PASSWORDLESS AUTHENTICATION

How to Get Started on Your Passwordless Journey

WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

The goal of many security teams is to maximize security while minimizing user friction. Passwordless authentication can help you achieve that. By authenticating users with something other than a password—like push notifications that require a fingerprint on a specific device, integrated MDM solutions or hard tokens—you can gain greater assurance that users are who they claim to be.

Yet while passwordless offers a means of providing stronger security and a better experience, few have a clear understanding of how to implement passwordless in their organizations.

Much of the confusion stems from the fact that "passwordless" is not a product or a technology per se. It's more of a goal or a future state, where you're leveraging multiple technologies in ways that support your business use cases and minimize your reliance on passwords to provide better usability and security. Ultimately, the goal of passwordless is to eliminate entirely the requirement for a password in most use cases.

The Problems with Passwords

You are probably already aware of the shortcomings of passwords. But others in your organization may not be. Should you need help justifying the importance of going passwordless to the rest of your organization, here's a brief summary of the issues.

Poor Usability

No matter how you slice it, passwords present usability problems. If you choose a simple one, it will be easy for you to remember, but also easy for someone else to guess or crack with dictionary-based attacks, putting your organization at risk. On the flipside, requiring complex passwords or frequent password resets can increase security, but then the passwords become increasingly harder to remember. This introduces the likelihood that users will reuse the same password or store passwords in insecure ways, like on sticky notes.

> 80% of hacking-related breaches involve weak or compromised credentials.[1]

Friction and Cost

For consumers, every extra step they need to take during an e-commerce transaction increases the chances that they won't complete their purchase. In fact, more than one out of four customers (28%) who start the checkout process will abandon their shopping cart if they feel the checkout process is too long or complicated. If your customers can't remember the password they used on your site, their next action will often be to abandon the shopping cart rather than have to go through the forgotten password flow. While the cost of using passwords is inexpensive, the ultimate cost in terms of lost revenue can be significant.

Risk of Breach

Despite being aware of the risks, some users are still using a single password across multiple websites, one of which may be yours. This credential reuse increases your vulnerability to attacks. Credential stuffing attacks using username and password combinations available on the dark web are successful up to 2% of the time.[2] This statistic might not seem that threatening, but if you have 1,000 employees and you're relying on passwords, it can translate to as many as 20 compromised accounts.

The average cost of a data breach is $3.92 million.[3]

It's not surprising then that organizations want to move beyond passwords. Oftentimes, though, it's difficult to know where to start. This paper will help with that. Read on to discover:

- The different categories of passwordless authentication
- Where you are on the passwordless maturity model
- How to build a passwordless authentication strategy for your specific needs

EVALUATING PASSWORDLESS AUTHENTICATION OPTIONS

Every authentication factor other than a password is by definition passwordless. But not all authentication methods are created equally. To determine which options will be best for you, you need to first be familiar with the different authentication categories, the authentication options within them, and the relative strengths and weaknesses of each.

Authentication Categories

There are three basic categories of authentication factors:

SOMETHING YOU KNOW

A knowledge-based form of authentication, such as a password, a PIN or the name of your first pet

SOMETHING YOU HAVE

Such as a smartphone, RSA key, OAuth token, FIDO authenticator or email account

SOMETHING YOU ARE

A biometric factor, such as a face, retinal pattern, fingerprint, voice or EKG

As you begin to identify the best authentication factors for your use cases, you'll want to evaluate each based on its usability, security and ease of implementation.

Usability

An authentication scheme should be easily accessible and intuitive to use. If it isn't, it could end up driving customers away and causing increased employee support issues. When evaluating usability, consider:

- How much friction are your users willing to tolerate? For example, users will generally have less patience when accessing resources of low perceived value, but they'll tolerate more friction when accessing higher value resources.
- How easy is it to enroll in and use the authentication? Look at the entire lifecycle, including what's required from a user when a password is forgotten, or a phone is lost or replaced.
- How reassuring is the system? For example, users will likely feel suspicious of a banking system that lets them transfer money from their account with no visible authentication steps.

Security

When evaluating the security of different authentication schemes, you'll want to look at their resistance to both attacks and data theft. Evaluate each according to the following criteria:

- How resistant is the authentication scheme to outside attacks leading to accounts being compromised?
- Does the authentication scheme cause data to be centrally stored that if stolen could allow an attacker to compromise an account?
- How does it affect the overall security posture? Look at the security of the entire lifecycle, including registration, forgotten password or lost phone, updates to information or device, etc. A chain is only as strong as its weakest link.

Ease of Implementation

You also want to be sure that any authentication scheme being considered is a viable option for both your organization and your users. If it falls short in terms of implementation ease or cost, your success could be limited. Consider the following:

- How much effort is required to roll out the authentication scheme to the desired users?
- What are the associated costs to your organization?
- Is there a cost to the end user that could hinder adoption?

With these considerations in mind, let's examine the relative strengths and weaknesses of each authentication category.

AUTHENTICATION CATEGORIES: STRENGTHS & WEAKNESSES

Something You Know (Knowledge-based) Factors

Passwords are the most common knowledge-based factor. And they're also notoriously risky. However, it isn't the passwords themselves that are the problem, but rather users' password practices. Single-use passwords that are long and randomly generated are extremely secure. But they're also hard to remember. And this is where the poor practices come into play, including the use of easily guessed passwords like "123456" or "letmein."

Poor practices also include the use of the same password or other knowledge-based information on multiple sites. This opens up even more risk. Even if a site has excellent security, its security is only as good as the weakest system when credentials used across other sites are compromised. The stolen credentials often end up on the dark web for resale, where they can be obtained by attackers who try them on high-value sites such as banks or played back en masse against sites the attacker wants to infiltrate using credential stuffing bots.

Also of importance is how the passwords are managed. Even the most hard-to-guess password can be vulnerable if it isn't hashed, stored centrally and made available to the system where the user is logging in to verify identity. When passwords are transferred or stored in the clear, they're at increased risk of being stolen and used for account takeover. This doesn't just apply to passwords either. Any knowledge-based factor that is stored by an application provider would be at greater risk of theft.

From a cost standpoint, passwords are cheap to implement since a user directory is generally the only thing you need to purchase to support them. From an implementation standpoint, they also rate highly as they are the default authentication method for pretty much everything and there is pervasive support for them across the entire software infrastructure.

In terms of usability, passwords are mixed. Simple, easy-to-remember passwords are very usable. But in addition to the credential stuffing attacks mentioned above, they are vulnerable to brute force dictionary or common password list attacks. Long passwords are more secure but become less usable, especially if they must be updated frequently. This lack of usability can result in increased password resets, support calls, password sharing between sites and the other usability and user friction issues we mentioned at the beginning of this paper.

By comparison, a 4- or 6-digit PIN is more susceptible to brute force than passwords as there are only 10,000 or 1,000,000 possible combinations, respectively. As such, a PIN would be a poor choice as the sole factor protecting a website and should never be stored in a central location. However, if the PIN is used solely to unlock a mobile application, it would take a long time for someone to brute-force the PIN. If there is a lockout after a certain number of bad entries, security is improved even more.

From an implementability standpoint PINs are straightforward and inexpensive to implement. Since most users have no issues remembering a 4- or 6-digit PIN they also score high on usability. In general PINs are an excellent local-only stored first factor in a multi-factor scenario.

Something You Have (Possession) Factors

A possession factor (something you have) can work great—until you lose or forget it. As such, any system that uses a possession factor needs to have a fallback plan. Case in point, a large consulting provider and Ping customer reports that on any given day somewhere between several hundred to a couple thousand employees either forget or lose their phones. Since they have very stringent security requirements for access to their sensitive applications, this results in hundreds if not thousands of phone calls to the helpdesk to manually validate the employee and issue temporary credentials.

From a security standpoint, though, possession factors can be extremely effective in preventing remote attacks. The one exception is SMS texts to your phone. There have been so many instances of attackers getting mobile providers to switch a phone number to a new SIM card (called SIM swapping) that the National Institute of Standards and Technology (NIST) has deprecated the use of SMS for authentication, and we generally recommend against it if other options exist.

From a usability standpoint, possession factors also rate pretty highly. Responding to a push notification on your phone, plugging a FIDO authenticator into a USB port or clicking on a temporary link in an email are all relatively convenient. Which one is the best choice, though, depends on the particular scenario, which we will talk about in a bit.

From a cost perspective, possession factors vary widely. There is no real cost if the user already has the device, or if the possession factor is software-based. Dedicated cards or tokens can vary in cost from a couple of dollars to as high as $50 for high-end authenticators with built-in biometrics. However, these high-end devices can offer great usability, portability and resistance to phishing attacks. For example, biometric-enabled FIDO authenticators such as Feitian BioPass store your identity and a biometric in the device to confirm your identity at login. This allows true one-touch login as there is nothing for you to type in.

Something You Are (Biometric) Factors

Biometric factors are becoming far and away the most popular passwordless option. This is in part because they provide unbeatable ease of use. Fingerprint readers are now standard on most every smartphone and laptop. Windows Hello offers integration with biometric devices, while newer devices such as the iPhone X and the Microsoft Surface Book 2 provide built-in facial recognition capabilities. These platform-provided capabilities can be easily utilized as part of an authentication flow.

From a security perspective, biometrics also score highly. Fingerprint readers have a negligible false identification error rate. Facial recognition technology has also made enormous strides in accuracy, including the ability to detect attempts to login with photographs or digital images.

However, biometrics do have some weaknesses, too. From a security standpoint, if the biometric is tied to a device, for example, then it is subject to the same forgotten-device issues that a possession factor is. Storing the biometric on a central server eliminates that problem, but care must be taken with this type of data as it is considered personally identifiable information (PII) under regulations like GDPR and CCPA. In the U.S., Texas, Illinois and Washington have passed laws concerning the collection and sharing of biometric information, and several other states have proposed similar regulations.

Usability issues with biometrics also vary widely depending on the use case. For example, a fingerprint reader would be a poor choice for verifying patients who were coming to a flu clinic. Similarly, facial recognition isn't reliable if the lighting cannot be controlled. One study of facial recognition-equipped ATMs found that facial recognition accuracy fell dramatically in the afternoon at some locations. Detailed analysis found that the machines were facing windows with western exposure. As a result, the reflection of the setting sun on those windows completely washed out the facial recognition images.

Biometrics also vary widely from a cost perspective. If the platform natively provides the capability, then there is no added hardware cost for using this capability in your authentication flows. But if add-on fingerprint readers are required, they can cost $30 to $40 while add-on cameras that support Windows Hello can cost from $75 to $150.

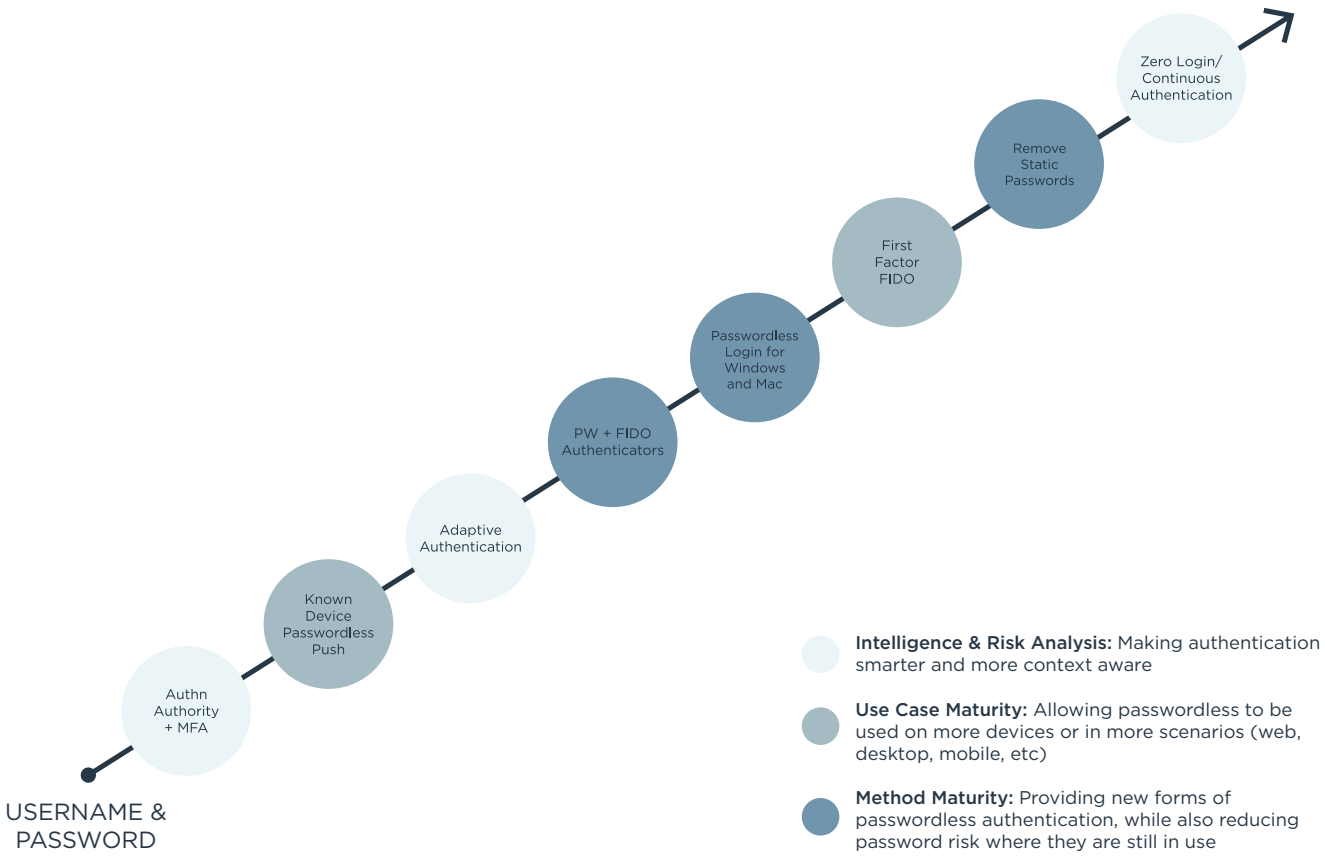
WHERE ARE YOU ON THE PASSWORDLESS MATURITY SCALE?

The passwordless journey involves a number of steps as shown in the passwordless maturity scale that follows. Each of these steps can pay dividends in usability and security. The steps on the curve are ordered based on how big an improvement in usability or security the step can make, how large an audience the step can apply to and the ease of implementation for the step.

As organizations prepare to go passwordless, a phased approach is often the most successful. The process typically starts with identifying the most critical business needs to address and selecting initial users with an eye toward gaining invaluable feedback in the initial stages of deployment. You should feel free to skip or reorder steps as needed to address your specific applications, user audience(s) and business needs.

The steps on the scale have been color coded to represent three basic themes of the passwordless journey.

PASSWORDLESS MATURITY SCALE



Step 1: Getting Started

If you're just getting started on your passwordless journey, the first step is typically to implement an authentication authority and multi-factor authentication (MFA) for all workforce applications. A global authentication authority or IDaaS service will provide you with a consistent authentication experience and give you a convenient control plane for determining which applications your users can access.

Read the paper to learn about implementing a global authentication authority.

For a workforce use case, a mobile authenticator is recommended over SMS-based OTP codes. While it is an extra step to download and register an application, a mobile authenticator has two major advantages over SMS:

- It isn't vulnerable to SIM swapping, where an attacker convinces your mobile operator to move your phone number to a new SIM card, effectively taking over your phone number.
- It works when you don't have cell coverage by providing TOTP codes that can be entered as a fallback to accepting a push notification.

For scenarios where mobile phones are not allowed, such as airline reservation or other call centers, you can use desktop authenticator applications to provide a second factor.

For consumer-facing applications and websites, you have several different choices. You generally need to offer OTP access, but you should also allow users to register their own TOTP application for authentication. If you have your own mobile application, then you can offer push notification to your application.

Critical internal systems are often accessed via VPN or SSH. To ensure you have a sound MFA baseline in place, you'll want to ensure VPNs and remote access protocols like SSH are configured to require MFA. This protection is achievable through a variety of approaches and should be added to your infrastructure security checklist.

Step 2: Reducing Password Use

Once you have the basic building blocks in place, you can start identifying opportunities to reduce password use. As a first step, you might implement known device plus push authentication. This will allow users to skip passwords when authenticating from a device that the authentication authority has seen before.

Once this is implemented for workforce, you can start rolling the same scheme out as an option for your customer-facing applications. This will dramatically increase the usability of these applications, and if you are actively selling product, this step should reduce shopping friction and shopping cart abandonment.

Read the blog to learn more about reducing customer password use.

Step 3: Implementing Adaptive Authentication

Adaptive authentication is a logical next step because it reduces authentication friction while maintaining the authentication methods that users are currently using. It can be applied to both workforce and customer authentication. Adaptive MFA works in the background to develop an active assessment of the user. This might include contextual, behavioral or correlative factors, including the geolocation, computing environment and nature of the transaction being attempted.

If policy surrounding any of these factors dictates greater security, the system can step up authentication requirements to apply the correct level of security based on the associated risk. But on the flip side, if the user is following a normal pattern, you can improve the user experience by requiring less frequent authentication. For example, you might authenticate the user once a day for the first week, then once a week for the first month, then once a month after that if they're following normal use and behavior patterns.

Read the paper to learn more about implementing adaptive MFA.

Step 4: Moving to FIDO Authenticators

At this point, you have the basics of passwordless in place and can start moving certain user groups and applications to more secure FIDO authenticators. Highly effective against phishing attacks, FIDO authentication requires that the user register the authenticator with each website that they want to authenticate with. The authenticator generates a unique public/private key pair for each website and returns the public key to the website. Authentication is only allowed over SSL, and the key is bound to the website's domain. If the user is subsequently phished to a fake website, the authentication request will fail since the attacker is not coming from the registered website domain.

Watch the video to learn more about FIDO works.

Because FIDO keys are accessed through the browser, they depend on the user's choice of browser to support the key on whatever platform the user is currently on. Until recently the availability of support for FIDO security keys was not consistent across browsers and operating systems. Now with the release of IOS 13.3, FIDO keys are supported across all major operating systems and browsers, including Chrome, Safari and Edge on Mac, Windows, Android and iOS.

Since the cost of FIDO authenticators has traditionally been a barrier, enterprises typically only require and distribute FIDO authenticators for select groups of people and for applications with the highest security needs. But as more and more platforms—like Android Version 7—implement certified FIDO authenticators, the cost will come down. This will make widespread rollout of FIDO more attractive financially and allow more employees and even customers to transition from hardware authenticators to soft FIDO authenticators.

Step 5: Enabling Passwordless Login

As you look to remove passwords from your systems, you'll also want to address login to laptops and PCs. This is typically done using the operating system's built-in biometric capabilities. Windows Hello supports both face and fingerprint biometrics for login. This can eliminate the need for passwords when combined with a locally stored PIN as a fallback. There are also commercial solutions available which will allow you to login to your desktop using your mobile device.

Step 6: Implementing First-factor FIDO

The FIDO standard allows for authenticators with biometric capability to store user identities and supply them during an authentication sequence. This is truly one-touch login. Since the identity is bound to the website and the biometric, there is no need to enter a username initially. The number of FIDO authenticators and websites that support this capability are currently limited, but strong growth in this area is anticipated in the near future. For desktop logins, some configurations of Windows Hello for business currently support using a biometric equipped FIDO authenticator to provide true one-touch passwordless login.

Step 7: Removing Static Passwords for Legacy Applications

Once you've rolled out a passwordless experience for the majority of applications and users, you can further improve the security of your remaining applications. While it would be great in theory to completely remove passwords, most enterprises will have applications and systems that require passwords for the foreseeable future.

The strategy to better secure these applications is two-fold. The first step is to wrap MFA around these applications as previously discussed. The second step—and more secure long-term strategy—is to use privileged access management and dynamic password rotation systems to eliminate static passwords and remove their theft as a possible security vulnerability. This step would also provide a passwordless user experience for the remaining applications that still use passwords, dramatically improving usability.

Step 8: Achieving Zero Login and Continuous Authentication

The ultimate expression of low-friction passwordless authentication is zero login and continuous authentication. Zero login means that the authentication authority has enough contextual factors at login time that it does not need to issue a user-visible challenge. These factors might be facial recognition, EKG or voiceprint analysis, even factors like typing analysis. If these factors can be securely gathered during initial registration, a password may never be required at all.

Continuous authentication is what happens after the initial identity is established. Using any number of factors including geolocation, IP, device posture, etc. the authentication authority determines if it has enough trust signals to balance against any risk signals given the sensitivity of the resources being requested. If needed, the authentication authority will issue challenges such as push notification or requesting use of your FIDO authenticator.

Because zero login and continuous authentication work invisibly behind the scenes, users may be concerned that the system is not secure enough, especially for high-value transactions such as transferring money from a bank account. In some of these scenarios, you may choose to retain explicit authentication in order to reassure users that the system is properly securing transactions.

CONCLUSION

You should now have a better understanding of how you can help your organization move toward passwordless authentication. You've learned about the range of authentication options available to you and are beginning to see how you can make choices that balance the security needs of your applications with the usability needs and experience expectations of your user community.

As you begin or continue on your passwordless journey, you may find it helpful to break the process down into a number of questions and gates that will guide you toward the authentication scenarios that best meet your needs. Here's a simplified checklist to help you along the way:

- ☐ What application(s) am I protecting?
- ☐ For each application:
  - ☐ How valuable is the application and its data?
  - ☐ What user communities need access to the application?
  - ☐ In what scenarios and under what circumstances do they need to access the application? Do any of these introduce special limitations?
  - ☐ What authentication method(s) meet(s) the security need?
  - ☐ Do the authentication methods work well in the desired scenarios and any special circumstances?
  - ☐ Is the deployment complexity or cost of an authentication method a significant barrier to adoption given the target audience?
- ☐ How does the usability compare for the authentication methods that meet the above requirements?

As you navigate your passwordless journey, you'll also benefit from understanding how Zero Trust and passwordless go hand in hand. Zero Trust is a security concept that addresses the realities of digital transformation and provides a framework to increase security in an increasingly open and connected world.

Zero Trust asserts that no user, system or service can be trusted, whether inside or outside the traditional security perimeter and that anyone or anything must be verified before granting access to resources. A global authentication authority is the basis of a Zero Trust architecture and provides a globally trusted single source of identity that also enables passwordless authentication.

To learn more about establishing a solid foundation for modern access challenges and requirements, get the white paper.

References

[1]2019 Data Breach Investigation Report. Verizon.

[2]Soverson, Jarrod. "What Your Login Success Rate Says About Your Credential Stuffing Threat." Shape Security Blog. April 23, 2019.

[3] 2019 Cost of a Data Breach Report. IBM & Ponemon Institute.

Ping Identity.