PASSWORDLESS SECURITY EVALUATION GUIDE

12 Key Considerations for Assessing Passwordless Multi-Factor Authentication (PMFA) Solutions

About this Guide

Organizations of all sizes and across all sectors are looking to passwordless authentication to make their authentication processes more secure while reducing friction. And for good reason. Nearly two-thirds of all breaches and all ransomware attacks start with credential theft and account compromise. Passwords are one of the key targets for attackers, largely because they are easy to steal and typically stored in one place.

True passwordless authentication keeps out those who shouldn't have access while making sure the right people can get in seamlessly — and it's the single strongest security measure you can implement to keep your organization, your users and your customers safe.

But the passwordless authentication landscape can be challenging to navigate. Not all solutions are created equal, and terminology can be confusing or even misleading. Some don't meet compliance requirements. Some may meet technical definitions but are still vulnerable to attack. And many have hidden costs in the form of lengthy and complex deployment, extensive and time-consuming training and support and vendor lock-in.

Gartner calls passwordless authentication a critical information security technology to adopt now.[1]

This guide will help you discern among available passwordless security products and determine which solution best suits all the needs and requirements of your organization. This guide is intended for:

- IT and system administrators
- Identity and Access Management (IAM) architects
- Security teams
- CIOs
- CISOs
- Anyone interested in better security

What You'll Learn:

- The biggest authentication security risks
- A comprehensive set of criteria to evaluate passwordless solutions
- Alignment of password authentication with compliance, certification, and standards
- Advancing your Zero Trust security model with passwordless authentication
- How to determine your total cost of ownership (TCO)

Where Do You Start?

Before you begin evaluating passwordless authentication vendors and solutions, it's critical to assess both your current and future security needs. As with any tool in your security stack, you need to weigh the risks, costs and your specific requirements. Consider these questions as a starting point.

Requirements	Risks	Cost
○ Are you in a highly regulated industry or sector? ○ Does your cyber insurance require you to have MFA? ○ What kind of sensitive data does your organization handle? ○ Do you have multiple identity providers? ○ Do you employ a hybrid or remote workforce? ○ Does your organization interface with customers online?	○ How much business disruption would be involved in making the switch to passwordless authentication? ○ Will users embrace the new technology or resist it? ○ To what extent do you want your passwordless authentication to protect against specific threats, such as credential phishing and push attacks? ○ How developed is your cloud infrastructure, and how do passwords and shared secrets make your organization vulnerable?	○ How much have you budgeted to cover the costs for multi-factor authentication (MFA)? ○ Have you included the intangible costs of deployment, such as implementation time IT resources needed and a potential slowdown in user productivity? ○ How much do fraudulent transactions and attack mitigations cost you currently?

Introduction

As any security professional can tell you, credentials and the people that use them constitute one of the biggest security risks. Yet, organizations are still heavily reliant on password-based methods to protect access to digital accounts, data and other resources. According to Forrester, more than 55% of organizations continue to use passwords as the primary authentication method.[2]

Approximately 65% of people reuse passwords across accounts, and nearly half hadn't changed their passwords in over a year, even after a known breach.[3]

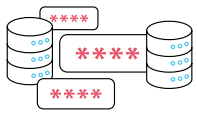
The pervasiveness of lax password practices makes account takeover trivial. It's no wonder that credential theft, is at an all time high. There's currently more than 15 billion stolen credentials for sale on various hacking forums.[4]

Credential-based attacks span a variety of methods — from phishing campaigns and credential stuffing to man-in-the-middle attacks. The Verizon 2021 Data Breach Investigations Report, found that 61% of all breaches exploit credential data and 60% of ransomware attacks begin with a compromised credential.[5]

Many organizations are adopting two-factor authentication (2FA) or MFA to strengthen their security posture, meet regulatory requirements and qualify for cyber liability insurance. While MFA certainly provides more security than passwords, it still falls short. Traditional MFA is often unwieldy, adding friction for users and IT teams. And, credentials remain at the core of most MFA solutions, making them vulnerable to attack.

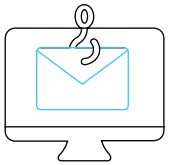
With automated hacking tools that can bypass MFA and massive credential leaks now ubiquitous, attacks will continue to rise unless organizations evolve their strategies. Passwordless authentication completely eliminates the biggest attack vector and the biggest target of hackers: credentials.

If you are looking at including passwordless authentication in your security arsenal, be aware that there are significant differences among passwordless products and vendors. This guide outlines the major features and capabilities you should be looking for, along with questions to ask potential providers. The relevance of each of these capabilities in your own evaluations will depend on the nature of your systems and business, compliance requirements and ongoing or planned strategic initiatives, such as Zero Trust.



34%

of organizations reported credential stuffing attacks



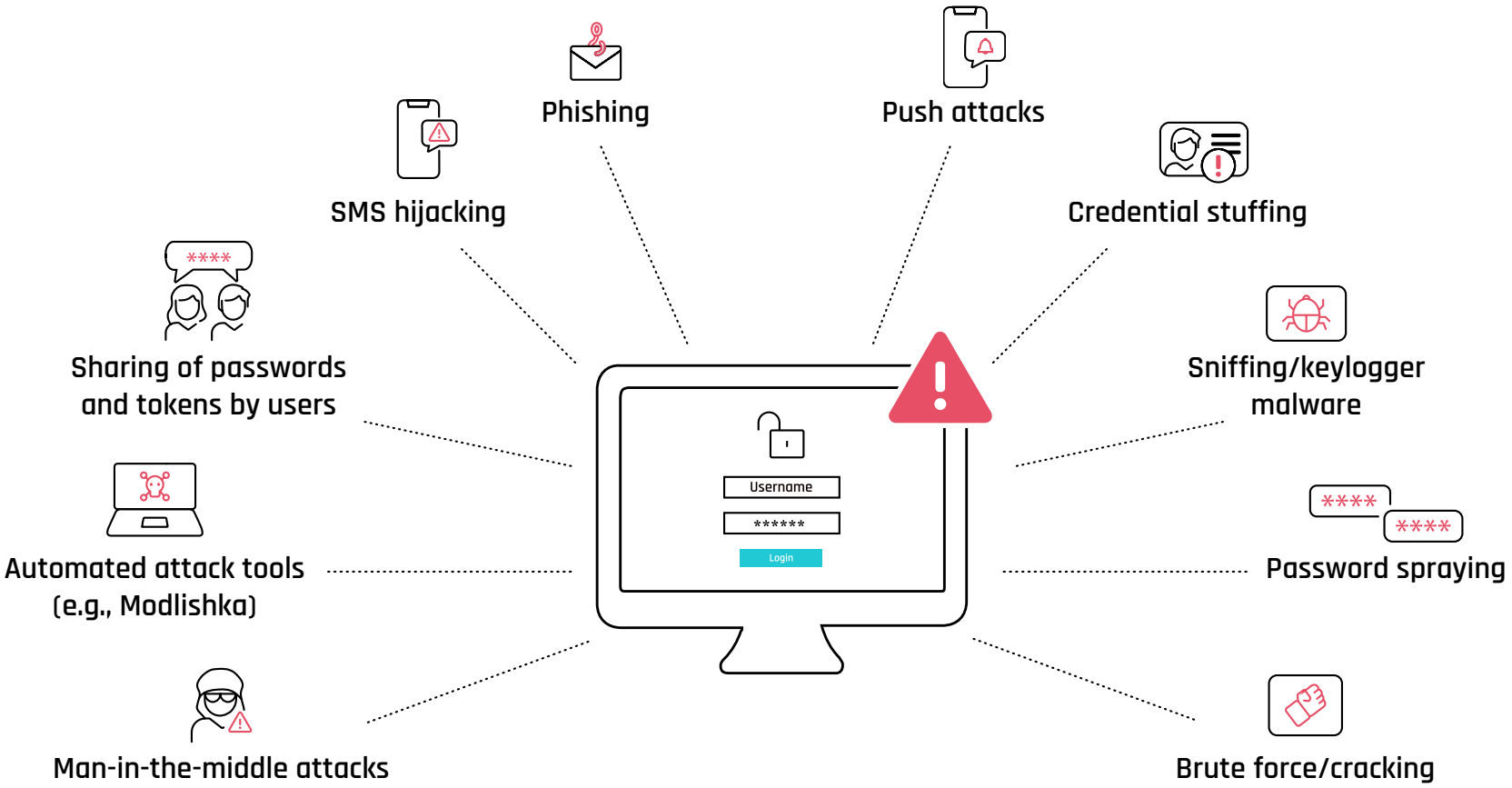
89%

of organizations experienced at least one phishing attack.

Source: HYPR State of Passwordless Authentication 2022

Top 10 Authentication Security Risks

Attackers use multiple methods to bypass passwords and traditional MFA security. These are the most common threats you need to guard against.



Core Capabilities to Look for

1. No Passwords or Shared Secrets Anywhere

Contrary to what you'd expect, passwordless authentication does not always eliminate passwords and shared secrets. Some approaches remove the password from the user's login experience for the sake of convenience, but centrally stored passwords remain part of the infrastructure. For example, they may use a biometric feature, such as Touch ID or Face ID for the login, but this simply unlocks and forwards a stored password for validation on the backend. Other solutions may send a one-time password (OTP) by SMS or email as part of their MFA flow. None of these solutions are truly passwordless multi-factor authentication (PMFA). Whenever there is a secret shared for verification, even if temporary, it is vulnerable to phishing and interception. Moreover, anytime there is a database of stored credentials, it will be a target for hackers.

True PMFA solutions are based on public key encryption. They use a private-public cryptographic key pair to authenticate a user's identity. The private key is stored in a secure enclave on a user device — a mobile phone, smart card or security key — while the public key is registered with the authenticating server. This ensures that user accounts and data stay safe, even if the server is breached. These systems also may include other verification factors, such as biometric recognition, local to the device.

65% of organizations' "passwordless" solutions actually require a shared secret, such as an underlying password, OTP or SMS code.[6]

Buyer's Tip:

Your passwordless solution should never use shared secrets, including during enrollment and account recovery.

2. Passwordless MFA for Desktop Login

Secure application login is important, as it ideally enables passwordless authentication from anywhere — any location and on any device. But if a passwordless authentication solution works only for applications, it leaves open a critical security gap for your workforce.

The initial authentication point for most of your employees is the laptop, desktop or workstation itself. Desktop authentication is now one of your most critical legal and business imperatives. Multiple regulatory bodies, including the NYDFS, CISA and the Federal OMB, are requiring affected organizations to implement MFA, and many cyber insurance companies insist on it as a requirement to obtain coverage.

Your passwordless authentication solution should offer several secure authentication options for desktops, ideally with the same user login experience as for applications. If you have cases where an employee logs into multiple desktops or multiple employees share the same computer, make sure the solution can address these situations. In addition, a secure roaming authentication capability is essential when employees are traveling or unable to connect to the internet.

Buyer's Tip:

Secure authentication for applications is not enough. To secure your workforce, you need passwordless authentication that begins at the desktop.

3. Support for Remote and Hybrid Workers

Flexible workplace policies are the norm today and nearly all organizations have a responsibility to secure their remote or partially remote and traveling workforce.

Remote working means that large numbers of employees access corporate resources through virtual private networks (VPN), virtual desktop infrastructure (VDI) and remote desktop protocol (RDP), which makes them susceptible to attacks and breaches of network security. Hardening your defenses at the point of access to these systems, such as through advanced PMFA capabilities, goes a long way toward securing your remote and hybrid workforce.

Forrester found that 75% of organizations experienced cyberattacks stemming from insecure technology deployed to cope with remote work.[7]

Secure offline access is another important consideration for remote and hybrid workers. Working remotely increases the need to unlock devices when internet coverage is patchy or inaccessible. Some methodologies, such as decentralized offline PINs available through an authenticator app, let users securely identify themselves offline and gain access to the devices they need to do their jobs.

Buyer's Tip:

Ensure that your passwordless authentication solution provides secure remote access, even when offline.

4. Integration with Your Systems, Identity Providers and Devices

As part of your preparation for passwordless authentication, you'll want to map out all the places your workforce uses passwords. Include device types (examples: Android, iOS, macOS, Windows, Linux) and login locations in addition to your identity providers (IdPs), virtual desktop infrastructures (VDIs), applications, proprietary programs and cloud services.

Many passwordless solutions either work only with specific IdPs or attempt to leverage their product to lock in organizations to their own IdP. This creates a disjointed user experience and can hamper cloud transformation initiatives. The passwordless authentication solution you ultimately end up selecting should integrate with all the major IdPs (such as Okta, Ping Identity, Azure AD, ForgeRock and others).

It should also support open standards (such as SAML or OIDC) to easily integrate with the secure single sign-on (SSO) service of your choice. Flexibility, portability and forward compatibility are essential.

Buyer's Tip:

Your authentication should be decoupled from your identity provider and integrate with a wide range of devices and services.

5. Resources Required to Deploy and Manage the Solution

An important step in planning your move to passwordless authentication is determining whether your in-house staff possesses the knowledge and skills to properly implement the solution. Depending on the solution and your team, you may need to engage professional services to support, install and test the solution and necessary integrations.

According to a recent poll, 67% of organizations contend that their staff doesn't have the needed skills and teams for adoption of passwordless authentication.[8]

Choosing the right solution can make deployment, integration and management faster, easier and less expensive. Make sure you consider the following questions as you evaluate solutions:

- Does the solution follow a standards-based approach? If that's the case, it should be trivial to integrate it with your current SSO providers.
- Is there a robust software development kit (SDK) that allows development teams to integrate the solution with custom or legacy applications not connected to your SSO?
- If regulatory obligations such as the PSD2 Strong Customer requirement impact your business, do the SDKs include built-in security controls and functions to help you meet them?
- How long will it take to deploy and enroll each user?

Buyer's Tip:

Do your due diligence in determining resources needed to rollout and manage a solution on an ongoing basis.

6. The User Experience

In this digital age, a consumer-grade experience is critical to business success — for both customers in a B2C setting and for the workforce. A recent report found that 67% of organizations say that improving user experience is a key factor in adopting passwordless authentication.[9]

User comfort with any security system plays an essential role in its successful adoption and makes it less likely that people will seek workarounds for expediency or ease. Solution providers need to make the passwordless authentication experience fast, intuitive and convenient. Ideally, there will be a single login flow — from the desktop through to cloud applications — with a consistent experience across devices and systems.

When you evaluate various passwordless authentication vendors, check to see whether their solutions can accommodate different requirements and user preferences across different demographics, verticals and industries. A sound passwordless authentication solution should provide alternatives for those who cannot or choose not to use biometrics. Ideally, the vendor will offer multiple secure authentication methods, including smartphone apps, Windows Hello, QR codes, hardware security keys and decentralized PINs.

User experience is inextricably linked to productivity. Whether applied to the workforce or for B2C applications, 73% of organizations believe that the most user-friendly and convenient method for MFA is smartphones.[10]

Buyer's Tip:

A positive and frictionless experience for every user should be a top priority.

7. Cloud Solutions: Availability, Security and Operational Processes

A security solution is only as valuable as it is available and resilient against security incidents and downtime. Some enterprises sometimes choose to deploy on-premises authentication solutions, believing they offer greater security control. However, such solutions are often less secure as it's more difficult to deploy urgent security patches.

Cloud-based authentication provides high scalability, flexbility and better integration with modern organizations' cloud applications and services. Make sure your passwordless provider maintains their solution independent from your systems. That way, even if you are breached, access to your applications is still securely managed by your provider. Check that it has mature and proactive monitoring capabilities, including automated anomaly detection.

If your business is subject to data privacy regulations, such as the EU General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), make sure the solution does not share or store sensitive or personally identifiable information (PII) in the cloud, or send users SMS codes. Any security-relevent data should be encrypted (AES-256 or stronger), with each tenant's data stored in a segregated database invisible to other tenants.

Make sure your vendor has a failover process in place, with service distributed geographically and across multiple providers and power grids.Ideally, your vendor should guarantee 99.99% uptime, backed by strong service level agreements (SLAs).

Buyer's Tip:

When assessing cloud-based solutions, ask about solution hardening against vulnerabilities and breaches, data privacy compliance and uptime guarantees.

One good test of a vendor's resilience is how quickly they respond to widespread security incidents like the recent Log4j vulnerability, which exposed all applications using the popular Java-based utility to attacks that could steal data, hijack servers and deliver ransomware or other malware.[11] Find out how long it took for vendors under consideration to test, remediate any exposure and communicate the mitigation to their customers.

8. Secure Storage of Private Keys

A passwordless authentication solution can still be vulnerable to device-side attacks by hackers, even if it uses public key cryptography. Malware, side-channel attacks and reverse engineering are among the many techniques available to attackers who want to steal the private keys of a cryptographic system. To ensure key safety on mobile devices, authentication systems should utilize 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.

Buyer's Tip:

Ask if the solution uses a device-level Trusted Platform Module (TPM) to store private keys and other sensitive data.

9. Certifications and Compliance

If your organization handles sensitive personal or payment data, make sure your passwordless solution meets relevant privacy and security compliance requirements, such as GDPR, CCPA, HIPAA, PCI DSS, NIST 800-63B and others.

In addition to adhering to compliance regulations, find out if the vendors under review hold up-to-date independent certifications. This provides assurance of their commitment to security and privacy standards and will enable you to obtain proof-of-compliance reports for your auditors. Vendors with SOC 2 Type 2 certification have had their security procedures and controls fully vetted by a third-party, independent auditor.

Various ISO certifications provide additional assurance regarding controls to ensure the confidentiality, integrity and availability of customer information; measures that reduce risk in the cloud; and data privacy and protection of personally identifiable information (PII) in cloud computing.

Finally, to further aid your organization with compliance audits, ask your vendor if they create an audit trail that reports data on authentications across mobile devices and workstations, along with errors that may have occurred.

Buyer's Tip:

Ask your vendor to supply up-to-date certifications and reports on their compliance with current regulations.

10. Total Cost of Ownership

As you contemplate the move to passwordless authentication, another area that needs to be considered is the total cost of ownership (TCO). The TCO encompasses deployment resources and management costs in addition to the initial dollar investment.

Other points to consider are productivity impact for employees and how successfully the solution reduces authentication-related help desk issues. For example, solutions that utilize a smartphone-based authenticator app generally have fewer help desk calls as users are less likely to forget or lose their smartphone.

Another critical question to ask a vendor is whether their passwordless authentication solution integrates with your legacy systems and preferred identity provider(s). Will the solution enable you to integrate and streamline fragmented authentication processes and identity systems?

Authenticator costs are another TCO consideration. Do you have to purchase, manage and administer hardware authentication devices? For mobile authenticators, confirm if there is any per-device cost or if an unlimited number of enrolled devices is permitted for each user license.

Data center costs are an often-overlooked expense of an on-premises authentication solution. With a cloud-based solution, you don't have to absorb the associated management costs.

Buyer's Tip:

Get a general idea of costs in your initial exploration and really dig into details when it comes time for a request for proposal (RFP).

11. Use of Open Standards Throughout

The FIDO (Fast IDentity Online) Alliance aims to improve cybersecurity with open standards that are more secure than passwords, SMS and OTPs, simpler for consumers to use, and easier for service providers to deploy and manage. The Cybersecurity & Infrastructure Security Agency (CISA) considers FIDO the gold standard for MFA. A FIDO Certified solution leverages public key cryptography for authentication and adheres to usability and interoperability standards to aid user adoption and ensure compatibility with other FIDO Certified products.

Some vendors claim that they are FIDO compliant or support FIDO, but this does not guarantee the same security, usability and interoperability as FIDO certification. It's also possible for a provider to have FIDO certification for its validation server, but not for its authenticator. This means their server has the ability to accept external FIDO Certified authentication verifiers but that the solution's client itself does not meet FIDO standards.

FIDO standards match guidance from these organizations and cybersecurity statutes, ensuring built-in compliance:

- NIST (800-63B)
- Federal Financial Institutions Examination Council (FFIEC)
- U.S. Federal Office of Management and Budget (OMB)
- PSD2 Strong Customer Authentication

Using a solution that is FIDO Certified on all of its components helps future-proof your authentication strategy. To determine a passwordless authentication solution's certification status, you can check FIDO's registry of certified technologies here.

How Critical Is FIDO?
Today, FIDO standards are the most widely adopted standards in the passwordless industry. Advocates include Mastercard, Apple, Microsoft, Samsung and others.

fido™ CERTIFIED

96%

say FIDO is important

Source: HYPR State of Passwordless Authentication 2022

Buyer's Tip:

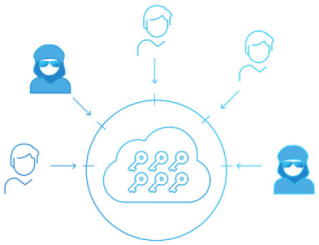
Make sure your vendor is fully FIDO Certified across all solution components.

12. Zero Trust Best Practices

Zero Trust is a security model that has gained tremendous traction worldwide. The core concept is simple: never trust anyone or any device. Zero Trust requires that the identities of all users and devices that try to access resources on a corporate network always be verified and that access needs are limited to the appropriate role.

A cornerstone of any Zero Trust initiative is phishing-resistant MFA. Under Zero Trust, MFA is the network gatekeeper — and the strength of that gatekeeper affects the security of the entire Zero Trust architecture. Unfortunately, some organizations find gaps in employee MFA adoption, especially among those who work remotely or travel often. The friction of forcing employees to juggle multiple authentication steps creates adoption hurdles that slow down the Zero Trust initiative as a whole.

Zero Trust With Passwords



- Low to Moderate Levels of Assurance (LOA)
- Higher operational costs
- Gaps in MFA adoption
- Vulnerable to credential-based attacks
- Slower overall program rollout
- Constraints on IT infosec resources

Zero Trust Without Passwords

- High levels of assurance (NIST AAL3)
- Lower operational costs
- Rapid scaling of MFA adoption
- Resistant to phishing and credential-based attacks
- Accelerated program cycles
- Reduce IT/IAM resource constraints

FIDO Certified passwordless authentication helps your organization enact Zero Trust principles, without a negative impact on the user experience. It builds trust into the user's identity, ensuring that authentication processes align with the highest level of assurance (NIST 800-63B AAL3) for Zero Trust initiatives. CISA, the Federal OMB and other compliance regulators strongly recommend technology based on FIDO and WebAuthn standards.

If Zero Trust is part of your security strategy, true passwordless authentication can bring this transformation about more quickly, at a lower cost, using fewer resources and with stronger, more reliable levels of security and compliance.

Buyer's Tip:

Even if your organization has no plans for a formal Zero Trust initiative, you should implement the framework's widely accepted best practices for authentication.

Additional Factors

You now have a solid basis for evaluating the ideal passwordless authentication solution for your organization. Once you have asked the hard questions about everything from capabilities to compliance to costs, there are still a few important things to consider. After all, you will be entering into a critical, long-term security relationship, so make sure you examine the vendor as thoroughly as the solution.

Research the vendor's reputation. Check analyst research from Gartner, Forrester and other industry experts to compare how the vendor rates against competitors and what their strengths and weaknesses are from an independent third-party perspective.

Make sure the vendor provides regular release updates and has a proven track record of responding to customers' needs in terms of fixes, features, protections and system coverage.

Ask your vendor for customer references that you can contact directly to gain insights on their experiences with the company and the solution. Talk to their customers about the responsiveness of the vendor's technical support and development teams.

Also, find out about speed of deployment and the time and resources involved in management and maintenance. Can and will your chosen vendor help you navigate the optimal deployment for your organization? Does your vendor have extensive, proven experience and skills in the field and especially in your industry sector and environment?

Buyer's Tip:

Inquire about customer satisfaction scores and retention rates. If a provider keeps their customers happy, it's a good indication that they will be a reliable security partner for you.

HYPR Checks All the Boxes and Then Some

HYPR's True Passwordless™ multi-factor authentication (PMFA) platform is designed to eliminate the traditional trade-off between security and a seamless user experience. It turns an ordinary smartphone or other device into a PKI-backed security key for frictionless, phishing-resistant login from desktop to cloud. Think of it as a hardware token like a YubiKey inside the device you already use.

A fully FIDO Certified authentication system, HYPR also serves on the board of the FIDO Alliance and is 100% committed to improving security and system interoperability. Our cloud-based solution is architected for 99.99% availability, and we deliver 100% monthly uptime for the majority of our customers. 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. Onboarding is straightforward and streamlined — new employees can be productive their first day on the job.

"After looking at countless authentication products, we decided that the best way to address our cybersecurity issues was HYPR's passwordless multifactor solution."

Joe Kynion, VP/Information Technology Officer
First Citrus Bank

Sources:

1 Gartner, Emerging Technology Horizon for Information Security, Published 16 November 2021

2 Using Zero Trust To Kill The Employee Password, Forrester Research, Inc., August, 2021

3 Psychology of Passwords, LogMeIn, August, 2021

4 From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover, July, 2020

5 https://www.verizon.com/business/resources/reports/dbir/

6 The State of Passwordless Security 2022, HYPR, January, 2022

7 Forrester, Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work, September 2021

8 https://www.forbes.com/sites/forbestechcouncil/2021/11/23/whats-blocking-the-adoption-of-passwordless-authentication/

9 The State of Passwordless Security 2022, HYPR, January, 2022

10 2021 State of Passwordless Security Report, HYPR, February, 2021

11 https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

See how passwordless MFA can secure your workforce and customers.

Visit: hypr.com/demo

About HYPR

HYPR fixes the way the world logs in. HYPR's true passwordless multi-factor authentication (PMFA) platform eliminates the traditional trade-off between uncompromising assurance and a consumer-grade experience so that organizations decrease risk, improve user experience and lower operational costs.