PRODUCT BRIEF

HYPR Solution Overview

Phishing-resistant MFA that empowers employees and customers to access accounts and systems faster, easier and more securely

Protect Access While Removing Friction

Modern organizations need to eliminate authentication-based threats while delivering a seamless user experience across all channels, from anywhere. HYPR is the recognized leader in passwordless, phishing-resistant, multi-factor authentication and is deployed at scale in some of the largest and most complex environments globally.

The Failure of Traditional MFA

The vast majority of security incidents can be traced back to a weakness in authentication. Legacy MFA cannot protect organizations as it has proven vulnerable to push bombing, MitM, phishing, smishing, password stuffing and other credential attacks. Furthermore, traditional IAM technologies force organizations to choose between security and usability, with more secure options introducing friction that negatively impacts user satisfaction and productivity.

Organizations are vulnerable unless they make a change. Passwordless MFA is the only way to break this cycle.

HYPR – Fixing the Way the World Logs in

HYPR provides the strongest authentication combined with a simplified user experience that accelerates business at scale. HYPR's frictionless, phishing-resistant MFA is certified by FIDO, which the Cybersecurity and Infrastructure Security Agency (CISA) considers the gold standard for Zero Trust Authentication. By deploying HYPR, organizations can decouple authentication from their identity providers to ensure best of breed technology and one consistent login experience.

How HYPR Authenticate Works

HYPR Authenticate replaces shared secrets such as passwords, PINs, SMS codes and OTPs with strong public key encryption based on the FIDO passkey standard. Biometric sensors such as Apple Touch ID, Face ID, and their Android and Windows counterparts, can be used to unlock these credentials that are verified against an authentication server using public key cryptography.

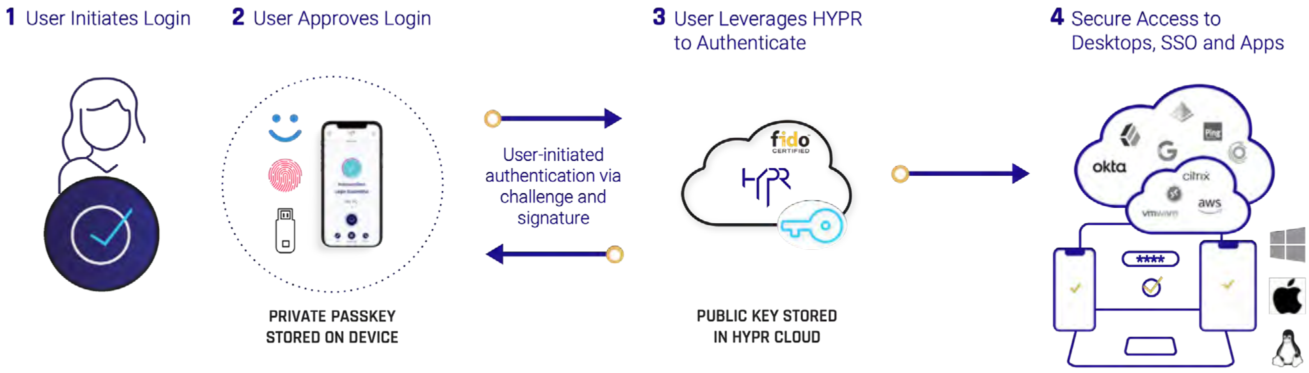
HYPR Key Benefits

- Solve your desktop MFA gap
- Stop credential phishing, fraud and account takeover with secure, modern authentication based on the FIDO passkey standard
- Combat identity fraud and reduce risk through sophisticated analysis of contextual information, real-time events, and user behavior
- Improve productivity and reduce password reset tickets by 95%[1]
- Integrate quickly with existing systems, IdPs and applications
- Deploy mature, enterprise-proven passwordless MFA that delivers validated ROI of 324%

[1] The Total Economic Impact™ Of HYPR True Passwordless MFA, Forrester Research, July 2023

At registration, HYPR securely generates a pair of cryptographic keys. The private key is stored on the user's mobile device at the hardware-level in the secure, isolated Trusted Execution Environment (TEE). The public key is stored on the HYPR Server. Simply put, it's like turning a smartphone into a FIDO2 Certified token. HYPR also works with any other FIDO Certified authenticator, such as hardware keys and smart cards, to provide flexibility and choice for users who cannot or choose not to use a smartphone.

Private Key Always Remains on User Device


1 User Initiates Login
2 User Approves Login
3 User Leverages HYPR to Authenticate
4 Secure Access to Desktops, SSO and Apps
User-initiated authentication via challenge and signature
PRIVATE PASSKEY STORED ON DEVICE
fido CERTIFIED
HYPR
PUBLIC KEY STORED IN HYPR CLOUD
okta
citrix
aws
vmware
****

HYPR Solution Components

HYPR Authenticate App

HYPR offers a lightweight mobile app that replaces passwords with passkey-based authentication that's 300% faster than traditional MFA. The HYPR App works across multiple user devices, providing secure login anywhere, even offline.

HYPR Desktop Client

The HYPR desktop client solves a serious yet common authentication gap. Eliminate passwords and shared secrets across Windows, MacOS and Linux workstations, including shared workstations and consoles. Comply with regulatory mandates and security framework guidelines for MFA at the desktop. Users gain single action login from desktop to SSO and cloud apps, including virtual desktops, VPN and RDP.

HYPR Control Center

Manage, provision, and deploy passkey-based authentication policies across millions of users with the HYPR Control Center. HYPR enables you to manage FIDO authenticators at scale, easily customize enrollment and create authentication policies, and monitor real-time user and system analytics and audit logs.

HYPR Adapt

HYPR Adapt provides real-time risk assessment and adaptive security controls so you can easily and effectively manage identity-related risks, even in rapidly changing security environments. Its powerful risk engine consumes and analyzes risk signals and telemetry from numerous sources, including user behavior analytics and contextual information from mobile, web and browser signals, and dynamically adjusts authentication security policies in response.

Results can be used to enforce step-up authentication as well as shared with SIEM, SOAR and other enterprise systems for additional enforcement or reporting actions. Detailed insight into individual risks enables your organization to deliver a personalized user flow that is optimized to reduce friction while maintaining stringent security measures.

HYPR SDK

With the HYPR SDK, embed frictionless, secure, regulatory-compliant authentication into your mobile and web applications. Give users the fastest login experience and achieve maximum security on any device. Gain a competitive advantage in business by accelerating deployment and time-to-market. HYPR's SDK supports both synced and device-bound passkeys.

Passwordless Authentication Based on the FIDO Passkey Standard for Workforce and Customers

HYPR covers both your workforce and your customers to ensure the highest levels of phishing-resistant security across all user populations. Modern CISOs, CIOs, COOs, IAM, IS and IT leaders look to HYPR to reduce the total cost of ownership of their IAM stack and align their security, usability, and efficiency goals. HYPR is proven to deliver 324% ROI and reduce employee onboarding time by 55%.[2]

HYPR Features and Benefits

Eliminate the Target

With HYPR, there is no centralized database of passwords or shared secrets that can be hacked. Credentials in the form of a private key are stored and remain in the most secured areas of the user's device at all times. This combination changes the economics of attack, making the target unattractive for attackers to even attempt.

Add Risk-Based Authentication Controls

HYPR Adapt employs a powerful risk engine that enables dynamic adjustments of security policies in response to real-time risk assessments. This feature ensures that access controls are flexibly tailored to each user's unique context and dynamic threat landscape. By continuously adapting security measures based on the latest risk evaluation, organizations can maintain a granular and personalized security posture, mitigating risks effectively and minimizing the potential for unauthorized access or breaches.

Deploy the Gold Standard in Authentication, End-to-End

The HYPR solution is FIDO2® Certified end-to-end. FIDO is considered the gold standard for phishing-resistant passkey based authentication by governing organizations such as CISA, NYDFS, OMB and others. Many solutions claim "FIDO-support" and "FIDO-compliance," which only suggests a basic level of interoperability. Others are only FIDO Certified in a single component, such as the server. HYPR is certified on all components to ensure organizations adhere to the latest FIDO specifications.

Secure Logins Desktop to Cloud

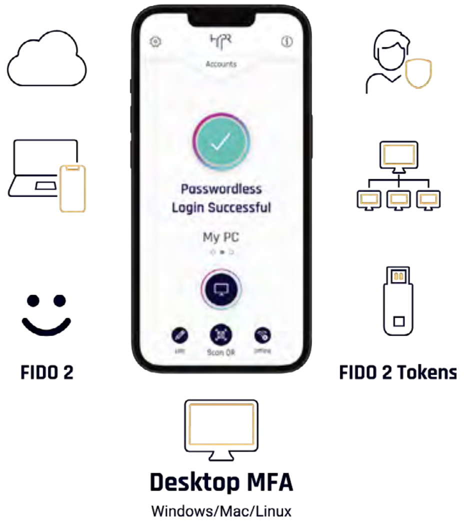
Users authenticate with HYPR when they first log into their device and it carries them through all login operations. In a single authentication operation, users get phishing-resistant, passkey-based MFA access to their device, data, local and cloud applications.

The average person performs 26 daily logins. HYPR reduces this to a single operation. There are no more passwords to remember, no downtime from being locked out and no calls to the helpdesk for password resets.

Full Integration Today and for What's Next

Eliminate passwords across Windows, MacOS, and Linux machines, as well as virtual desktops (VDI) and virtual private networks (VPN).

Many organizations manage multiple SSOs and identity providers such as Okta, Ping and Azure AD. HYPR integrates with all major providers, decoupling the authentication process so you don't get caught in vendor lock-in and users gain a unified authentication experience. Deploy best-of-breed technology and extend the investment in your existing infrastructure.



[2] Forrester Research

Bring Legacy Apps Into The Passwordless Era

Legacy and proprietary applications traditionally pose a challenge in updating to current authentication standards. HYPR partners with identity orchestration providers so even the oldest applications and most customized security stacks can seamlessly use passwordless MFA.

Passwordless Anywhere, Including Offline

HYPR Offline Mode ensures passwordless MFA is available even when connectivity isn't. Offline Mode leverages a secure decentralized PIN that allows your mobile workforce to safely log in from anywhere.

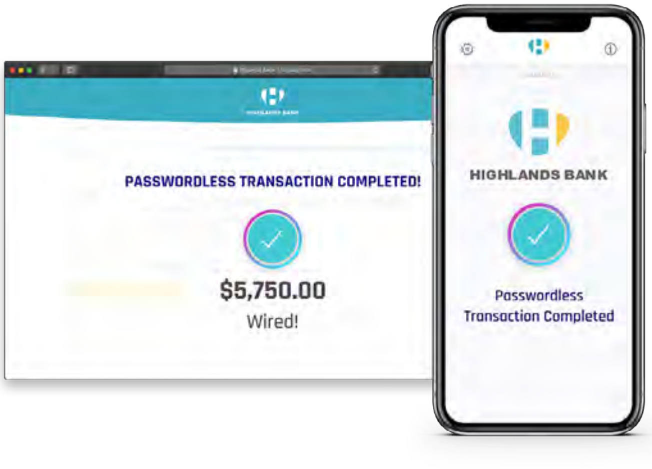
PINs are stored in the device secure element and can only be used once. Administrators choose to activate this feature along with the PIN definition, number of PINs permitted and validity period. Each time the user successfully authenticates online, new PINS are generated, and all current PINs discarded.

No OTPs Ever

Users securely invoke authentication on their mobile device; OTPs are never used in HYPR's authentication process. With HYPR you eliminate MFA attacks and breaches including push attacks (MFA bombing), OTP-interception, man-in-the-middle, replay attacks, credential stuffing and social engineering. It also means no time lost to typing in passwords, tokens, OTPs or other cumbersome legacy MFA methods.

Secure Customer Authentication

HYPR's secure passwordless customer authentication gives your users a consistent mobile-to-web login experience and accelerates transaction velocity with passwordless transaction approval. HYPR is scalable to millions of transactions per minute and addresses PSD2 SCA requirements, including cryptographic signing of every transaction and unique dynamic linking. HYPR performs under pressure so you can handle usage spikes as well as growing demand.



PASSWORDLESS TRANSACTION COMPLETED!

$5,750.00

Wired!

HIGHLANDS BANK

Passwordless Transaction Completed

Meet Compliance Requirements

HYPR does not use passwords, PINs or shared secrets that could violate data security mandates. Each user's cryptographic material, including authentication keys and biometrics, is stored in the trusted platform module (TPM) on their device. HYPR helps you align with official industry guidance for phishing-resistant MFA and meets and exceeds MFA requirements set by the NYDFS, the FFIEC and other regulatory bodies.

Why HYPR

HYPR combines open standards, best-of-breed security and a fast and consistent user experience to deliver a proven, fully scalable authentication solution for your workforce and customers. HYPR protects your users, services and brand reputation now, with the flexibility and forward compatibility to meet future evolving conditions.

HYPR has a demonstrated track record securing organizations globally, with deployments in some of the most complex and demanding environments, including 2 of the 4 largest US banks, leading critical infrastructure companies and other technology-forward businesses. HYPR's solutions have been independently validated to return a 324% ROI.

HYPR

THE PASSWORDLESS COMPANY

www.hypr.com | hypr.com/contact