HYPR True Passwordless™ MFA

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 threats to their IAM processes while delivering a seamless user experience across all channels, from anywhere. HYPR ensures secure, frictionless, phishing-resistant authentication that makes both security teams and end users happy.

HYPR is the recognized leader in True Passwordless™ 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 problem with authentication. Passwords and shared secrets are the weakest link in the authentication chain, creating an entry point for various threats including credential stuffing, brute force, and phishing attacks.

Traditional multi-factor authentication does not solve the problem as it relies on passwords and compromisable factors. The sheer number of MFA breaches prompted CISA, OMB, FTC, NYDFS and GDPR to all come out with guidance stating traditional MFA is not secure and organizations should move to phishing-resistant, passwordless MFA.

HYPR — Fixing the Way the World Logs in

HYPR's True Passwordless™ MFA provides uncompromising security together with a consumer-grade experience. HYPR's frictionless, phishing-resistant MFA conforms to FIDO specifications, 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.

HYPR Key Benefits

- Solve your desktop MFA gap

- Stop phishing, fraud and account takeover

- Enable fast, easy login for employees and customers

- Eliminate password resets and improve productivity

- Integrate quickly with existing systems, IdPs and applications

- Deploy mature, enterprise-proven passwordless MFA

Keys Always Remain on User Device

How It Works

In HYPR's True Passwordless architecture, the use of shared secrets such as passwords, PINs, SMS codes and OTPs are replaced with public key encryption. 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.

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 True Passwordless 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, to provide flexibility and choice for users who cannot or choose not to use a smartphone.

HYPR Platform Components

HYPR App

Deploy True Passwordless MFA across your organization with the lightweight mobile app to eliminate passwords with the push of a button and deliver authentication that's 300% faster than password-based MFA.

HYPR Desktop MFA Client

HYPR's Desktop MFA client solves a serious yet common authentication gap. Eliminate passwords and shared secrets across Windows, MacOS and Linux workstations. Once a user registers their smartphone they gain secure and frictionless access to desktops. Single Sign-On (SSO), web, VDI, VPN, RDP and more.

HYPR Control Center

Manage, provision and deploy passwordless authentication policies across millions of users with the HYPR Control Center. HYPR enables you to manage FIDO authenticators at scale, and integrates with your existing online fraud detection and risk engine.

HYPR True Passwordless SDK

Integrate the True Passwordless SDK into 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 with HYPR.

Eliminate Passwords For Both The Workforce & Customers

HYPR delivers True Passwordless MFA for both your workforce and your customers that ensures the highest levels of phishing-resistant security across all your 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 Features and Benefits

Eliminate the Target

With HYPR, there is no centralized database of passwords or shared secrets that can be hacked to gain access to everything. 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.

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 passwordless 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 until they shut down. In a single authentication operation, users get phishing-resistant MFA access to their device, data, local and cloud applications.

The average person performs 26-plus daily logins. HYPR slims this down to a single operation. There are no more passwords to remember, no downtime resulting 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, Azure AD and more. 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 of your existing infrastructure.

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.
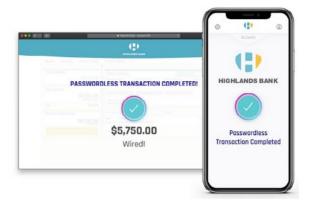
No OTPs Ever

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 passwordless customer authentication performs under pressure so you can handle usage spikes as well as growing demand.

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's True Passwordless Security leverages open standards, combined with best-of-breed security, and a user experience that's unparalleled in speed and ease of use.

Organizations face a multitude of problems with passwords and legacy MFA, cutting across security, operations, productivity, engagement and user adoption. Moreover, as history has demonstrated, security threats, business climates and operating environments are all dynamic. HYPR delivers a proven authentication solution that 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 with deployments in some of the most demanding and secured organizations in the world including finance and banking, critical infrastructure, government, nonprofit and more.

THE PASSWORDLESS COMPANY

Email: info@hypr.com
Learn more: www.hypr.com

HYPR fixes the way the world logs in. HYPR's True Passwordless™ multi-factor authentication 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.