HYPR Solution Brief

HYPR Passwordless Desktop MFA

Get seamless, secure authentication that begins with initial endpoint login and carries through to all downstream resources. HYPR's True Passwordless™ multi-factor authentication secures your access points everywhere, from desktop to cloud.

Most authentication and authorization systems are geared toward controlling access to enterprise systems and services. Access to the endpoint itself — laptop, desktop, workstation, console or server — is often protected with only a password. This leaves a major security gap as passwords and weak two-factor authentication lead to the vast majority of breaches.

The Overlooked Login

When it comes to authentication, IT and security teams typically focus on logging into accounts, such as email or applications. However, before these operations can occur, users must first log into their desktop, laptop or console. Yet, we rarely consider the potential security risks that can occur by someone defeating our desktop access, which usually has only a password standing between your systems and malicious intrusion.

Why Desktop Security Is Critical

Logging into a desktop provides access to a myriad of data and applications. Users may save confidential data or files on the local drive; there may be passwords for sites and applications stored or cached in the browser; communication apps on a device, such as WhatsApp or Slack, can be used to elevate attacks. The often overlooked attack vector is our first login of the day — the desktop.

HYPR Protection Begins With the Initial Login

HYPR provides phishing-resistant, passwordless MFA that starts at the desktop login. Instead of logging in with a password, users invoke authentication using their smartphone or other designated device as a FIDO token. A biometric is used to verify user identity and authentication takes place using public key cryptography. The private key remains securely stored in the TEE or secure enclave — no password or shared secret is ever passed. Organizations with Windows Hello for Business can leverage HYPR to eliminate passwords from the authentication process while still using the Windows Hello-generated biometric to gain access.

HYPR follows protocols considered the gold standard for authentication security and forms a key pillar of the Zero Trust model. At the same time, it makes login frictionless and fast for your workforce and removes the burden of resets and other password support issues.

HYPR Key Benefits

Uncompromising Security Assurance

- Deploy seamless phishing-resistant MFA from the desktop to the cloud
- Stop phishing, fraud and account takeover
- Satisfy cyber insurance requirements and security and data privacy regulations
- Cover all your use cases, including remote employees and shared workstations

Consumer-Grade Experience

- Improve the authentication experience for your workforce
- Eliminate password resets and improve productivity
- Integrate quickly with exisiting systems, IdPs and applications
- Onboard new employess in minutes

Desktop to Cloud, for Windows, Mac and Linux

As organizations migrate to phishing-resistant, passwordless authentication, it is crucial to cover all authentication scenarios — from desktop to cloud. The average person performs over 23 discrete logins to their desktop, accounts and applications. HYPR takes the original authentication from the desktop and makes all subsequent authentication requests seamless and invisible to the user. This creates a "continuous authentication" security environment that is frictionless to the user while securing previously unaddressed attack vectors.

HYPR is the only solution providing passwordless desktop SSO for both macOS and Windows, as well as Linux-based VDIs, protecting users across the vast majority of desktops, laptops and other endpoint devices.

Remote Lock

Locking an unattended workstation is a critical security measure, yet many people forget or deliberately neglect it to avoid re-logging in. With HYPR, users can remotely lock the desktop from anywhere using their HYPR-enabled device. Moreover, login is so quick and seamless that it cuts down avoidance behaviors.

Offline Access

Many "desktops'' are laptops, tablets or other portable devices. Users may need to access their systems when traveling or other times when they do not have reliable connectivity. HYPR provides an offline access mode which relies on securely generated one-time PINs stored in the TPM or secure enclave.

Integrations

The strength of your security stack depends on your various security technologies working together and never locking you into a sub-optimal choice. HYPR integrates with leading identity providers (IdPs), SSOs and other security vendors. This ensures forward compatibility, so your organization is prepared to address new security challenges, new environments and new initiatives as they happen.

Essential Desktop Passwordless MFA Requirements

- Deploy seamless phishing-resistant MFA from the desktop to the cloud
- Zero passwords or shared secrets
- Continuous authentication technology
- No lock-in but fully integrated with exisiting deployed technology
- FIDO Certified end-to-end
- Adherence to Zero Trust model

HYPR
THE IDENTITY ASSURANCE COMPANY

www.hypr.com
hypr.com/contact

HYPR creates trust in the identity lifecycle. HYPR Identity Assurance provides the strongest end-to-end identity security for your workforce and customers, combining phishing-resistant passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience. HYPR's solutions have been independently validated to return a 324% ROI.