HYPR

PASSWORDLESS REMOTE WORKFORCE

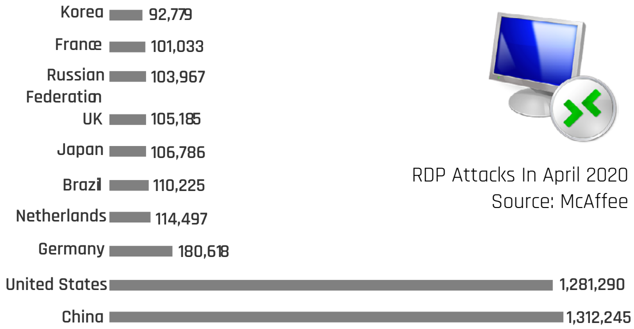
A How-To Guide by HYPR

Remote Work is at an All Time High – and So are Credential Reuse Attacks

Credential theft and phishing have skyrocketed in recent years as most organizations shifted to remote work. According to ESET research, there was a 768% increase in RDP attacks targeting remote workers in 2020. The number of Virtual Private Network (VPN) users also increased by more than 54% in 2020, while MFA adoption remained relatively flat. The success of MFA adoption depends greatly on its usability. It's no surprise remote MFA experiences are due for an upgrade.

The problem is that passwords have always protected the front door. So what do businesses do when that front door is no longer under their control? They add layers on top of the password – creating friction and forcing users to log in multiple times throughout their day. That friction was tolerated when remote access was infrequently used by few members of the workforce – but not anymore. A remote-first workforce requires a new approach to authentication.

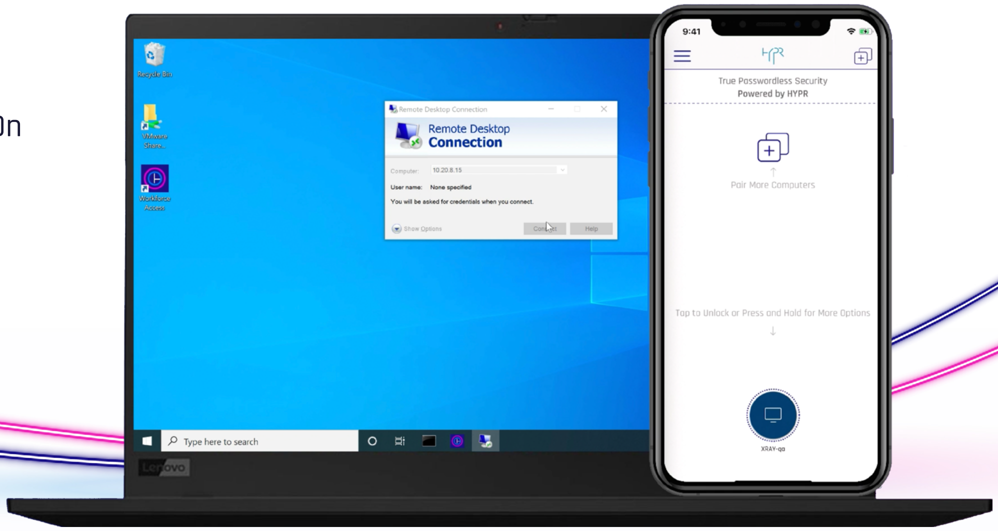
True Passwordless MFA disrupts that model and replaces it with a remote login experience that is fast, consistent, and easy to use. This guide provides a high-level overview of how to achieve passwordless security with HYPR.



RDP Attacks In April 2020
Source: McAffee

3 Steps to a Passwordless Remote Workforce

1. Solve Your Desktop MFA Gap
2. Connect Web & Single Sign-On
3. Secure RDP & VPN Login


Remote Desktop Connection
Computer: 10.20.8.15
User name: None specified
You will be asked for credentials when you connect.
Show Options
Connect
Help
Type here to search
9:41
True Passwordless Security
Powered by HYPR
Pair More Computers
Tap to Unlock or Press and Hold for More Options
XRAY-qa
Lenovo

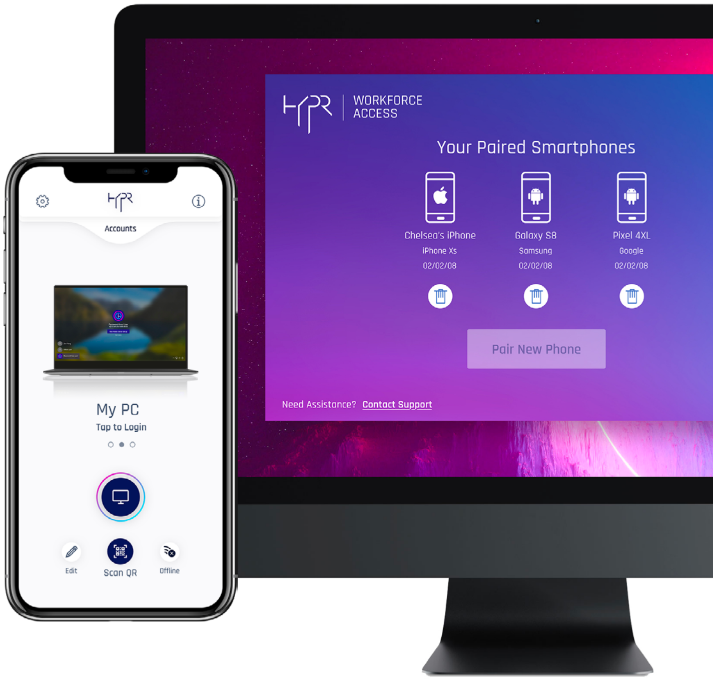
1 Solve Your Desktop MFA Gap

Your workstation is the first thing you log into each day, and your remote team depends on fast and easy access for productivity. Whether it's a Windows 10, 7, or MacOS workstation, your desktop remains the front door to the workforce experience. But did you know most companies have a large Desktop MFA gap?

That gap was overlooked when the employee was more or less "in the office" – but what about when teams are working from your home, traveling, or in a public area? Passwordless desktop MFA provides everything you need to deliver passwordless MFA for Windows and Mac machines to your entire workforce. The HYPR App provides easy user onboarding and is available for Android and iOS. Onboarding is simple, and the HYPR App takes just a minute to install with a QR code and is then ready to use for mobile, web, and workstation login.

Turn Your Smartphone into a Smart Card

By combining public key encryption with lightning-fast authentication, HYPR's True Passwordless Desktop MFA enables mobile-initiated login to workstations through your mobile device. It's fast. It's easy to use. And it's FIDO-certified®.



Stop Push Attacks with Mobile-Initiated Login

HYPR is the only provider to enable passwordless login that begins on a mobile device. With mobile-initiated login, HYPR stops PUSH attacks, MITM, replay, credential stuffing, brute force, and social engineering – before they happen. These innovations are just some of the reasons why enterprises choose HYPR to eliminate passwords.

Go Passwordless Anywhere with Offline Mode

Secure a roaming workforce with Offline Mode, which leverages a secure decentralized PIN to ensure your mobile workforce can log in anywhere – whether they're in transit, on an airplane, or underground.

WATCH VIDEO

2 Connect your Web & Single Sign-On

The next step is to enable HYPR for your Single Sign-On (SSO) providers. If we think of the workstation as the front door to a building, then SSO is the elevator that gets your employees to where they need to go. Deploying True Passwordless MFA for your Identity Provider (IdP) is critical, and by activating True Passwordless SSO, many more use cases are now covered. These include web applications, Virtual Private Networks (VPN), Virtual Desktop Infrastructure (VDI), third party applications, and other services that typically rely on passwords.

HYPR supports your IdP out of the box so you don't need to displace any technologies or make changes to your infrastructure. Simply activate your IdP in your HYPR Control Center, and invite your users to enroll HYPR for their SSO.

✓ Streamline passwordless experiences across web and mobile apps with plugins for Okta, Azure AD, ForgeRock, Ping Identity, FusionAuth, and more

✓ FIDO®-Certified end-to-end security

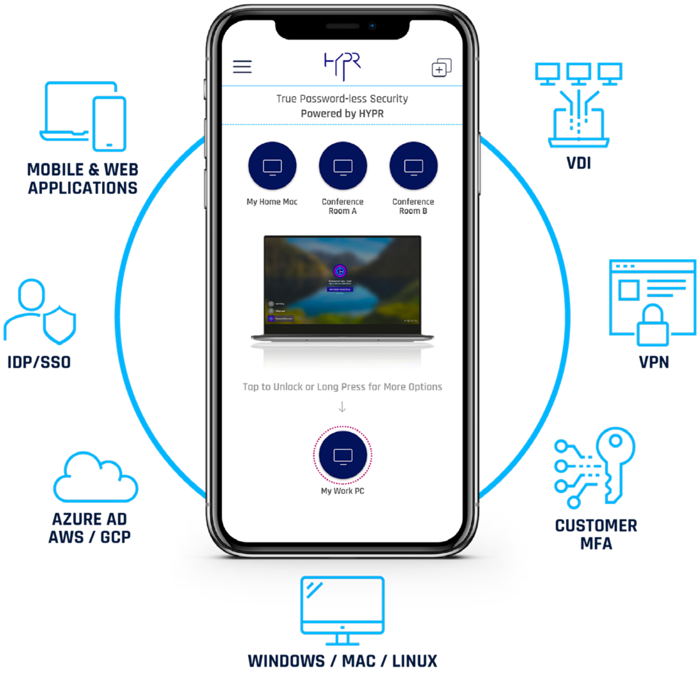
✓ Cloud-native deployment

✓ Smart card and Yubikey interoperability

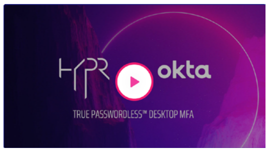
✓ Unify fragmented login experiences with a single app for all web and workstation use cases

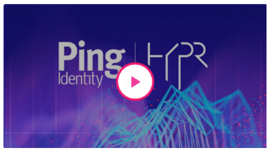
✓ Leverage certified integrations with leading virtualization platforms such as Citrix Store & VMware

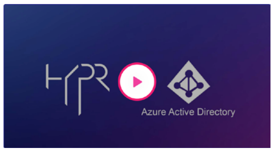
✓ Extend MFA across enterprise uses cases such as VPN and VDI using open standards: RADIUS, SAML, OpenID



See True Passwordless SSO in Action >







> “Most legacy ‘MFA’ tools are really only ‘+1FA’ tools, adding a single extra factor to a legacy password.”
>
> **- Gartner**
> 2020 Market Guide for User Authentication

3 Secure VPN & RDP Login

With an 87% increase in the number of remote workers in 2020, more people than ever are using Virtual Private Networks (VPN), Virtual Desktop Infrastructure (VDI), and Remote Desktop Protocol (RDP) to access corporate resources. Legacy MFA ultimately defeats your organization's security and productivity at the user and administrator levels. This is compounded in instances where teams are working remotely.

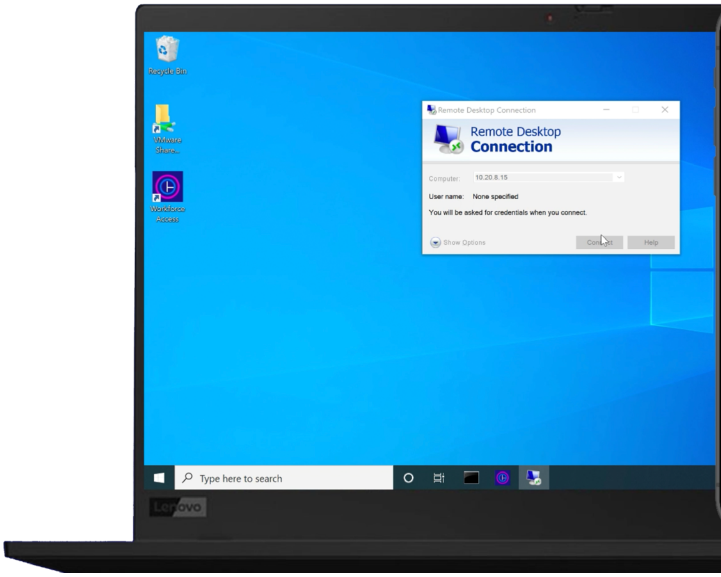
Here are three key reasons why legacy MFA based on shared secrets and passwords fail to support a remote workforce:

- Passwords and shared secrets expose people to credential reuse and phishing attacks
- Passwords and legacy 2FA are costly and cumbersome to use, which is why the desktop MFA gap exists
- Disparate MFA login experiences reduce productivity and fragment the login journey across desktops, applications, and remote access tools

HYPR provides True Passwordless MFA for VPN, VDI, and RDP login, eliminating the use of passwords and shared secrets. The result is a login experience that's protected against brute force attacks, credential reuse, and phishing.

HYPR replaces the use of passwords and shared secrets with Public Key Cryptography and open standards such as FIDO2. This involves using a pair of cryptographic keys: a private key that's kept secret on the user's mobile device at the hardware-level, and a public key that is stored on the HYPR Server.

It's like turning your smartphone into a smart card.

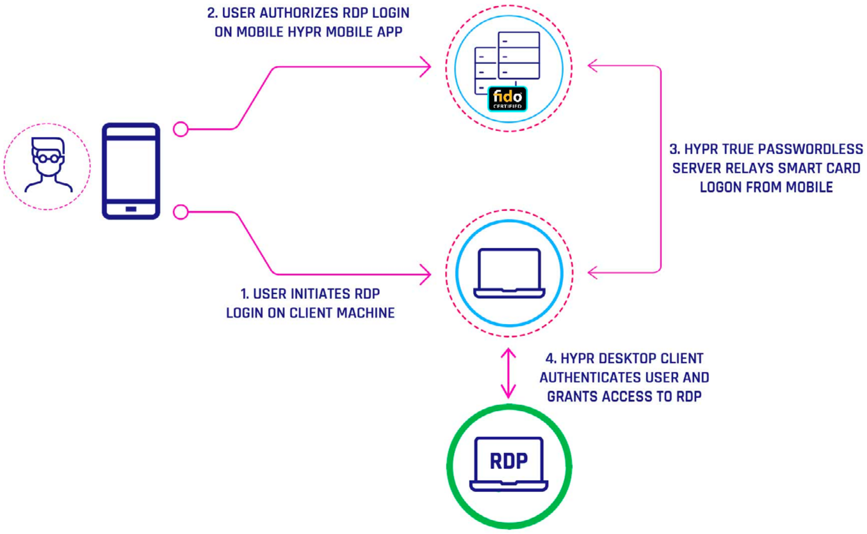


Computer: 10.20.8.15

User name: None specified

You will be asked for credentials when you connect.

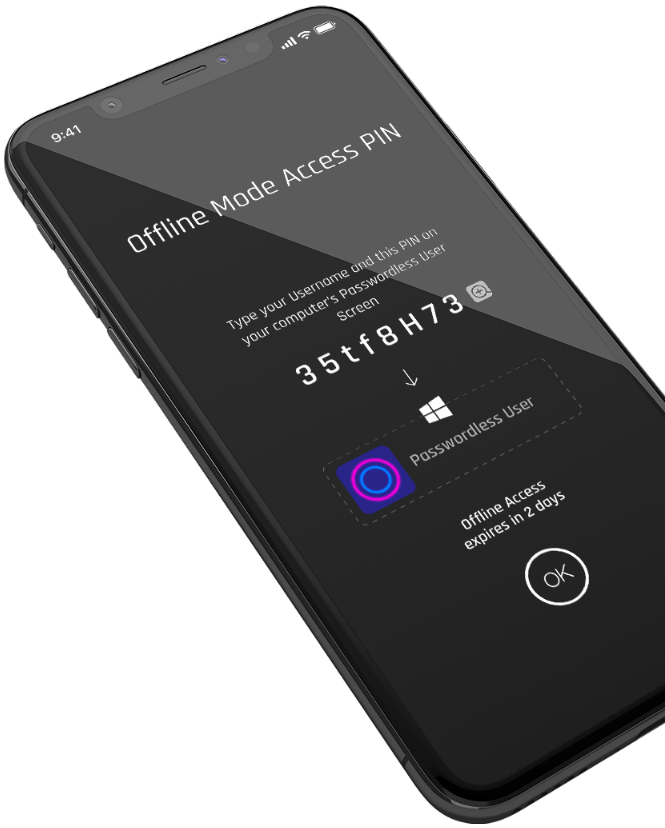
WATCH VIDEO


2. USER AUTHORIZES RDP LOGIN ON MOBILE HYPR MOBILE APP
fido CERTIFIED
3. HYPR TRUE PASSWORDLESS SERVER RELAYS SMART CARD LOGON FROM MOBILE
1. USER INITIATES RDP LOGIN ON CLIENT MACHINE
4. HYPR DESKTOP CLIENT AUTHENTICATES USER AND GRANTS ACCESS TO RDP
RDP

What if Users Are Offline?

The FIDO PIN is one of the most important features of a strong platform. It can be used for step-up authentication, gives users an alternative authenticator, and even enables a truly passwordless Offline Mode.

Watch Video of HYPR Offline Mode



9:41

Offline Mode Access PIN

Type your Username and this PIN on your computer's Passwordless User Screen

35tf8H73

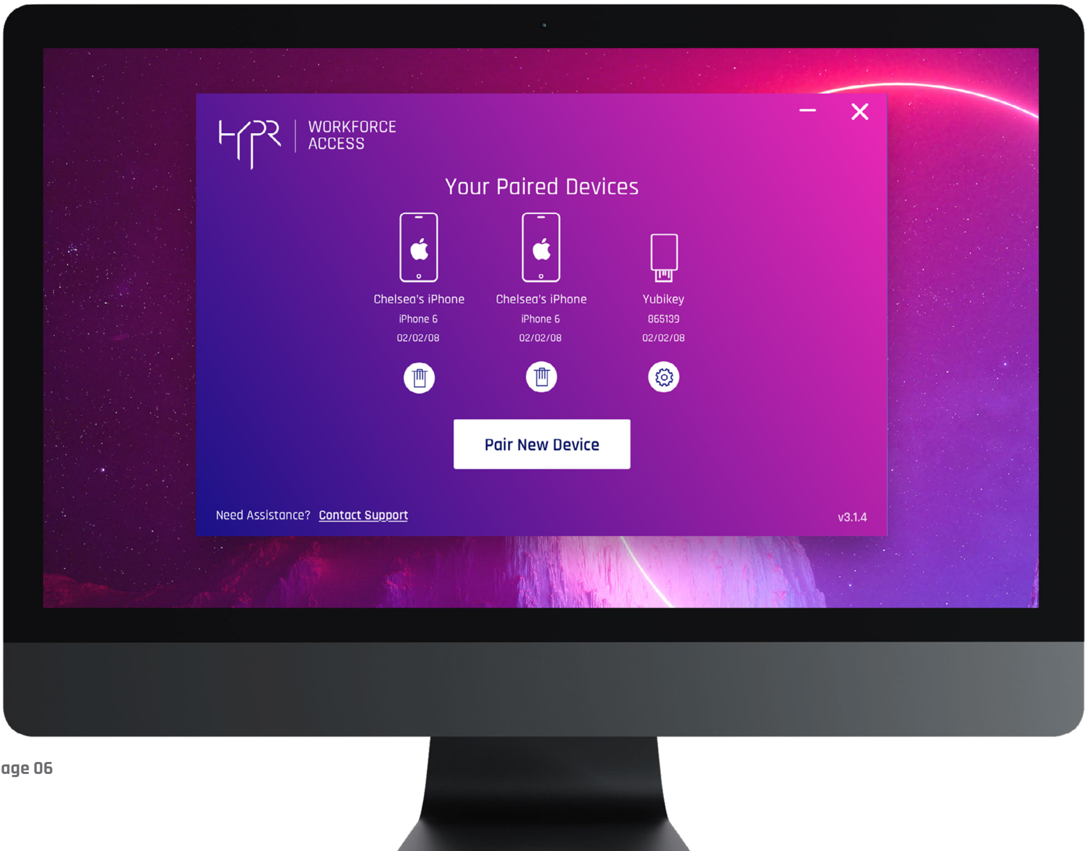
Passwordless User

Offline Access expires in 2 days

OK

Can Users Use a FIDO Token?

What happens if an employee loses their corporate issued device or personal phone? Security tokens provide a great solution for scenarios when users lose their smartphones. This is especially important for administrators who have a higher level of access or users who lack access to a smartphone. Your remote workforce should be able to remain passwordless by using secondary authenticators, such as a FIDO token. YubiKey provides a great example of a secure, easy-to-use FIDO token.



WORKFORCE ACCESS

Your Paired Devices

Chelsea's iPhone
iPhone 6
02/02/08

Chelsea's iPhone
iPhone 6
02/02/08

Yubikey
865139
02/02/08

Pair New Device

Need Assistance? Contact Support

v3.1.4

Watch Video of HYPR + FIDO Security Key

The Impact of a Passwordless Remote Workforce

Soon the notion of a "remote workforce" will disappear, and all workers will be equipped to work from anywhere. With the right tools, a remote workforce is just a workforce. It's simply a matter of giving them the tools to remotely work efficiently and securely. The timing for a passwordless approach couldn't be better.

A Happy Help Desk Unbothered by Password Lockouts

Save thousands of hours in help desk and service costs caused by password fatigue and the frustration that comes with long, complex passwords.

A Workforce Immune to Phishing & Credential Reuse

Phishing and credential stuffing attacks exploit passwords and their reuse. Instead of typing in passwords, enable your workforce with lightning-speed passwordless authentication initiated via a mobile device.

A Productive and Improved Remote Work Experience

The modern-day employee wastes an average of 24 hours per year logging into workstations. Improve workforce productivity by shaving down valuable time wasted on legacy MFA apps and typing in long, complex passwords.

A Consistent, Unified Login Experience

Your workforce is likely fumbling with your numerous MFA apps spread across multiple identity providers with different authentication modalities. Unify your identity portals with a consistent passwordless login experience that's easy to use and deploy.

> "Password lockouts generate service desk calls and lost user productivity. The adoption of HYPR passwordless is the rare cyber investment that returns immediate and measurable bottom line benefit."
>
> **- Karl Mattson**
> CISO

1001 Avenue of the Americas, 6th Floor
New York, NY 10011

1-866-GET-HYPR
www.HYPR.com