organizations combine smart card passwordless and FIDO2 passwordless to solve specific use cases.

No matter which direction an organization takes, modern passwordless authentication can be enabled with hardware-based security keys that can support a variety of passwordless-based approaches. Organizations should consider a future-proofed security investment, such as multi-protocol hardware security keys that can secure legacy, and modern environments with passwordless MFA.

1. Smart card passwordless approach

We've mentioned smart cards as a step toward passwordless, and many companies already use them for secure access to sensitive resources and systems. Those companies that do not have a cloud-first environment (i.e. instead have legacy systems and applications that are largely on-premises) should consider implementing a smart card-based passwordless approach. This offers both the benefits of strong security and a passwordless user experience.

Smart cards are eminently less phishable than a password-based system, and used effectively in some of the most security-conscious

organizations in the world today. Traditional smart deployments are complex and time-consuming. So when considering a smart card passwordless approach, organizations should also look at simplifying deployment with a strong authentication solution that is both easy for IT to adopt and doesn't saddle users with peripherals like smart card readers and other related accessories.

Finally, consider the mix of devices in your environment. If you have a bring-your-own-device (BYOD) environment or there is a mix of Windows 10 and Macs in the organization, a smart card-based passwordless approach might be best, as smart card PIV support is natively implemented on both Windows and macOS. The YubiKey can support both smart card and FIDO2 with a similar authentication flow, such that when you move to FIDO2 the user experience is already familiar.

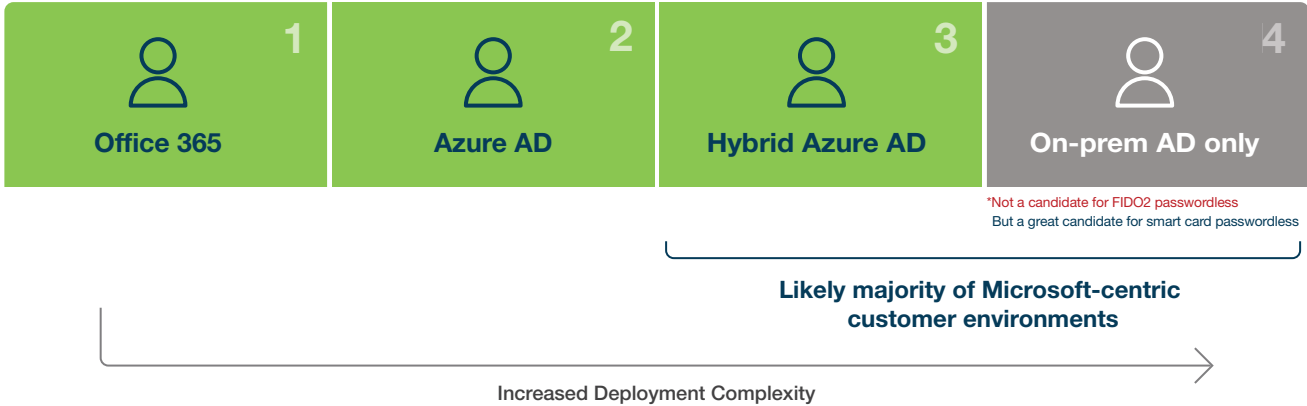
2. FIDO2/WebAuthn passwordless approach

FIDO2 is the newest (introduced in 2018) [FIDO Alliance](#) specification for authentication standards, and WebAuthn is a web-based API that allows websites to update their login flow to add FIDO-based authentication on supported browsers and platforms. This is an evolving security ecosystem that will make adopting passwordless easier. Whether you will be able to pursue implementing a FIDO2 passwordless

approach will depend on what you have in place already. If you are still operating in an Active Directory (AD) only environment with on-premises administration, then a smart card implementation is probably your best first step toward passwordless. However, if you have cloud-based applications like Office 365 or other SaaS applications (e.g. Salesforce federated with Azure AD (AAD)), and operate under AAD or a hybrid AD-AAD backend environment, then FIDO2 passwordless is something worth considering. If you are working with other Identity Providers such as Okta or Ping, you can also consider a FIDO2/WebAuthn-based passwordless approach.

One last thing to consider while pursuing a FIDO2/WebAuthn passwordless strategy is what devices and systems users are on most of the time. Typically, the organization would need to be on new Windows 10 devices and latest version of the browsers to unlock all the benefits of FIDO2/WebAuthn passwordless available today.

As mentioned earlier, modern hardware based security keys can support the range of passwordless authentication options available to organizations today. And, they can also work seamlessly with an existing IAM solution's mobile app authenticator. Some of the more familiar IAMs – Okta, Duo or Ping – are fully



*Not a candidate for FIDO2 passwordless
But a great candidate for smart card passwordless

compatible with FIDO2/WebAuthn security keys and can be used to strengthen security and gain access to a Digital Operations Platform (DOP) system. A FIDO2-compliant security key can boost security to levels that weren't available when you first implemented the IAM, when the users were possibly accessing the environment with just a password or some other weaker form of authentication.

3. Hybrid smart card/FIDO2 passwordless approach

Increasingly, customers have opted to choose a combination of two different types of passwordless approaches to create a solution that solves their passwordless needs. As an example, customers are opting to go with FIDO2/WebAuthn passwordless for computer login and federated web apps, while choosing a smartcard passwordless approach for secure remote access (RDP, VPN, VDI). In this manner organizations can adopt a passwordless strategy to map to specific use cases, given

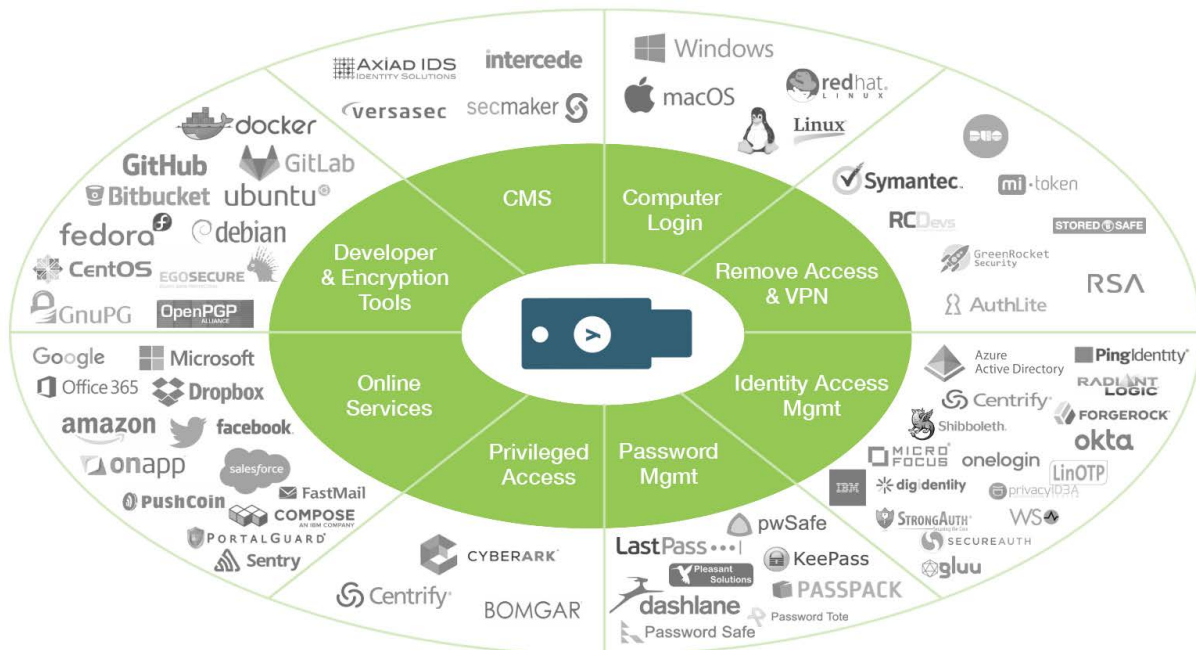
their environments and user segments. The key to remember here is that there are many roads to phishing-resistant passwordless, and all roads lead to stronger security and a better user experience, and finally, peace of mind for the organization as a whole.

YubiKey 5 Series as the bridge toward passwordless

Moving to secure passwordless is a journey and requires flexible tools that can evolve with your changing environment. The YubiKey 5 Series is compatible across a full range of environments, from legacy applications to a modern environment. There are no new software or peripheral investments to be made before integrating the [YubiKey 5 Series](#) as part of your system. In this respect, YubiKeys will act as your bridge to passwordless – supporting you every step of the way, and future-proofing your security investment as your needs continue to evolve.

YubiKey is the “bridge to passwordless”

Works with over 700+ services



The passwordless readiness checklist

Make sure you keep these seven considerations top of mind before kicking off your passwordless strategy initiatives. If you can come to the table with accurate information in these areas, you're well on your way to having a solid game plan.

Consider users and their use cases

- What are your users' needs, behaviors and risk profiles? For example, do they use mobile, desktop devices or shared workstations?

Cross-functional alignment

- Have you included all appropriate departments within your organization in planning meetings for your passwordless journey? For example, HR often may get left out of a meeting that's initiated by IT, but their input on user onboarding and training could be invaluable.

Assess existing technical environment, investments and resources

- For example, review what your current IAM provides and determine whether they are on-premises or in the cloud. How complex is your software supply chain?
- Do you have all appropriate technical resources to implement and integrate a passwordless solution?

Workforce location

- Where are most of your users located, remote or in offices, or a hybrid model?
- How will they receive any hardware they might need for access? Do you plan to handle distribution in-house or outsource the delivery and activation process?

Training and support

- How will you train and support users once you decide to go down the road to passwordless?
- Do you have a communication plan with accessible assets that will help support users?

Measurement

- How will you measure the progress and success of your passwordless deployment? What specific metrics make sense for your organization?

Additional technical services

- Would industry expertise augment and accelerate your journey?

At Yubico we've helped many companies and government entities start down the road to passwordless. [Get in touch](#) and we will help you review your Passwordless Readiness Checklist, or you can learn more about our [professional services](#) for passwordless deployment.



About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.