

Simplifying and Strengthening Authentication with Passwordless Desktop MFA

If a password is like a house key, the security foundation of an organization's IT systems should have a securely locked front door. Make the front door as secure as possible, and you may as well never need a house key again. By implementing more complex passwords, organizations end up wasting time, money, and resources on password resets while reducing workforce productivity. Secure application login is important, however the initial authentication point for most of the workforce is the laptop, desktop or workstation itself. HYPR provides a simple yet secure login with its passwordless and phishing-resistant MFA solution, which identifies the user at the desktop and makes the front door as secure as possible. As a result, your desktop MFA can be used to seamlessly and safely log into your device, enabling access to applications in real time.



By [Alejandro Leal](#)

Content

1 Introduction	3
2 Highlights	5
3 True Passwordless Authentication	6
4 Key factors for making passwordless authentication a reality	8
5 Implementing passwordless authentication: How to move forward	10
6 The HYPR approach on passwordless authentication	11
7 Recommendations	14
8 Related Research	15
Content of Figures	16
Copyright	17

Commissioned by HYPR

1 Introduction

To ensure that the right people have access to the right data and IT resources under the right conditions is perhaps the main security objective in an organization. Traditionally, passwords were supposed to add a protection layer to the overall security of IT systems. However, when an individual uses many password-protected services, memorizing unique passwords for each platform is impractical and time consuming. It is also relatively easy to defeat with minimal effort.

Passwords are problematic, risky, and managing them is a constant headache. Organizations often require employees to comply with a long list of requirements to ensure password safety. This leads to poor user experience, costly password resets, and password fatigue in workspaces where IT departments and employees are already overburdened and understaffed.

Adding multi-factor authentication (MFA) alongside traditional passwords only increases the burden on both employees and IT teams, and organizations often struggle to enforce its adoption by their employees. MFA consists of users gaining access to a website or application by providing two or more factors in order to be authenticated: something they are, something they have, and something they know. This usually comes on top of a password.

These other factors may include PINs, mobile SMS codes, and one-time passwords (OTP). While these are certainly better than passwords alone, determined hackers and cybercriminals can exploit account-recovery systems, intercept access codes, or use other methods to bypass MFA. This is what happened in the massive Solar Winds attack and the recent attacks by the Lapsus\$ hacking group. The latter group gained access to victims through an overload of notifications and prompts via MFA applications. Despite the use of MFA solutions, individuals in organizations continue to fall victim to password-based attacks such as credential stuffing, credential theft, man-in-the-middle attacks, and phishing attacks.

Zero Trust should begin at the laptop, desktop or workstation, as this is where most users - and attackers - are entering your IT infrastructure

The spike in password-based attacks has coincided with the shift to remote and hybrid work and the deliberate targeting of remote workers. While a password-based MFA system may once have been effective enough, its viability in today's threat landscape is fundamentally diminished. As a result, many organizations are increasingly considering passwordless authentication methods that will achieve security assurance along with a consumer-grade, frictionless experience. Additionally, removing passwords reduces the help desk cost, which is significantly affected by the cost of resetting passwords.

Since the initial authentication point for most of the workforce is the laptop, desktop or workstation itself, it is essential to ensure security at the very beginning. Using a passwordless authentication solution that only works for applications and websites can leave your workforce vulnerable to serious security risks. It is evident that desktop authentication has become a critical component to the overall security posture of an organization. A passwordless authentication solution should offer a variety of secure authentication options for the desktops of an organization's workforce, ideally with the same login experience as apps.

HYPR provides true passwordless authentication that starts at the desktop and integrates with various Identity Providers (IdPs). With HYPR, organizations can protect their resources, eliminate credential reuse, and stop phishing attacks, and, at the same time, accelerate employee productivity. HYPR reduces your attack surface and delivers a seamless, frictionless authentication flow and user experience from desktop to cloud, including remote access points.

2 Highlights

- More remote and hybrid employees working outside the secure corporate perimeter and an increase in password-based attacks of all types have made it clear that traditional MFA and 2FA leave security gaps and create productivity obstacles. In response, many organizations are considering passwordless authentication solutions that will enhance security and improve user experience at the same time.
- Organizations should consider taking a phased implementation approach to passwordless authentication that is well-suited from a business perspective without disrupting operations during the transition.
- To mitigate poor user experience, MFA fatigue, and password-based attacks, securing the initial authentication point is fundamental. Therefore, desktop authentication has become an increasingly critical component of an organization's security posture.
- A passwordless authentication solution should offer secure authentication for your workforce's desktops, ideally with the same security and user login experience as for applications.
- HYPR extends the simplicity of passwordless SSO to desktop login. By using HYPR, the desktop SSO functionality can also grant access to your applications since the desktop identity has already been validated.

3 True Passwordless Authentication

Secure application login is important, however the initial authentication point for most of your workforce is the laptop, desktop or workstation itself. Attackers could steal data from organizations or launch further attacks without the use of a secure passwordless authentication solution. By adopting passwordless desktop MFA, however, users are validated at the initial authentication point, eliminating the reliance on passwords while accelerating employee productivity.

Passwordless authentication, an advanced MFA subset, has proven to be a simple yet secure alternative. However, there are varying approaches to passwordless authentication; if the passwordless solution relies on shared secrets that hackers can access, the organization will continue to face significant risks.

Today's cybersecurity threats cannot be mitigated by using traditional MFA solutions that rely on passwords. Properly implemented, passwordless authentication has the ability to provide a better user experience coupled with increased security.

True passwordless authentication solutions are based on public key cryptography (encrypted tokens including hardware and software keys) and biometrics (such as a fingerprint and face scan), or alternatively a de-centralized PIN. For MFA to be truly passwordless, shared secrets must be completely removed from the equation.

A phishing-resistant passwordless MFA (PMFA) authentication solution should have at least the following features and capabilities:

- Integrated authentication approach
- Consistent login experience across all devices
- Simple onboarding and device registration/mapping
- Replace passwords with cryptographically secure methods
- Prevent credential identity theft, identity fraud, and phishing
- Integration to access management products via standards such as SAML or OAuth/OIDC
- Frictionless user experience
- Support for industry standards such as FIDO2

Passwordless authentication cannot be achieved without completely eliminating passwords from the

authentication process. Here, the emphasis is on the authentication process and not the login procedure. Several authentication vendors claim to offer a passwordless solution, but in reality, they only provide a passwordless login experience. For example, they may use a fingerprint scan to unlock a vault-stored password, which is then relayed to the server for authentication. This means that an attacker can still use a compromised password to get into the system.

Many passwordless solutions are simply disguised passwords with extra steps that add minimal security value. For example, some solutions use OTP sent via SMS as part of their MFA authentication flow, leaving users vulnerable to phishing, fraud, SIM swapping, and man-in-the-middle attacks. Therefore, it is important for organizations to review their MFA solutions and make sure these utilize strong cryptography and do not rely on insecure authentication methods such as passwords, OTPs, or SMS tokens at any point during the login process.

Moreover, all SSO solutions only allow users to authenticate into applications and websites. By limiting passwordless authentication to applications and websites, an organization's desktops could expose its workforce to serious security risks. Sensitive information may be stored on the desktop device, there may be services and apps directly accessible from the device, without additional authentication challenges, and attackers could target a device to gain entry into corporate networks.

Desktop authentication is a critical component of the overall security posture of an organization. If done right, web applications that come later will have the same level of security, assurance, and login experience as the desktop. Hence, implementing passwordless MFA at the desktop leads to a true Single Sign-On user experience.

As organizations continue to embark on their passwordless authentication journey, it is crucial to adopt a solution that replaces passwords with public-key encryption, offers full support for FIDO standards, provides a smooth and fast user experience, stops credential stuffing and phishing attacks, and makes the front door of the workforce as secure as possible.

4 Key factors for making passwordless authentication a reality

The adoption of passwordless authentication should encompass authentication both at the application and desktop level seamlessly. While different organizations face different challenges when implementing certain technologies, the transition to a passwordless solution does not have to be an arduous process and can make your organization more secure.

Today, organizations face several challenges associated with traditional MFA. Data breaches and stolen credentials are rapidly increasing in scope, frequency, and sophistication. Even though organizations continue to spend millions to improve security, legacy MFA solutions have left workstations wide open and vulnerable to attacks.

Deploying new security can often feel daunting and takes time and effort. While a phased approach is recommended, deploying passwordless MFA can be accomplished in hours to days rather than weeks to months.

To successfully meet regulatory compliance, reduce costs, and improve user experience, a true passwordless desktop authentication solution is critical. It is important to note that transitioning from a legacy MFA system to a passwordless MFA solution is generally understood to be a phased approach.

Organizations need to consider a step-by-step implementation approach that is well-suited from a technical and business perspective. How, where and when to deploy passwordless authentication heavily depends on an organization's business model, industry standards, and requirements.

Here are six key factors for making passwordless authentication a reality:

1. Implementing a consistent and secure approach for passwordless authentication (e.g., using secure elements, all users authenticate in one consistent way with the aim to minimize friction)
2. Delivering a strong level of usability, convenience, and manageability (e.g., easy deployment, simple device onboarding, registration and change of devices)
3. Integrating it with existing systems and processes (making it work with, e.g., AD/AAD, VPNs, SSO and Access Management Solutions, certificate-based AuthN, etc.)
4. Mitigating lateral movement and always verifying for Zero Trust. Providing a much more fine-grained, secure, and modern alternative to legacy MFA is a perfect quick win on the road towards ZTA adoption (e.g. recurring authentication)

5. Simple approaches for offline access or in an emergency (device lost)
6. Option to use passwordless MFA without having to rely on a smartphone, if required

In general, a passwordless strategy should be designed together with a Zero Trust strategy. To support government agencies and other organizations on their journey toward zero trust, the Cybersecurity and Infrastructure Security Agency (CISA) adopted a Zero Trust Maturity Model in 2021. The model provides the requirements necessary to support the development, implementation, enforcement, and evolution of security policies in an organization. Zero Trust is not a technology but a paradigm that applies beyond IT to every aspect of the company's organizational and business processes. The passwordless journey must begin with a clear and long-term business strategy that aims to integrate new solutions while maintaining the continuity of business operations.

Zero Trust helps to redesign your cybersecurity architecture to function consistently and holistically across multiple IT environments and systems

The migration from a legacy MFA system to a passwordless MFA solution can make an enormous difference in remaining competitive and surviving in a fast-changing world. Organizations should strive to build a modern security architecture, which must be underpinned by adequate technical solutions. If successfully implemented, organizations will remain competitive, secure, and compliant.

5 Implementing passwordless authentication: How to move forward

In addition to establishing a long-term business plan, implementing an alternative to passwords requires a strategic approach. It is important to consider your business needs for the future to ensure that a passwordless MFA strategy will support these wider strategies going forward.

The passwordless journey involves several steps, each of which can result in substantial improvements in the security of an organization. However, in all cases, a consistent approach, where all users authenticate in one consistent way, should be one of the principal objectives in order to minimize friction and improve user experience.

By taking this approach, organizations can carefully assess the best way to conduct the initial stages of deployment. Any replacement authentication system will likely need to interact with more than just the systems your organization physically owns and directly manages. It should also form a key part of your architectural strategy for interacting with infrastructure, existing solutions, and 3rd parties.

To help your organization move forward in your passwordless journey and reduce its reliance on passwords, here are some recommendations.

Step-by-step guidance:

- Choose a vendor that understands all your key systems and meets the demands of your customer / user base.
- Understand your corporate strategies for Zero Trust, BYOD, remote work and ensure your passwordless/MFA strategy will enable these wider strategies.
- When planning a migration to passwordless MFA, it is important to keep authentication independent from their identity provider (IDP) or identity and access management (IAM) in order to reduce complexity and lock in.
- Implement a consistent approach, where all users authenticate in one consistent way with the aim to minimize friction and improve adoption.
- Ensure that the solution is certified by FIDO end-to-end rather than only a part of the solution. Do not be sold by provider claims of being "FIDO compliant" or "FIDO like."

If planned and implemented properly, a new passwordless solution has the potential to be a strategic and security advantage to your organization. Therefore, it is important to look for trusted advisors and competent vendors that will understand and support your business requirements during the course of your passwordless authentication journey.

6 The HYPR approach on passwordless authentication

HYPR's approach to passwordless MFA is designed to be a simple and secure way to eliminate passwords and shared secrets, enable organizations to reduce user friction, stop phishing attacks, reduce fraud, and deliver strong security. HYPR provides a seamless and frictionless authentication flow from desktop to cloud, including remote access points.

Founded in 2014, HYPR is a global company with offices in North America, EMEA, and Asia. HYPR's mission is to fix the way the world logs in to deliver uncompromising assurance and consumer-grade experience. With HYPR, secure logins can be performed with its passwordless phishing-resistant MFA solution that uniquely identifies users before they even enter the network.

HYPR offers a desktop MFA solution, which in many cases eliminates the need for additional authentication steps that are inconvenient for employees, such as logging off and on again to single sign-on / identity providers or applications such as Microsoft 365. Although the capability of desktop SSO has usually been limited to Windows environments, HYPR is the first vendor to offer passwordless desktop SSO for both macOS and Windows. In addition, other solutions in this market segment only target access to, e.g., cloud services, but not the initial access. Thus, the entire path from initial access to a system such as a desktop PC, and forward to backend services, can be protected at multiple levels.

The elimination of passwords is recognized as an important goal by the security industry. However, it remains challenging to achieve this goal without widespread adoption and support for standards like FIDO and OAuth. As a member of the FIDO Alliance, HYPR replaces the use of passwords with Public Key Cryptography and open standards such as FIDO2. Consequently, HYPR's solution easily integrates and eliminates passwords across Windows, MacOS, and Linux machines, as well as virtual desktops (VDI).

HYPR's strength is derived from the support for the entire flow from desktop authentication to backend applications, and the utilization of the established FIDO2 standards as well as strong cryptographic algorithms.

By using Public Key Encryption (PKE), HYPR's solution eliminates shared secrets and reduces the possibility of an attack. In order to do this, the solution uses two cryptographic keys: a private key kept secret on the user's mobile device at the hardware-level, and a public key stored on the HYPR True Passwordless Server. HYPR's passwordless MFA technology transforms a regular smart device into a secure FIDO authenticator while improving productivity and reducing the total number of authentication steps.

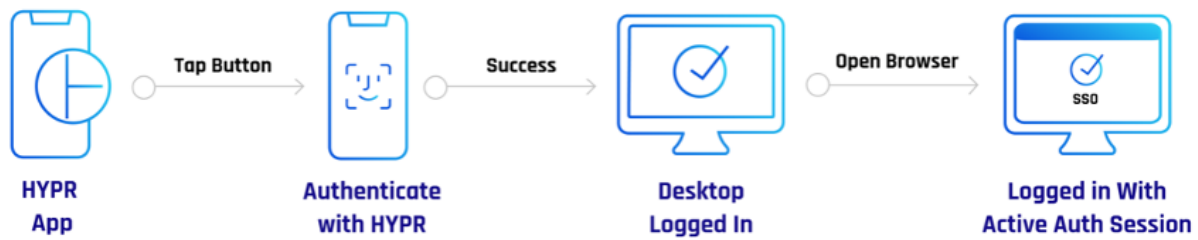


Figure 1: Login Flow with True Passwordless Desktop [Provided by HYPR]

The solution allows users to authenticate their identity using their mobile device's native biometrics, decentralized PIN, security keys, and platform authenticators built into existing devices such as Windows Hello, Touch ID, as well as FIDO authentication tokens such as Google Titan and YubiKey. The HYPR app also provides public key encrypted offline PINs for safe yet simple authentication when there is no internet connection available.

Unlike Windows Hello or similar authentication methods, where passwordless login is only possible on one device and with one user account, HYPR supports roaming users and shared devices. Since HYPR can authenticate multiple users on the same device, it is also possible to switch from the standard user context to a privileged user context without logging off and on again.



Figure 2: Authentication Flow [Provided by HYPR]

HYPR's passwordless solution enables organizations to fully leverage their Microsoft Azure environment. By integrating Azure Active Directory and HYPR, you can provide your workforce and customers with a modern passwordless experience across cloud apps. For organizations that rely on Active Directory authentication -- still most organizations -- this provides excellent integration.

Furthermore, HYPR's model of decoupling authentication from the Identity Provider (IdP) makes the solution a perfect fit for organizations that leverage multiple IdPs for their cloud apps as well as on-premise applications. Its integration with existing Identity Providers, including Okta, Ping Identity, ForgeRock, OneLogin, Azure AD, and more, gives organizations the option to use HYPR as one streamlined Passwordless Authentication solution, offering the same seamless login experience to their users from desktop to cloud. By incorporating HYPR with SSO, users can log in faster and more securely than with traditional password-based MFA.

Legacy MFA solutions that rely on passwords have demonstrated several problems in the past, such as increasing security risk and vulnerability to password-based attacks. As a result, organizations must adapt to new threats and incorporate new authentication technologies. HYPR provides a solution that eliminates the need for passwords and multiple push authentication requests while maintaining a frictionless and seamless authentication flow.

In sum, HYPR counts amongst the leading-edge solutions for passwordless authentication. By securing the initial authentication point, HYPR's passwordless desktop MFA solution offers several secure authentication options for desktop login while achieving an unprecedented level of security and productivity. The solution removes attack vectors associated with shared secrets and improves the security posture of your organization. If implemented correctly, it will dramatically improve your business processes and users' experience.

7 Recommendations

Although any type of MFA is an improvement over the use of a password, if it relies on shared secrets that hackers can steal, your organization will be subject to considerable risks. When migrating to passwordless MFA, talk with your incumbent IT vendors and understand their vision for "passwordless" and how it can be integrated with existing infrastructure in a passwordless manner for your company's needs.

While there are many things to look at and do, there are some key recommendations:

- **Identify your organization's needs:** Carefully analyze the long term strategic goals of your organizations and determine whether adopting a passwordless authentication solution will support your business needs going forward.
- **Work with your incumbent system vendors:** As part of any migration to passwordless MFA, understanding whether their vision for "passwordless" and how to interface it with existing solutions in a passwordless manner matches your corporate needs.
- **Consider implementing a phased implementation approach:** Follow a step-by-step methodology that replaces traditional MFA providers with passwordless solutions in accordance with your business model.
- **Be aware of existing limitations:** Be critical of the passwordless hype and make sure that a vendor's solution is a good fit for your organization's long term prospects.
- **Select the right passwordless solution:** A passwordless authentication solution should provide an easy deployment, consistent login experience across all devices, integration with SSO, support for FIDO standards, and eliminate the dependence on passwords or other easily phishable factors.
- **Choose an appropriate deployment model:** As you decide what solution to incorporate into your organization, it is important to make sure that it meets your requirements. Especially the elasticity and scalability necessary to support digital services.

8 Related Research

[Leadership Brief How to Get Rid of Passwords - Today?](#)

[Leadership Compass Access Management](#)

[Leadership Compass Enterprise Authentication Solutions](#)

Content of Figures

Figure 1: Login Flow with True Passwordless Desktop [Provided by HYPR]

Figure 2: Authentication Flow [Provided by HYPR]

Copyright

©2022 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.