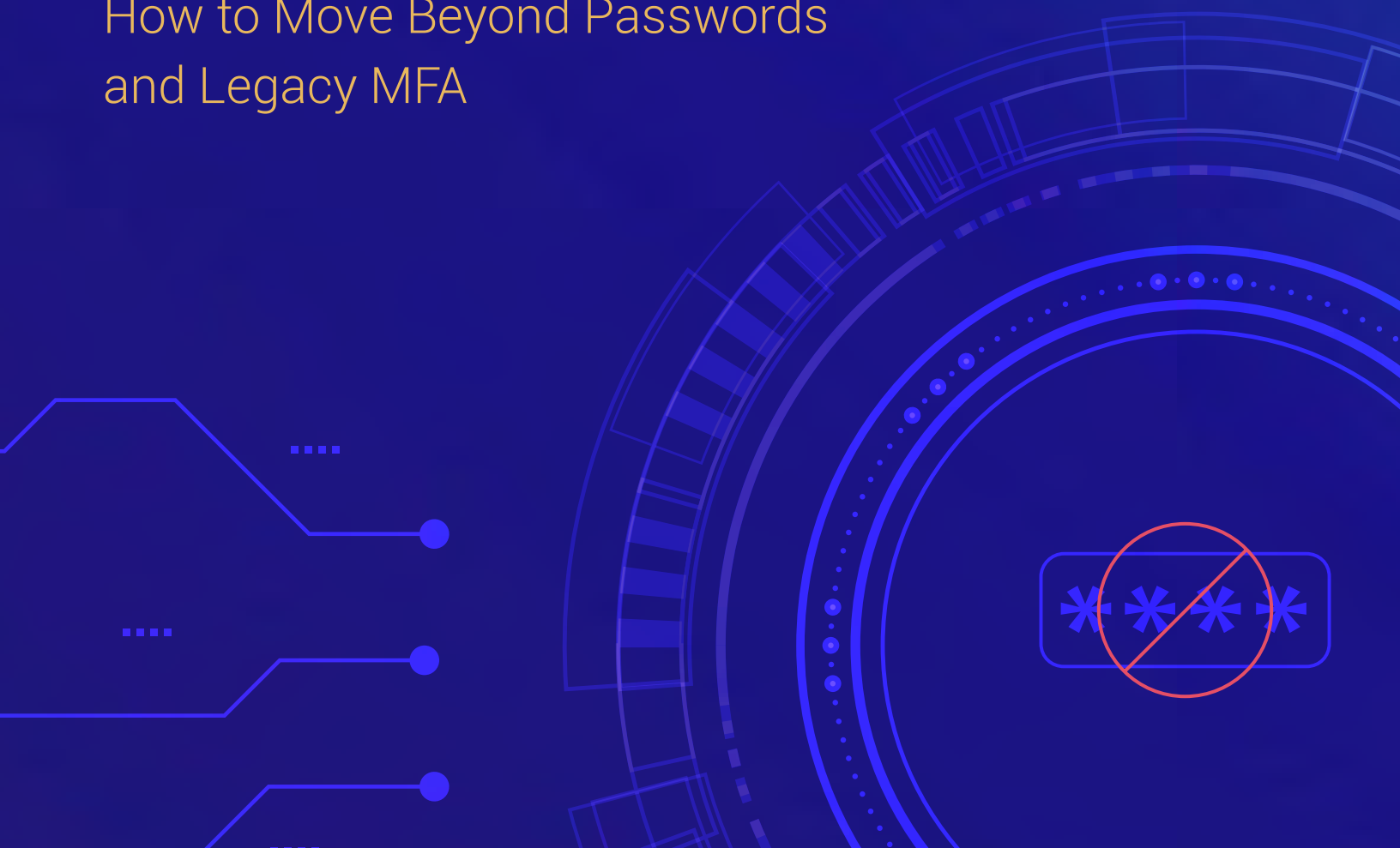


HYPR

A STEP-BY-STEP GUIDE TO BECOME TRULY PASSWORDLESS

How to Move Beyond Passwords
and Legacy MFA



Introduction

While identity challenges and IT environments can be complicated, going passwordless doesn't have to be. This step-by-step guide contains best practices and tips to eliminate passwords from your organization.

Who should read this guide?

IAM buyers, IT Managers, C-Level Executives and business leaders who are considering more secure and less friction laden authentication methods for their workforce. It doesn't matter how mature your identity program is or how many of your employees use multi-factor authentication (MFA). This guide provides an easy to understand and prescriptive roadmap to move away from passwords and legacy MFA that expose your organization to unacceptable risk.

Steps to Becoming Truly Passwordless

1. Deploy Passwordless Desktop MFA
2. Connect Your Single Sign-On
3. Disable Unnecessary One-Time Passwords
4. Secure Legacy Applications
5. Staying the Course



1. Deploy Passwordless Desktop MFA

Your workstation is the first thing you log into each day and it's the first place your passwordless journey should begin. Regardless of which OS you use, your desktop remains the front door to the workforce experience. Most companies have a large Desktop MFA gap. Think of the data that is stored on PCs and the passwords stored within the browser. Securing this highly vulnerable attack path will quickly demonstrate the biggest time to value for your organization.

What's the Impact?

- Frictionless workforce login experience.
- Removal of all passwords and shared secrets provide a higher level of security assurance.
- Faster login speeds lead to improved employee productivity.
- Alignment with regulatory compliance standards and guidance.
- An IT Team and Help desk that sees fewer password reset calls.

How does passwordless desktop MFA compare with legacy methods? Watch a video of [HYPR Passwordless MFA vs. Legacy MFA](#) for desktop login.



Tips

- Deploy passwordless MFA based on FIDO authentication standards — this is considered the gold standard for phishing-resistant authentication by CISA, the OMB and other regulatory bodies.
- Make sure the authenticator type(s) meet the needs of your user population and offer options if possible. These might be FIDO tokens in a smartphone app, security keys such as YubiKeys, or platform authenticators such as Windows Hello and Touch ID.
- Don't forget to secure virtual desktops (VDI) & roaming user logins (i.e., VPN, RDP).

Traditional MFA Methods Are Increasingly Under Attack

Employees spend up to 24 hours each year typing in passwords. Workstation login is a majority of those use cases. Desktop MFA enables your employees to log into their workstations more securely and without friction.

By adopting phishing-resistant passwordless MFA, you eliminate the vulnerabilities associated with passwords and traditional MFA methods.



33%

Increase in push notification attacks



34%

Of organizations were victims of credential stuffing attacks



89%

Of organizations experienced phishing attacks

Source: [The State of Passwordless Security 2022](#)

2. Connect Your Single Sign-On

The next step is to connect your passwordless solution for your single sign-on (SSO) provider.

If we think of the workstation as the front door to a building, then SSO is the elevator that gets your employees to where they need to go. Deploying True Passwordless MFA for your Identity Provider is critical and allows you to cover many more use cases. These include web applications, VPN, third-party applications, and other services that typically rely on passwords.

It's important that your passwordless solution supports your Identity Provider natively so that you don't need to displace any technologies or make changes to your infrastructure. In general, decoupling your identity and authentication providers eliminates lock-in or rip-and-replace scenarios. It empowers you to deploy a best in class, solutions based approach for your secured and assured operations.

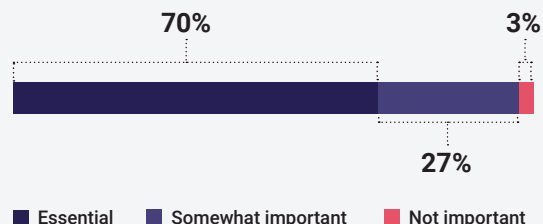
What's the Impact?

- Users don't need to remember a password for their web login
- A more productive and secure user experience
- Your employees have a single, seamless login flow from desktop through to cloud applications, with a consistent experience across devices and systems
- Eliminates virtually all password lockout tickets for IT and help desk staff

Passwordless Adoption

With SSO covering most of your applications, password-based logins across the vast majority of your systems can be quickly replaced with phishing-resistant Passwordless MFA. The key is deploying passwordless technology that is independent from identity and access management (IAM) and works across multiple IdPs.

97% of IT and security professionals state it's essential or important to for a passwordless solution to be seamlessly interoperable with multiple identity providers.

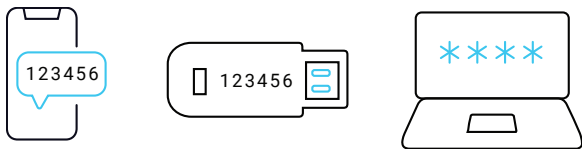


Tips

- Your passwordless solution should support open standards (such as SAML or OIDC) to easily integrate with the secure single sign-on (SSO) service(s) of your choice both now and in the future.
- Your passwordless SSO should not use centrally stored credentials or shared secrets in the verification process, even temporarily.
- Make sure your passwordless solution utilizes hardware-based security, such as ARM's TrustZone technology, Android's Trusted Execution Environments, the iOS Secure Enclave or Samsung KNOX to store keys and perform cryptographic operations.

3. Disable Unnecessary One-Time Passwords (OTPs)

At this stage, your employees are using passwordless authentication at the desktop and into the cloud. Your next step is to reduce your remaining insecure authentication points by getting rid of expensive OTP licenses. Some applications that haven't been transitioned to your SSO might still require legacy OTP at this point, but those typically make up <10% of an organization's login footprint. Remember — you can still use OTP from your existing provider, but sunsetting them reduces cost while eliminating SMS and push notification attacks. It also eliminates the user friction and fatigue that results from managing and responding to OTP alerts.



Traps to Look Out For

Calls to “Slow Down”

As your passwordless journey is progressing, an incumbent MFA vendor may suggest you slow down and try to justify continued use of OTP, SMS 2FA, or worse — stronger passwords(!). Even if you still have apps that require OTPs, you can significantly reduce your number of licenses.

Is It Really Passwordless?

Some MFA providers claim that they are passwordless, pointing out that users never type in a password or shared secret. While this may be the experience for the user, the question really is what happens on the back-end? In some cases there may be passwords or shared secrets passed behind the scenes. This is not truly passwordless and worse, it generates a false sense of security since passwords or shared secrets are still being used — and can be easily defeated.



When your legacy MFA Provider tries to convince you to keep using 2FA, SMS, or OTP, you risk push fatigue and other attacks that can bypass MFA controls.

When your leadership team finds out they can significantly reduce IAM costs while also improving authentication security, that's a win for everyone.



Tips

- Make sure that your passwordless solution does not fall back to passwords or another form of shared secret for account recovery.
- Use multiple communication channels to educate your user base on why you are making the change to passwordless authentication, explain the benefits for themselves and the organization and provide ongoing opportunities to address any concerns.
- Your passwordless solution should meet relevant privacy and security compliance requirements (GDPR, CCPA, PCI DSS, NIST 800-63) and align with guidance such as CISA and MITRE Att&ck. Check if vendors are SOC 2 and ISO certified and ask them to provide an up-to-date proof of compliance report.

4. Secure Legacy Applications

At this point the only applications remaining that aren't tied into your passwordless MFA system are legacy apps that require passwords. These might be very old financial applications, embedded systems or unsupported enterprise software.

As your passwordless apps become faster and easier than the legacy OTP login, more users will want to make the switch for all their authentication points.

Options for Legacy Applications

There are a few ways for your IAM and IT teams to bridge the gap for these password-based applications.

Add these Apps to Your SSO

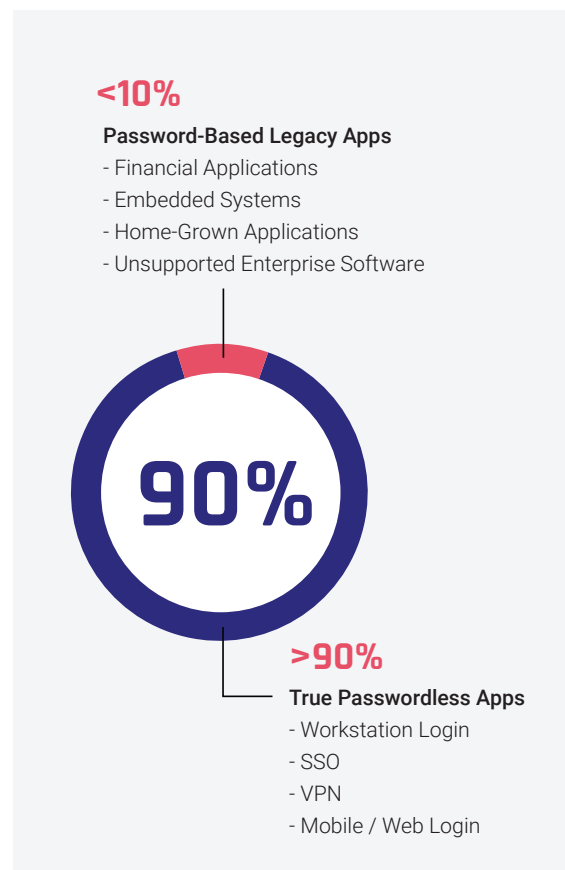
With the productivity of passwordless users measurably and visibly increasing, use the opportunity to drive the remaining applications to your single sign-on.

Replace the OTP With a Unified Identity Solution

Consider a unified identity platform (e.g., Silverfort, Strata Mavericks), which can enable legacy and customized security stacks to support Passwordless MFA. This eliminates the need to rip and replace or for custom rewrites which are error prone and time consuming. This will create a meaningfully better user experience while reducing your reliance on OTPs and Passwords.

Integrate Passwordless MFA Directly Into Your Apps

Some passwordless solutions support off-the-shelf integrations for specific applications that can't be tied into your SSO environment. They should also provide an SDK that allows passwordless technology to be directly integrated into these applications.



Tips

- At all stages, keep the passwordless implementation process purposeful and transparent. Allow your users to become familiar with passwordless before making it mandatory.
- Make sure your help desk and IT teams have the training and materials they need to help end users with setup and troubleshooting.
- Empower users with self-service and automated options.

5. Congratulations, You Eliminated Passwords

If you followed these steps, you have joined the world's most secure organizations in eliminating the leading cause of security breaches. Your users are more productive, your IT team is much more efficient, and your workforce experience has improved significantly. As you continue your passwordless journey, the important thing is to stay the course and keep from going backwards.



**Passwordless
Adoption**



Tips for Remaining Passwordless

- Don't introduce password-based login for new apps.
- Avoid password managers — they'll take you backwards.
- Don't increase your legacy 2FA/OTP footprint.
- If utilizing hardware security tokens, only use FIDO-Certified, PKI or smart-card based approaches.
- Continue to use single sign-on as broadly as possible.

Eliminate Passwords with HYPR

This guide outlines the rough steps for an organization to become fully passwordless but it rests on choosing the right passwordless provider. It's critical that your passwordless technology meet the rigorous security, usability and interoperability standards set by the passwordless standards body, the FIDO Alliance (Fast Identity Online). This is considered the gold standard for phishing-resistant MFA by the [Cybersecurity & Infrastructure Security Agency \(CISA\)](#). It's also critical that your passwordless technology partner is able to support and equip your organization on its transition.

HYPR True Passwordless™ MFA delivers the security assurance and frictionless experience organizations require, with phishing-resistant login that begins at the desktop and extends to the cloud. Designed to deploy rapidly into existing infrastructure, it turns an ordinary smartphone or other device into a PKI-backed security key.

As the only authentication system that is fully FIDO Certified across all components, HYPR is 100% committed to improving security and system interoperability. HYPR has been recognized by Gartner in its "2021 Market Guide for User Authentication" and its 2022 "Emerging Technology Horizon for Information Security" as a leading supplier of passwordless authentication. Additionally, HYPR holds SOC 2 Type 2 and ISO 27001, 27017 and 27018 certifications.

HYPR dedicates itself to the success of its customers and believes in providing a positive and productive experience — from initial deployment to ongoing technical support.

HYPR

THE IDENTITY ASSURANCE COMPANY

Contact: hypr.com/contact

Learn more: www.hypr.com

HYPR creates trust in the identity lifecycle. The HYPR solution provides the strongest end-to-end identity security, combining modern passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience.

©2022 HYPR All Rights Reserved

