TRUE PASSWORDLESS SECURITY WHITEPAPER

HYPR

> Only the paranoid survive.
>
> **- Andy Grove**

Andy Grove's quote has aged well. In the digital era where change is constant, only the innovative survive.

Today's economy thrives on disruption. Unless you maintain quality services and keep up with technology, you are likely to become obsolete. Blockbuster, Tower Records, and Myspace are reminders of what can happen if your business fails to adapt and evolve with technology. Streaming ended Blockbuster, digital photography dethroned Kodak, and the mobile touchscreen revolution silenced Nokia. The list goes on. One by one, industry leaders are toppled as their verticals are disrupted.

Where is the transformation for cyber security?

INNOVATION = SURVIVAL

NO ONE WANTS TO BE THE BLOCKBUSTER OF THEIR INDUSTRY.

Cyber security innovation poses similar risks for leading brands. As security technology evolves, so does its counterpart – the cyber attack. News of online threats and data breaches are the first to steal headlines and impact the market. As of 2019, the average cost of a data breach is $8.19 million. But that isn't the only cost. More importantly, people are quick to lose trust and cut cords with brands when such events occur.

If a business loses a million customer passwords, can you blame the customer for ending their relationship? Of course not. So you invest precious time and resources in defending passwords - the hackers' favorite target. The single point of failure. The one part of your business that is impacted by outside breaches that have nothing to do with you.

You tell users to reset passwords regularly. You deploy more difficult ways to log in. You plead with them not to reuse passwords from other websites. And still your users fall victim to credential stuffing, password reuse, fraud and phishing attacks.

Businesses have invested millions of dollars in authentication and yet continue to rely on passwords. For the past 60 years the password has remained the crown jewel for any hacker. This is why authentication is finally being disrupted. Out of necessity for survival, we need new models for protecting our front doors to the digital world because the old ones no longer apply.

This paper is about the transformational moment for cyber.

This is about True Passwordless Security.

THE CURRENT STATE OF AUTHENTICATION

Authentication is the primary way we prove we are – who we say we are – in the physical and digital world. Knowing or unknowingly, we authenticate dozens, if not hundreds of times a day. We use it for work, banking, shopping, health, entertainment, bills, and nearly all other facets of our lives.

In 1961, Fernando Corbató at MIT invented the first computer password for the Compatible Time-Sharing System, or C.T.S.S. This allowed multiple users in different locations to access a single computer at the same time. His solution protected individual privacy and data on a small number of shared computers which proved to be helpful – at the time.

60 years later and with billions of dollars invested in digital security, we still use the half-century old password.

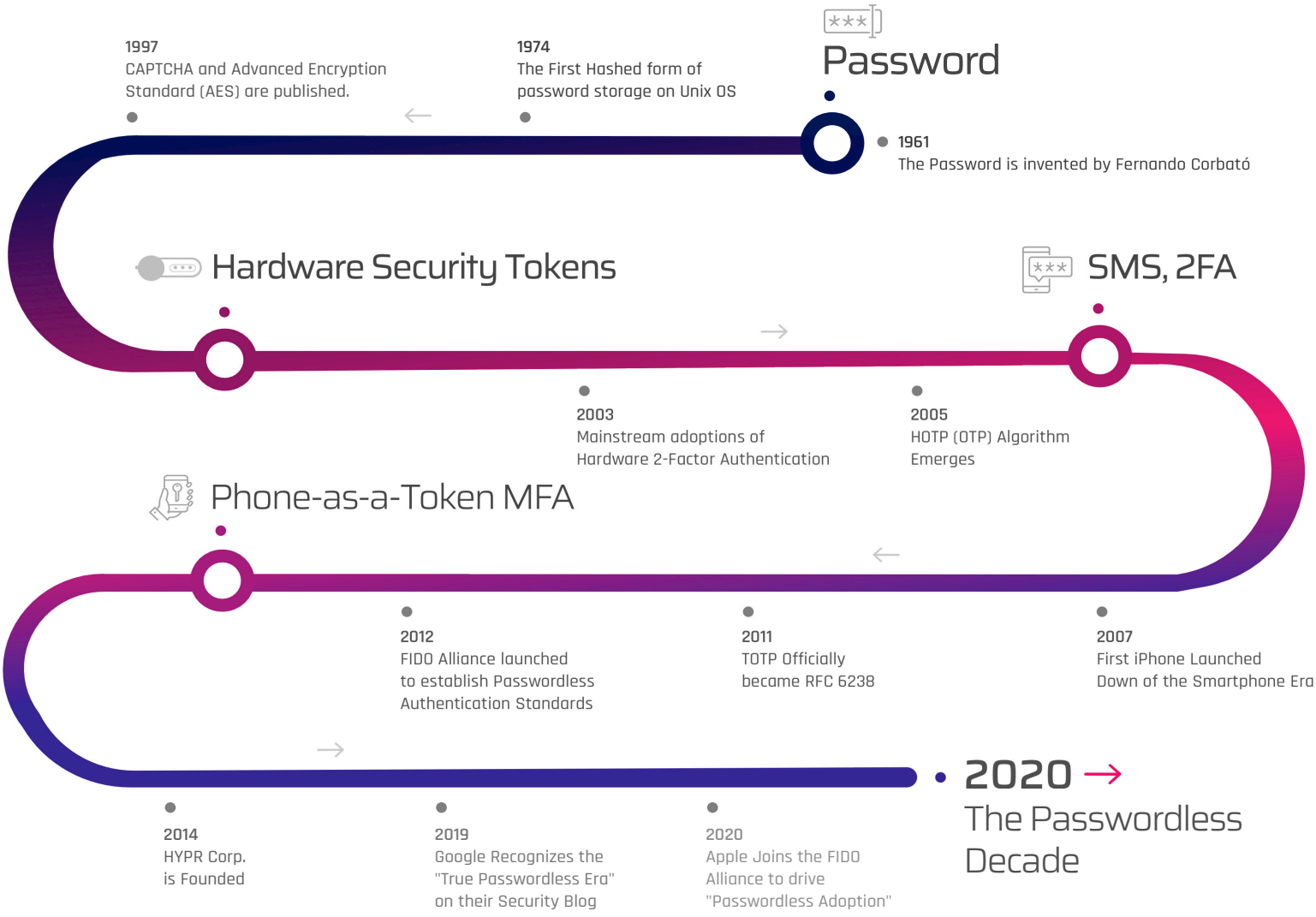
Over the last few decades, hardware security tokens like SecureID used for Two-Factor Authentication (2FA) turned mainstream. Then came the rise of SMS 2FA and software One-time Passwords (OTP). In 2013, Apple took biometric authentication to the masses with Touch ID. The common denominator is that none of these advances have replaced the password. Instead, they are often used alongside a password either protecting or adding a shared secret.

Today's security and identity teams across all industries recognize **shared secrets are an achilles heel**. Shared secrets we use for authentication include passwords, PINs, 2FA SMS codes, and One Time Passwords (OTP). It is a crumbling foundation which, if not addressed, negatively impacts the future of authentication – and global security for that matter. Modern credential reuse and 2FA replay attacks are low cost and easy for the hacker, while expensive for organizations to defend against.

Credential stuffing is at an all-time high, costing the US banking industry alone $50 million on a daily basis. 2FA phishing is now also a major concern. OTP over SMS can be intercepted via SIM swapping and via a vulnerability in the SS7 protocol. Like traditional passwords, OTP, PINs, credit card numbers, are still shared secrets. **Shared secrets leave people vulnerable to fraud and breaches**.

WHAT ARE SHARED SECRETS?

They are passwords, PINs, 2-Factor SMS codes, One Time Passwords (OTP), even credit card numbers. Any digital key posessed by both a user and a centralized database can be a shared secret. They are often the cause of large scale breaches, credential reuse, phishing and replay attacks. Despite millions invested in authentication, businesses continue to rely on passwords and shared secrets.



THE PASSWORDLESS FUTURE IS ALREADY HERE. IT'S JUST NOT EVENLY DISTRIBUTED.

Despite millions invested in authentication, businesses continue to rely on passwords and shared secrets. Most legacy MFA products rely on passwords. And, confusion around what "true" passwordless security really means has led to a disparity among organizations that are passwordless and those who are not.

In order to understand why True Passwordless Security is so urgent, we must first understand why legacy MFA has failed.

THE PROBLEMS WITH LEGACY MFA

Organizations today face various challenges with legacy multi-factor authentication (MFA) that's built upon the use of shared secrets. There are a few major pain points legacy MFA fail to address:

Enterprises Have Failed to Solve the Desktop MFA Gap

Customer-facing MFA has Stagnated Globally

Credential Stuffing and ATO Fraud has Skyrocketed

IAM Infrastructure and User Experiences are Fragmented

THE DESKTOP MFA GAP IS GROWING

Simply put, workforces across enterprises have failed to adopt MFA at scale due to user friction. Despite the intent to improve security for internal and external facing applications, legacy MFA has left workstations wide open. In fact, the 2019 Internet Trends Report by Mary Meeker found that MFA is most often used for VPN and remote login – but not for workstation access. Why is that?

Slow Login Speeds = Poor User Experience

Some products attempt to enforce Password + 2FA via a mobile app or SMS as an additional factor. However these MFA practices are typically used with passwords and make the workstation login so difficult that users revolt in anger. Forcing an employee to enter a long password *and* use MFA will slow login speeds to a crawl, reduce workforce productivity, and frustrate users.

High Costs of Additional Hardware Tokens and Smart Cards

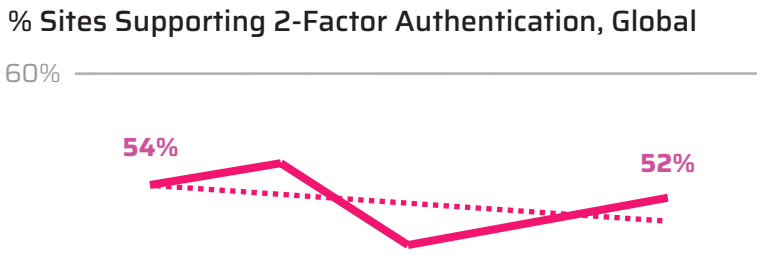
Businesses enjoy the security that comes with security tokens such as smart cards and Yubikeys which utilize Public Key Cryptography. Users and admins, however, do not share that same joy. Additional hardware devices are often easily forgotten, stolen, shared, and lost – this forces organizations to buy a larger supply than needed to compensate for keys lost over time.

Passwords are Cumbersome

Additionally, typing long complex passwords at the workstation, whether in the office, or remotely, takes away from productivity. Seconds add up to minutes, and over the course of the year, your workforce begins to lose hours that otherwise would have been more productive.

Windows Hello or Goodbye?

Although Windows Hello has been applauded by consumers, Gartner observed that enterprise adoption was struggling for a number of reasons. Windows Hello forces users to use a single desktop, preventing the use of shared workstations and hot desking. Windows Hello also only works on Windows 10, so the use of iOS, Android, MacOS and other devices creates fragmentation and barriers for scaling.



DID YOU KNOW?

Despite billions of dollars invested in MFA, adoption has stagnated globally. According to Mary Meeker's 2019 Internet Trends Report, the number of sites supporting 2-Factor Authentication has dropped to 52%.

CUSTOMER MFA HAS STAGNATED

Most organizations do not have customer MFA. Those that do, struggle with low rates of adoption. This is due to friction. The current state of customer authentication is worrisome because a majority of users worldwide still habitually use passwords.

Evolving Regulatory Requirements

The European Union (EU) pushed Strong Customer Authentication (SCA) as a requirement of the Directive on Payment Services (PSD2). This is a step forward for enforcing MFA for payments, but what are the implications for other industries, and the rest of the world? The good news is that regulations are causing financial institutions to take notice and innovate on how they enforce and utilize MFA.

The Friction Factor

Customers do not want to use MFA – it's that simple. People want to log in quickly and easily without thinking about how many factors they must use. Regulations may address security but it does not provide guidance on the user experience (UX) which directly impacts adoption. For customer MFA to really take off, regulatory enforcement may not be enough.

Fear of Cart Abandonment

UX is the backbone of the customer experience which drives revenue. Cart abandonment is a growing concern due to friction imposed during the checkout process. Forrester notes that 37.4% of shopping cart abandonments occur at login. A recent report by 451 Research also found that Europe's online economy risks losing €57 billion when SCA goes into effect.

CREDENTIAL STUFFING AND ACCOUNT TAKEOVER (ATO) FRAUD HAS SKYROCKETED

Data breaches and stolen credentials are still the biggest cyber threats organizations face worldwide. Nearly every week there's a new breach that affects millions of users and has long-term impacts on the organization's services and brand. But what about the collateral damage from breaches that happen outside of your control?

Hackers aren't trying to crack your passwords – they're weaponizing millions of passwords against you.

Hackers attempt to find accounts that reuse passwords across websites for Account Takeover (ATO) fraud. Targeted attacks like credential stuffing and password spraying will only become more commonplace as long as we continue to use passwords. Some financial services scan the dark web and unsafe sites for compromised credentials and alert their customers upon its discovery. Websites like *Have I Been Pwned?* allow people to check whether their personal data has been compromised by data breaches. Other providers compile a list of blacklisted passwords or automatically prevent users from including personal information. **Credential Stuffing has become an undeniable epidemic.** Malicious logins account for more than half of consumer banking traffic.

$1.7B
Account Takeover (ATO) fraud costs have doubled since 2015

+56%
Of Consumer Banking traffic is malicious login attempts

+30B
Login attempts in 2018 were Credential Stuffing attacks

> The cost of the attack has gone down for the adversary. The cost of defense has never been higher.
>
> **- Abbie Barbir**
> Senior Security Architect, Aetna CVS Health

Has risk-based authentication solved the credential reuse problem?

We've been hearing about it for over a decade – the risk-based approach that leverages "Machine Learning" and "Adaptive Risk" to provide a silver bullet to your credential reuse problem. Adaptive authentication approaches are valuable for environments where credential reuse is a factor, but the reality is that even the latest solutions rely on the use of passwords and shared secrets. These approaches are built on top of a broken foundation and act as a Band-Aid rather than a solution. Organizations that utilize such tools often continue to struggle and defend against attacks that are easily and cheaply executable by bad actors.

HAVE YOU DEPLOYED A RISK-BASED IAM PRODUCT?

Consider two questions:

- Have your fraud rates gone down?
- How long does it take a user to login?

FRAGMENTED IAM INFRASTRUCTURE LEADS TO FRAGMENTED USER EXPERIENCES

Fragmented IAM infrastructure makes it difficult to deliver a unified authentication experience. For many organizations, digital transformation is a resource-intensive and urgent initiative. Despite mass migration to the cloud, on-premises infrastructure is not going away anytime soon. There's a need for modern technology to accommodate diverse architecture and infrastructure. Larger organizations are likely to have older technology they must maintain due to its natural growth over the past decades. Fragmentation can also be caused by mergers and acquisitions, or having multiple lines of business that span across the globe.

Vendor lock-in may prevent organizations from growing their services as needed. This can entail deployment to a new preferred cloud provider, or more importantly, addressing region-specific regulations on data residence. **Organizations need the flexibility and speed to go cross-cloud, cross-platform, for any app.**

IAM and security teams must often manage multiple identity providers with various ways of authenticating. Building a team with the experience that matches your purchased solutions is a task in itself – it drives the need for vendor consolidation. This initiative is time and resource intensive. Meanwhile, people demand a single, unified experience. **As new lines of business and apps emerge, organizations need a fast, consistent way of providing access to their workforce and consumers.**

MORE PASSWORDS, MORE PROBLEMS

The average user is burdened with remembering 20+ passwords. Forrester notes that 20-30% of helpdesk calls are password related - costing over $179 per user per year to resolve password issues.

Longer Complex Passwords = Unhappy Users.

According to SplashData, the most popular password for the past seven years was *123456*, and before that it was *password*. Poor password hygiene is widespread, and there's a reason for it. A study has shown that the longest sequence an average person can recall contains a sequence of seven alphanumeric characters. However, password policies have grown stricter over time to prevent brute force and dictionary attacks.

NIST guidelines attempt to help organizations make passwords safer by enforcing password policies with a minimum of 8 characters. Organizations go as far as making the minimum 16, 32, and some even 64 characters. There are also requirements for special characters, blacklists of previously or commonly used passwords, and the notorious 90-day expiration policy.

72%

Of individuals reuse passwords according to a recent survey by HYPR - while nearly half (49%) of employees simply change or add a digit or character to their password when updating their company password every 90 days.

The Business Impacts of Password Fatigue

Too many authenticators and too much choice usually backfires. By now users are overwhelmed and will either reuse passwords or resort to sticky notes, notepads, or digital documents to store their complex passwords. People simply can't remember long complex passwords. Password reset costs take a toll on organizations internally and externally, costing on average $40-50 per reset. Some organizations even budget for password-related support costing millions on an annual basis. This spikes the cost of ownership for organizations that manage both workforce and customer users through multiple authentication products.

We need to acknowledge that the trajectory passwords are on is simply not sustainable. They are costly to manage, and impact help and support desk productivity. Long complex passwords may address password hygiene, but they do not address the vulnerability of credential stores, head-on.

TRUE PASSWORDLESS SECURITY

Eliminate passwords and you eliminate the Hacker's favorite target.

Building a passwordless world is the single shared mission that drives HYPR. The key to unlocking this world is what we call True Passwordless™ Security.

At HYPR, we engineered a proven model that is trusted by industry leaders with millions of users deployed across companies such as Mastercard, Aetna CVS Health, Rakuten, First Citrus Bank, T-Mobile, and many more. Today, HYPR is the leading authentication platform designed to eliminate passwords and shared secrets across the enterprise. With HYPR, businesses are finally able to deploy Desktop MFA and Strong Customer Authentication with ease to millions of users worldwide.

We help you evolve your organization from a target that's expensive to defend, to an infrastructure that's expensive to attack. And we do this by forcing hackers to go after each device individually. This approach nullifies mass credential stuffing, password reuse and phishing attacks.

Dozens of MFA vendors claim to offer passwordless authentication. It may appear to be true on the surface, however, they are not truly passwordless. A passwordless user experience does not equal true passwordless authentication. For example, One-Time Passwords (OTP), are often mistaken for passwordless authentication.

Methods like OTPs still require a password or shared secret on the back-end. It's just hidden behind the scenes – away from the user's purview. This can be deceptive and damaging when an organization realizes it's still open to attack.

The legacy MFA approach certainly does not change our security model and it does not address the critical and direct need for eliminating shared secrets. To achieve True Passwordless Security, we must take a different approach you may already be familiar with – Public Key Encryption.

WHAT DOES IT MEAN TO BE TRUE PASSWORDLESS?

Your users don't remember their password. They don't even know what it is. They use their mobile phone to log into desktops, mobile, and web applications. Your admins don't need to reset passwords. They don't worry about password reuse. They can use alternatives such as smart cards, biometrics, and hardware tokens.

Users never type in a password. Anything less just isn't True Passwordless Security.

HOW IT WORKS

A Combination of Public Key Encryption + Open Standards + User Experience

In a true passwordless architecture, the use of shared secrets such as passwords, PINs, SMS codes and OTPs is replaced with public key cryptography. Private keys are generated by the user on their device and remain on the device at all times. Biometric sensors such as Apple Touch ID, Face ID, and their Android and Windows counterparts, are often used to unlock these credentials that are verified against an authentication server using public key cryptography.

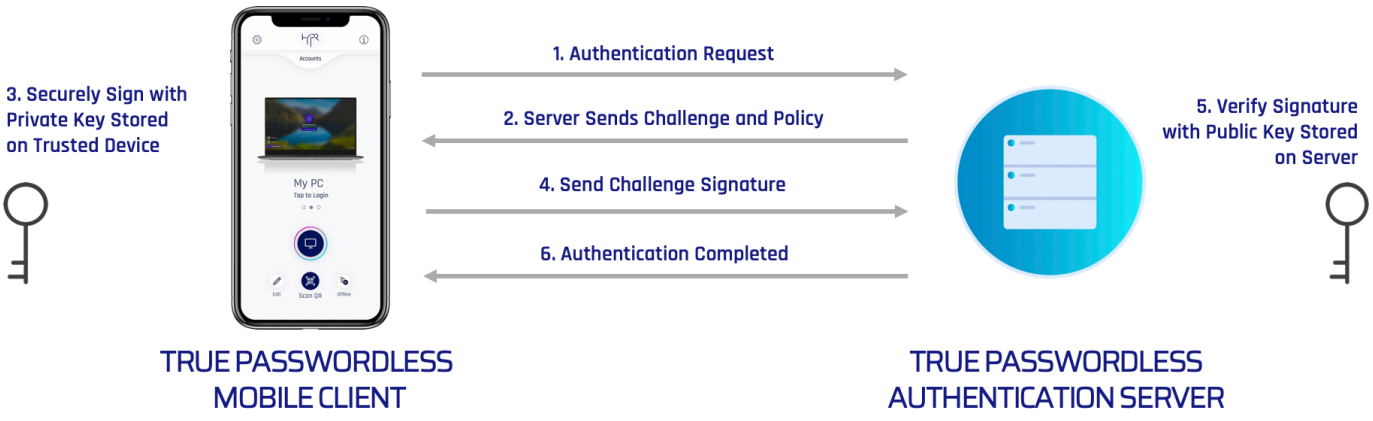
Rather than storing passwords and shared secrets inside the enterprise, True Passwordless Security moves the crown jewels to the edge. User credentials are stored securely in the most trusted areas of smartphones and devices that are in the control of the user.

HYPR replaces the use of passwords and shared secrets with Public Key Cryptography and open standards such as FIDO2. With HYPR you eliminate shared secrets through the use of Public Key Encryption (PKE) which drastically reduces the attack vector. 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 True Passwordless Server. Simply put, it's like turning your smartphone into a smart card.

As authentication keys move to the user's device, attackers shift their focus on the mobile ecosystem. That's why HYPR was designed to take advantage of advances in hardware-backed security by storing private keys inside the most trusted area of any mobile device – the TrustZone. Mobile TrustZones such as the iOS Secure Enclave (SE) and Android's Trusted Execution Environment (TEE) serve as a foundation for true passwordless authentication.

In addition, the HYPR platform is FIDO® Certified end-to-end. This means we go beyond the common "FIDO-support" and "FIDO-compliant" claims which only suggest a basic level of interoperability and understanding of the open standard for authentication. HYPR provides all of the necessary components to help organizations adhere to the latest FIDO UAF, U2F and FIDO2 specifications so you can deliver true passwordless security and usability to all users.

And unlike most other passwordless providers, HYPR is a board member of the FIDO Alliance. The FIDO Alliance includes members such as Apple, Microsoft, Google, Samsung, and other industry leaders focused on eliminating passwords.



TRUE PASSWORDLESS™ MFA

Lightning-Fast. Easy to Use. Easy to Deploy.

Fast. Secure. Passwordless. That's what organizations across all industries seek to provide their workforce, and it's made possible with True Passwordless MFA by HYPR. With built-in support for your favorite Identity and Single Sign-On (SSO) providers, HYPR helps you extend passwordless authentication across your enterprise.

Solve Your Desktop MFA Gap

Eliminate passwords across Windows, MacOS, and Linux machines, as well as virtual desktops (VDI). HYPR provides out-of-the-box support for all SSO so you can easily close the desktop MFA gap, once and for all.

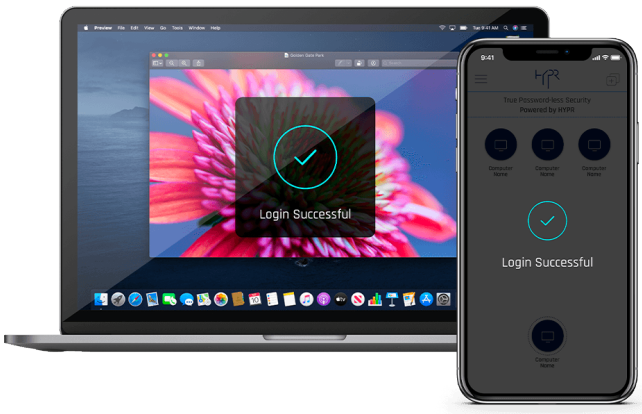
Go Anywhere with Offline Mode

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.

By starting the login experience on your mobile device, HYPR eliminates PUSH attacks and 2FA breaches. This advanced innovation is one of the many reasons why enterprises choose HYPR to eliminate the password.

HYPR is the only provider to enable passwordless login that begins on the mobile device. By initiating authentication on the mobile device, HYPR stops attacks before they happen including: PUSH attacks, man-in-the-middle (MITM) attacks, replay attacks, credential stuffing attacks, brute force attacks, and social engineering.

In addition to stopping large-scale attacks such as credential stuffing, HYPR helps you protect against emerging threats such as PUSH attacks. It also saves an average of 8 seconds for each login. This approach enables your workforce to quickly log into their Windows, Mac, and virtual desktops – saving time that's lost to typing in passwords, tokens, OTPs and using other cumbersome legacy MFA methods.



> Passwords are not security – they are a vulnerability. The world needs to move beyond password-based authentication. HYPR provides identity authentication without the passwords.
>
> **- Michael Christenson**
> COO, New Relic

BENEFITS OF TRUE PASSWORDLESS™ MFA

Eliminate Password Reset Costs

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

Stop Phishing & Credential Reuse

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

Unify Authentication Experiences

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 easy to deploy.

Save 24 Hours a Year in Workforce Productivity

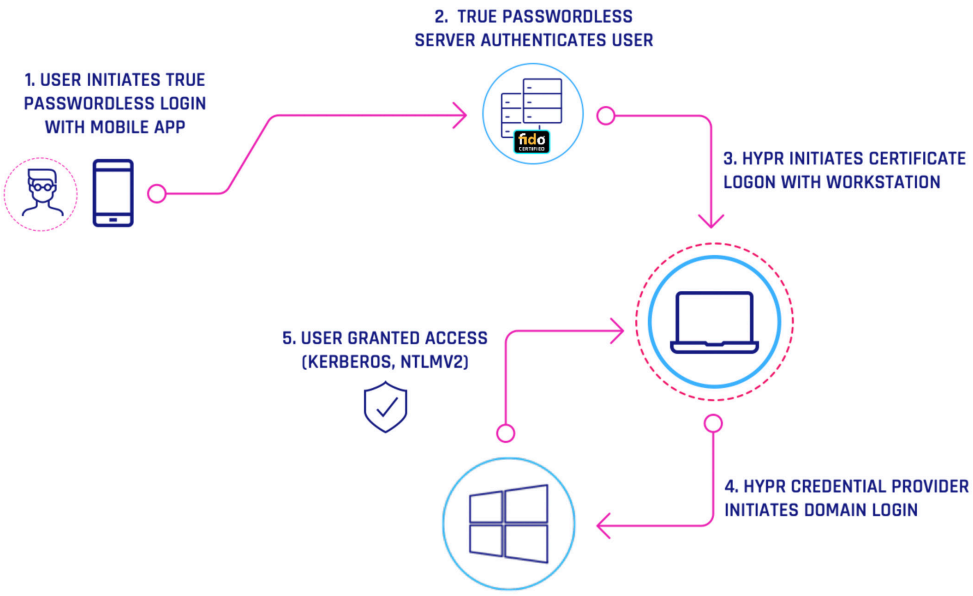
The modern day employee wastes an average of 24 hours per year logging into workstations. Improve workforce productivity by shaving down valuable time wasted on legacy MFA apps and typing in long, complex passwords.

Do More with Your Authentication Spend

Your organization invested a lot of time, resources, and effort into your identity stack. We enable you to put True Passwordless MFA in front of your existing solutions so there's no need for rip and replace. Our native plugins are fully interoperable with your existing identity infrastructure.

TURN YOUR SMART PHONE 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 FIDO-Certified. It's fast. It even works on Windows 7.



TRUE PASSWORDLESS™ SCA

Deploy Strong Customer Authentication in a Day

Strong Customer Authentication (SCA) under the PSD2 regulation addresses security protocols but it can introduce friction if not addressed correctly. The success of these security mandates heavily depends on customer adoption at scale. This requires a solution that enhances security without compromising on excellent UX demanded by customers.

Lightning-Fast Mobile-to-Web Authentication

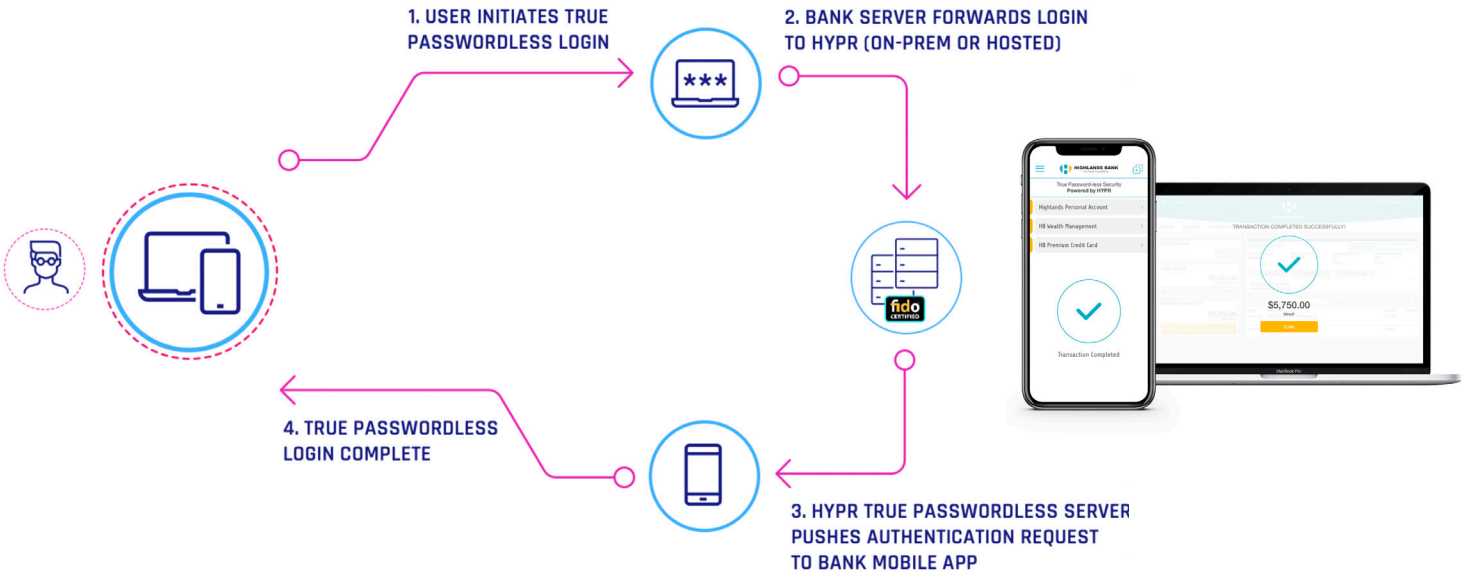
HYPR gives your users a consistent mobile-to-web login experience and accelerates transaction velocity with passwordless transaction approval. Additionally, HYPR is scalable to millions of transactions per minute. True Passwordless SCA performs under pressure so you can handle usage spikes as well as growing demand.

Meaningful UX for Everyone

Everyone is a user: customers, employees, and admins. At HYPR, we believe everyone deserves a thoughtful user experience. Our lightning-fast UX applies to all users, including your technical team.

Time is money and your organization needs agility. This remains true even for small teams that have minimal resources. That's why HYPR is built for speed. True Passwordless SCA makes life easier for admins and developers from a delivery standpoint.

HYPR's mobile and web SDKs put emphasis on fast developer integration and deployment so your team can quickly provide secure access on any app across all your business lines.



> HYPR's Passwordless FIDO authentication provides an alternative to phishable and inconvenient passwords/PINs - and it works across devices customers use in their daily lives already.
>
> **- Arshal Ameen**
> Application Architect, Rakuten

BENEFITS OF TRUE PASSWORDLESS™ SCA

Achieve SCA in a Single Day

True Passwordless SCA makes life easier for organizations and their teams to quickly deploy passwordless authentication millions of customers worldwide. Maximize your reach with passwordless security that eliminates poor UX that comes with shared secrets and legacy MFA. It's time to evolve your security to better tackle fraud and friction, at global scale.

Stop Credential Stuffing and ATO Fraud

Customers habitually reuse passwords across websites. This poses a widespread security risk because credential harvesting has a domino effect that impacts organizations worldwide. By eliminating passwords, you protect your customers against large-scale credential reuse attacks.

Save Millions in Password Resets

You know the drill. Users get locked out, Customer Service teams spend thousands of hours a year on this problem. Long, complex passwords are expensive to manage and frustrating for everyone. You can instead, enable your workforce with lightning-speed passwordless authentication initiated via mobile

Satisfy PSD2 Compliance

Section 9.3 of the PSD2 Regulatory Technical Standards (RTS) specifically describes the use of "separated software execution environments" for achieving Strong Customer Authentication (SCA). This means passwords and legacy 2FA are no longer good enough to secure customer applications – as they rely on shared secrets that do not make use of a secure software execution environment. HYPR provides a fast and simple way to achieve PSD2 compliance by eliminating the use of passwords and shared secrets for authentication.

Accelerate Mobile Adoption and Enhance Customer Experiences

Usability drives adoption. HYPR provides fast and easy UX that's designed for everyone. With True Passwordless Security you can create a frustration-free experience that prevents cart and checkout abandonment. It also frees up time for your customer support team to focus on providing stellar service instead of password resets.

> "After more than 50 years in the IT industry, I'm finally seeing the password come to an end. What HYPR has done for passwordless authentication is nothing short of phenomenal."
>
> **- Nicholas Donofrio**
> EVP of Technology, IBM (Ret.)

WHY HYPR?

The Secret Sauce is Execution

True Passwordless Security is not just one thing. It's the sum of all the parts working together in unison. We built upon familiar concepts, tried and tested security practices that have worked for decades, and leveraged open standards developed and driven by industry leaders. We combined this formula with best-of-breed security, and an innovative groundbreaking user experience that's unparalleled in speed and ease of use.

Organizations face a multitude of problems with passwords and legacy MFA. Pain points cut across security, operations, productivity, engagement, and user adoption. Organizations need a proven model that doesn't rely on the password – a model that protects users, services, and brand reputation.

At HYPR, we understand organizations must address attack vectors to protect both workforce and consumer users. A "user is user is a user is a user," may or may not be attributed to Getrude Stein, but we do know people ultimately want the same thing: safe and easy access to the digital world. As long as we maintain credential stores of shared secrets, we will continue to play whack-a-mole with our pain points unnecessarily into the future.

The time is now. The urgency for True Passwordless™ Security is here – and it's important to get it right from the start. Evolve beyond legacy MFA and outdated security models. Unlike legacy MFA vendors HYPR is laser-focused on key elements:

Elimination of Passwords and Shared Secrets for Leading-Edge Security

Evolve your organization from a target that's expensive to defend, to an infrastructure that's expensive to attack.

True Passwordless Offline Mode

True passwordless offline mode is unique to HYPR, uses a decentralized PIN, and ensures your roaming workforce is safe wherever they are. This unique approach is a prime example of the depth of expertise that goes into addressing edge cases to ensure passwordless adoption across the globe.

Mobile-Initiated Authentication

Enable passwordless login that begins on the mobile device to stop attacks before they happen including: PUSH attacks, man-in-the-middle (MITM) attacks, replay attacks, and credential stuffing attacks.

Public-Key Encryption and Open Standards

Reduce your attack vector by replacing passwords and shared secrets with Public Key Cryptography and open standards such as FIDO2.

Lightning-Fast Deployment, Integration, and Ease of Use

Arm your teams with true passwordless SDKs to achieve fast developer integration, deployment and login experiences. If your organization has customer-facing apps, we can help you achieve SCA in a single day.

Right Balance of UX and Security

These two disciplines have traditionally lived within their own siloes. Today, the expanding digital landscape calls for UX and security to combine into a dynamic yet balanced whole. Use cases are converging. People want to authenticate securely and enjoy using products and services, at work and at home.

A SINGLE HOLISTIC APPROACH

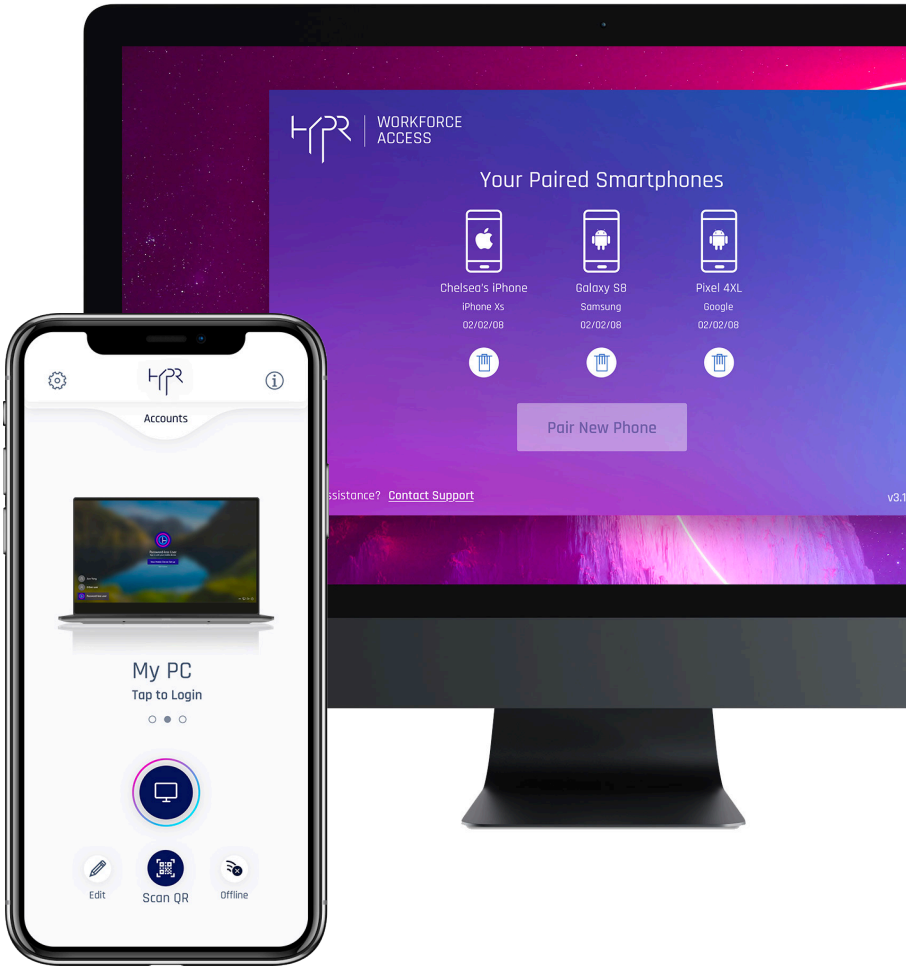
Eliminate Passwords For Both Customers and Workforce

At HYPR, we designed our passwordless authentication platform to address the accelerated convergence of workforce and customer use cases. HYPR provides everything your organization needs to deliver True Passwordless™ Security to customers, employees, partners, and contractors.

For modern CISOs, CIOs, security, IAM, and IT leaders across the organization, the cost-benefit ratio is key. HYPR provides a unified passwordless authentication platform for both workforce and customer users which presents your organization a level of efficiency, cost savings, and ease of use that was previously unachievable.

Do more with your authentication spend when it comes to securing access for everyone. HYPR's unified solution helps you eliminate passwords across your organization. Many organizations must manage multiple identity providers such as Okta, ForgeRock, Ping, CA, FusionAuth and more. With our holistic approach, you don't have to worry about vendor lock-in. You can extend investment in your existing infrastructure and provide fast, easy access for both your workforce and consumers that's cross-platform, cross-cloud, and in your own app.

A passwordless future is inevitable – and we want to help you get there quickly. Set your organization ahead from competitors with best-of-breed authentication that goes beyond outdated security models and the status quo. With HYPR you can achieve the necessary balance between security and UX in order propel your organization into a brighter future.



START YOUR FREE TRIAL NOW

FIND OUT WHY LEADING ENTERPRISES

DEPLOY HYPR TO ELIMINATE PASSWORDS:

WWW.HYPR.COM/FREE-TRIAL

ABOUT HYPR

HYPR is the leading provider of True Passwordless Security™ Backed by Comcast, Mastercard, and Samsung, HYPR is the first authentication platform designed to eliminate passwords and shared secrets across the enterprise.

With HYPR, businesses are finally able to deploy Desktop MFA and Strong Customer Authentication to millions of users worldwide.

Learn how to stop credential reuse and account takeover fraud at www.HYPR.com

#ELIMINATETHETARGET

> Without change there is no innovation, creativity, or incentive for improvement. Those who initiate change will have a better opportunity to manage the change that is inevitable.
>
> **- William Pollard**

www.HYPR.com