DECOUPLING AUTHENTICATION FROM IDENTITY PROVIDERS

Cloud Wars and Identity Turmoil

The cloud wars have created a state of identity turmoil characterized by poor user experience, MFA fatigue, and an unsolved password problem. In an effort to mitigate this chaos, businesses are decoupling authentication from their identity providers. IT teams are taking a renewed focus on the authentication problem with new products and initiatives separate from the numerous incumbent identity products.

The separation of authentication and identity is noticeable in customer case studies and leading analyst research. Standards bodies have also taken notice, with NIST and EU guidance recommending stronger authentication practices.

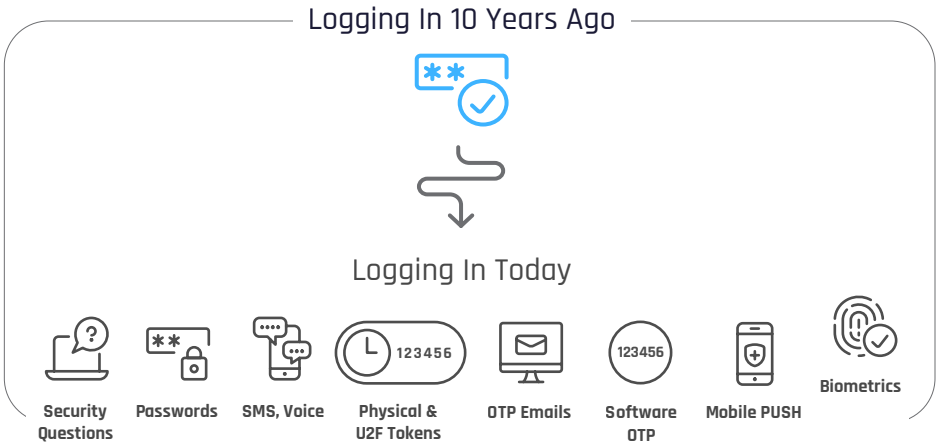
This paper explores this growing trend, why it's happening, and the impact it can have on the next 5 years of digital identity.

Authentication has Become Too Complicated

There was a time passwords and hardware tokens were the gold standard for secure login. Businesses had office drawers stocked full of RSA SecurID tokens.

In the 2010s, smartphones took user authentication to the next level with new methods such as soft tokens, One-Time Passwords (OTP) or PUSH-based login using a mobile app. Duo Mobile was a great example of an app that displaced hardware tokens as a mainstream method for multi-factor authentication (MFA).

As smart phones became ubiquitous across the enterprise the identity platforms saw an opportunity to merge MFA with their products. Soon enough everyone had a dedicated MFA app baked into their Identity suite. Today there are *over 200* IAM vendors. For many users the drawer of RSA tokens has been replaced by a smartphone full of MFA apps.



Users Struggle with MFA Fatigue and Password Pain

Fast forward to 2020. Users have many ways to log in such as passwords, hard and soft tokens, OTPs, smartphones, wearables, Windows Hello, SMS, SamsungPass, Touch ID, Face ID... and the list goes on. The authentication landscape has become much more complex and businesses are finding it difficult to maintain a consistent user experience. Ask end users if they enjoy their login experience and you might hear complaints about password complexity, a sense of reduced productivity, and what some call "MFA fatigue."

MFA has been commoditized and mandated in many places - yet most businesses still have a difficult time enforcing it for customers and employees. Remote work has reignited urgency for multi-factor security by exposing adoption gaps across desktop login, remote access and customer-facing applications. According to Mary Meeker's 2019 Internet Trends Report, the number of websites supporting Two-Factor Authentication (2FA) had *dropped* to 52% - with friction being a key factor.

Businesses have more MFA options than ever before and yet they still have gaps in user adoption. The worst part? Everyone is still using passwords.

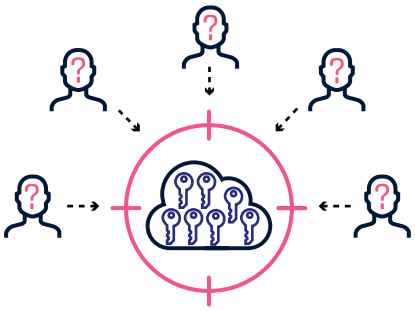
Looks familiar?

MFA Fatigue is a growing problem

Password-Based MFA was Commoditized by the Identity Providers

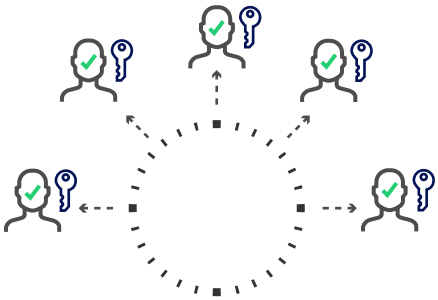
Identity platforms built their multi-factor products on top of passwords and shared secrets. The result was a commoditized password-based MFA experience that was "good enough" for most use cases and solved the compliance "checkbox." Most mainstream PUSH, OTP, SMS, or Soft Token products utilize a similar combination of passwords + symmetric cryptography to provide a multi-factor authentication experience.

In the late 2010s "True Passwordless" authentication gained notoriety. Unlike legacy MFA, such password-less approaches prohibit the use of passwords or other shared secrets, instead relying on public-key encryption and open standards for strong authentication. This fundamentally challenges the password-based authentication methods that are deeply embedded in the identity stack. Surprisingly, the same approach that made it easy for Identity products to commoditize MFA is often the reason businesses have such difficulty moving away from passwords.



PASSWORDS & LEGACY MFA

- High Friction Login & User Disruption
- Rely on Passwords and Shared Secrets
- Susceptible to Credential Reuse & 2FA Phising
- Adoption Gaps for Customer & Desktop MFA



TRUE PASSWORDLESS MFA

- Provides a Lightning-Fast User Experience
- Replaces Passwords with Public-Key Encryption
- Stops Credential Stuffing, Fraud and Phishing
- Solves Customer and Desktop MFA Gap

Password-less MFA Demands a Different Approach

As organizations became more aware of the password-based MFA provided by incumbent identity vendors, they focused their attention on next-gen solutions such as as YubiKey, Windows Hello, and HYPR - all of which are laser-focused on solving the password problem. There is an ecosystem of next-gen MFA products, with analysts projecting TAM growth to $20B by 2025.

Legacy MFA products were prone to silos and vendor lock-in, while the new-school of authentication focuses on interoperability. Bringing together open standards such as FIDO2 and SAML, they emphasize interoperability and integration *with* identity platforms rather than working to displace them. This new authentication segment has visibily "decoupled" from the broader Identity space.

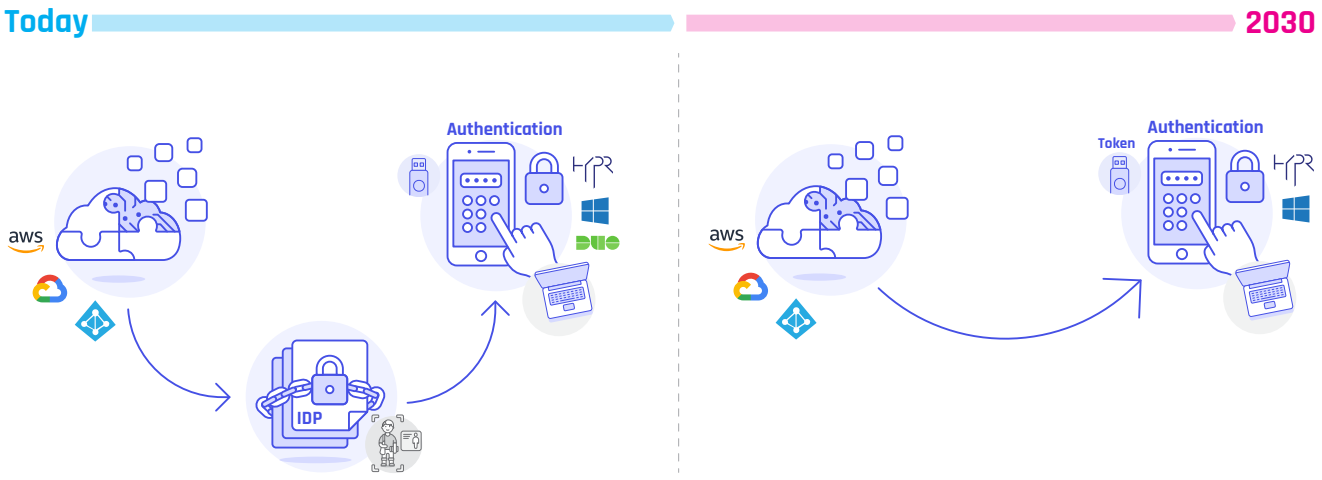
Analysts have also taken notice. Gartner, for example, have outlined a new "User Authentication" segment separate from the broader Identity Access Management category. In their 2020 Market Guide to User Authentication, Gartner suggests that, "Most legacy 'MFA' tools are really only '+1FA' tools, adding a single extra factor to a legacy password. New "True" MFA tools are gaining attention among clients; these typically provide passwordless MFA."

> "Legacy MFA tools are really only adding a single extra factor"
> -Gartner

Identity is Now Being Commoditized by The Cloud

The cloud wars rage on. Amazon, Microsoft and Google compete for the pie in the sky, building more and more features into their massive platforms. As of 2020 Microsoft states that Azure AD manages more than 1.2 billion identities and processes over 8 billion authentications every day. The sheer size and scale of these initiatives is mind-boggling. Identity is a core component of the cloud story and as these industry titans continue to expand their offerings, 3rd party Identity Products (IdPs) risk being commoditized. With more than 200 IAM providers out there the space is likely to consolidate.

5 Years From Now - What is the Role of a 3rd Party IdP?



Key Authentication Challenges Remain Unsolved

While digital identity has become more centralized and commoditized, the authentication layer has grown more fragmented. Enterprises are all too familiar with the identity headaches of a cloud transformation. MFA fatigue slows down the users, while fragmented identity systems burden a resource-constrained IT team. And while SMBs and new products born in the cloud may never encounter the need for a third party IdP, they too suffer from the same reliance on passwords and password-based MFA. Businesses of all sizes face authentication challenges that have been left unsolved such as:

- **MFA Fatigue**
  Caused by an overabundance of authenticator applicationss and methods.
- **Reliance on Passwords**
  Password-based MFA is baked deep into existing identity products and processes.
- **User Disruption**
  Recurring user re-enrollment and re-education is disruptive and carries switching costs.
- **MFA Gaps and Inconsistent Login Experiences**
  From customer MFA to desktop login, businesses struggle with large gaps in MFA usage and adoption.

Businesses are Solving the Authentication Problem by Decoupling Authentication from Identity Providers

A growing number of organizations are solving their authentication challenges with new products and initiatives that are separate from the password-based MFA provided by their incumbent IAM vendors.

3 key drivers stand out:

1 Decoupling Mitigates Identity Turmoil and User Disruption

The cloud wars have amplified the pain of identity fragmentation and its burden on IAM teams. Relying on multiple MFA products can lead to disruption when users are forced to re-enroll and re-learn their login experience. Such identity chaos creates operational risk, increases helpdesk costs and strains IT resources.

Businesses are investing in next-gen authentication platforms that are distinct from their identity providers. Their desired outcome is a consistent, secure authentication experience that is insulated from identity chaos. By decoupling from the broader Identity stack they ensure user authentication works *with* their cloud transformation – not against it. IT teams can accelerate their cloud journey and future-proof the organization against user disruption caused by an always evolving Identity strategy.

2 Decoupling Accelerates Passwordless Initiatives

True Passwordless authentication is powerful, effective, and in high demand. It is one of the few cyber initiatives that satisfies the goals of security, IT and business leaders. Businesses that stay with the password-based products of their identity providers cannot easily migrate to passwordless. They are married to a password-based infrastructure. They find that they must decouple from legacy IAM to enable their next-gen authentication initiatives.

Leading IAM teams are well aware of the difference between passwordless marketing and passwordless MFA. Rather than wait for product roadmap promises to materialize, they are taking charge and accelerating the elimination of passwords on their own terms. Businesses are using these passwordless initiatives as an opportunity to deploy a focused authentication platform. Decoupling gives them quick time to value and a decisive win for IT leaders who can proclaim "We solved the password problem."

3 Decoupling Satisfies New Regulatory & Compliance Requirements

How do you know a space has gotten big? Standards and regulatory bodies take notice. A few noticeable compliance guidelines are influencing this focus on authentication.

- NIST 800-161* contains guidance towards supply chain separation of vendors. We are likely to see such separation of primary identity and MFA vendors as a consideration for meeting policy requirements.
- NIST (SP) 1800-17* also recommends FIDO as an optimal approach to MFA. This clearly distinguishes what Gartner calls "FIDO-Centric authentication" approach as superior to legacy MFA.
- PSD2 RTS Guidelines* describe the use of "separated software execution environments" such as a mobile device or secure element for achieving Strong Customer Authentication (SCA). The implication is that password-based legacy MFA is insufficient to secure consumer transactions – especially MFA that relies on shared secrets (e.g. OTP) or lacks a seperate execution environment for key storage.

Case Study

Challenge | Identity Fragmentation in the Enterprise

A leading North American financial institution had a large-scale initiative to simplify authentication for their employees, partners, contractors, and high net-worth clients. The IT org was required to support multiple Identity Providers, while more than 10,000 employees had to utilize 3 separate MFA apps in addition to 14-character complex passwords. What might cause such Identity Turmoil?

New Leadership can bring new strategic direction. Assume you have Okta deployed and are using Duo for 2-FA. Your new CIO is going all-in on Azure AD, bringing the Microsoft Authenticator app into the mix. Which MFA app is your primary login method? Are you going to switch employees from one app to another? Why is everyone still using passwords?

Mergers & Acquisitions introduce new Identity layers into an organization. Tying them together often requires significant time and effort and can create a fragmented environment for a team that is already juggling too many initiatives. Which identity platform is your source of truth? Who is the primary SSO? What about all the new customer identities that have been acquired?

Cloud and IT Strategy is constantly evolving and can push IAM in a whole new direction by introducing users to new products and processes. When IT strategy changes course, are you going to re-enroll the whole organization? Will this exercise be repeated upon similar circumstances?

Signs of Identity Turmoil

- MFA Fatigue
- User Disruption
- Reliance on Passwords
- MFA Gaps & Inconsistent Login Experiences

Solution | Unifiying Identity Experiences with True Passwordless SSO

This organization leveraged their cloud transformation budget to jumpstart their passwordless initiative. They focused on perfecting the authentication experience, leaving the IdP and SSO layer untouched. The result was a unified passwordless login across all identity products and services. Most importantly, users benefited from a passwordless login experience more than 300% faster than what they had before.

> The Benefit of Passwordless is Disrupting Authentication without Disrupting the User. - CISO

Fast, Consistent Login Experiences

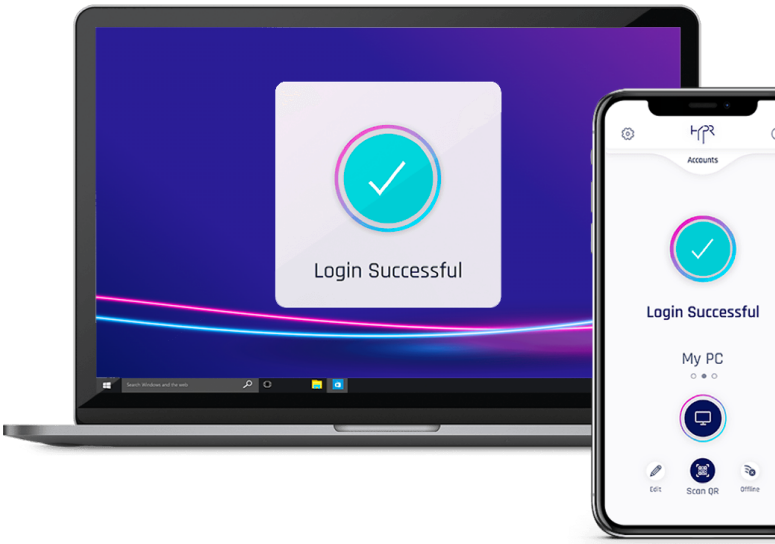
They replaced 3 separate password-based MFA apps with a single Passwordless app. Users are able to enroll in a single authentication layer that secures all mobile, web, desktop and SSO login experiences. User login became faster, easier, and consistent.

Rapid Password Elimination

The IT team was able to accelerate the rollout of passwordless authentication. The organization eliminated passwords faster than they anticipated – and they did so without the pain of managing a crowd of fragmented MFA apps, flows, and experiences.

Future Proof Authentication

They were able to offset any user disruption by future-proofing the user authentication experience against the constantly evolving IT initiatives.



Case Study

Challenge | A Healthcare Leader Eliminates Customer Passwords

Aetna, a CVS Health Company, is one of the world's largest health insurers and managed healthcare providers. As part of their digital transformation initiative, the company had a C-level directive to improve both user experience (UX) and security.

Going Passwordless Required a Next-Gen Approach

Security leadership needed the organization to move away from passwords since they were the target of credentials-based attacks, account takeover (ATO) and phishing. Beyond the security org, business leaders were aware that expensive password resets were impacting their bottom line. Despite heavy investments in a very mature identity program, Passwords were an especially difficult problem for the company. To Aetna, this meant moving away from passwords to what they called "Next Generation Authentication."

> You're not using your insurance app every day. Users often forget their passwords, especially when it's time to renew a policy. You can see thousands, millions of password reset calls in a small time frame. It's almost like a Password Armageddon.
>
> **- Abbie Barbir**
> **Senior Security Architect**

CVSHealth

Solution | Mobile ATO Fraud Plummets by 98%

CVS was able to integrate True Passwordless authentication across customer-facing iOS and Android apps. Today, more than 10 million users benefit from a true passwordless login experience that doesn't rely on legacy password-based MFA. These users who adopted the new passwordless authentication experience were safe from credentials-based vulnerabilities enabling the security and risk teams to decrease Account Takeover (ATO) fraud and reduce incident response costs that totaled millions of dollars. The impact was stunning - with more than 98% reduction in ATO.

Preventing the "The Password Armageddon"

The number of password resets also fell and resulted in a direct ROI. This is especially beneficial in the context of identity and access management (IAM), since the annual cost in password resets was the top expenditure for the security team.

Fast Time To Value and The Ability to Scale

Authentication speed and security increased, and so has the year-over-year increase in mobile engagement rates. By focusing on authentication, CVS can now quickly scale passwordless across a growing user base.

Case Study

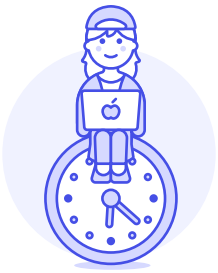
Challenge | A 100 Year Old Business Wants to Go Passwordless

As part of their digital transformation, the IT team decided to eliminate the use of passwords. They were satisfied with their Identity Providers and did not want to make any changes. The team had a C-Level directive to go passwordless.

Complex passwords were painful across the company. The incumbent identity products created a reliance on password-based MFA. Worst of all, customers were logging into mobile and web portals with nothing but a 12-character password. This led to a high volume of password resets and helpdesk calls.

Significant MFA adoption gaps were discovered as they evaluated the password problem. Workstation login, RDP, and VPN login were all areas that lacked MFA. These gaps were especially painful for employees who work remotely, travel often, and might use their workstation in public areas.

Password-based MFA reduced productivity. The IAM team had attempted to deploy a combination of Password + MFA login but users found it too painful. Some employees reported that when forced to use an additional authenticator, it could take up to 30 seconds to log into their desktop. Let's quantify that.



With complex passwords each successful workstation login averaged 5 seconds. An employee logs onto their computer approximately 12 times a day.

5 x 12 x 252 x 8,000 = 33,600 Hours or 3.8 Years!

Solution | They Saved 32,000 Hours in Employee Productivity

Passwordless enabled the IT team to secure access across all channels without the headache of managing a multitude of fragmented MFA apps, login flows, and remote access experiences.

> 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**

Enforced Lightning-Fast Desktop MFA
With Smart Card enforcement, Passwordless login became mandatory across the company.

Remote Services are Now Fully Protected
Employees now utilize Remote Services Such as VDI, VPN, and RDP without concerns about password theft.

Achieved Gartner's CARE
By deploying best-of-breed passwordless capabilities, they achieved Gartner's guidance for CARE - Consistent, Adequate, Reasonable, and Effective authentication.

Case Study

Challenge | New Regulation for Strong Authentication

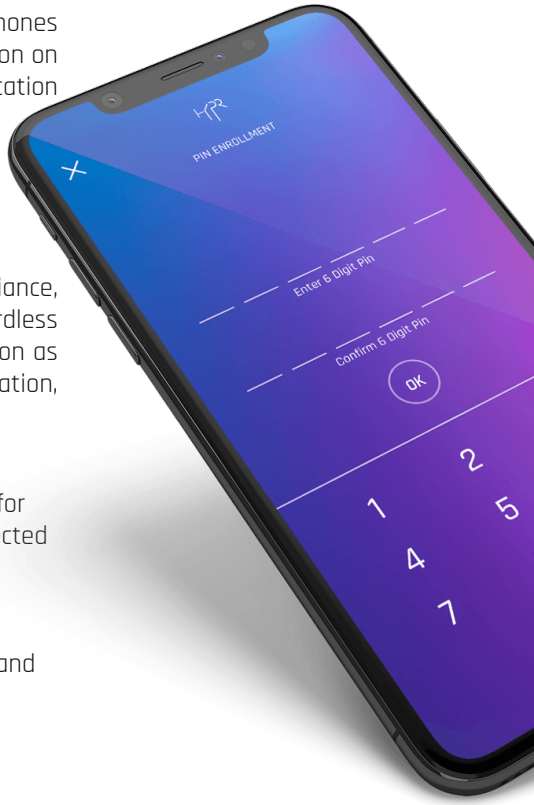
Ireland's largest health insurer is leading the way in passwordless authentication. VHI Healthcare expressed that this new approach to authentication was needed to satisfy PSD2 Compliance requirements. Specifically, they sought to address Section 9.3 of the Regulatory Technical Standards (RTS) which describes the use of "separated software execution environments" for achieving Strong Customer Authentication (SCA). This means passwords and legacy 2-Factor Authentication were 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.

Interoperability and Accessibility

VHI stressed the importance of deploying a mobile experience with best-in-class protection that was accessible and usable by all age groups, demographics, and devices. They requested a password-less experience that is easy to understand and intuitive for their customers, many of whom are senior citizens. A mobile passwordless authentication experience would improve usability - but the security team didn't want to stop there. Users needed to be able to authenticate with biometrics as well as more familiar knowledge-based factors such as PINs.

A Fragmented Device Ecosystem

Finally, they required that all devices be able to authenticate with the same consistent user experience. The device population was very diverse and fragmented. For example, legacy iPhone 5 devices would need to be supported as well. This presented a unique challenge as older iPhones lack a Secure Enclave and prevent most vendors from deploying passwordless authentication on such devices. A standard Identity Platform was not enough need for a dedicated authentication platform was clear.



Solution | Straight to PSD2 Compliance

VHI decided on passwordless authentication as a fast and simple way to meet PSD2 compliance, eliminate fraud, and enhance user experience. VHI quickly integrated True Passwordless authentication into their consumer-facing mobile applications. By focusing on authentication as its own initiative, the company was able to address their uniquely complex device fragmentation, compliance, and accessibility requirements.

Password Pain Eliminated

VHI's elimination of passwords has increased security for the company and for their customers, who enjoy faster authentication experiences that are protected against credential reuse.

Consistent Authentication, Anywhere, Any Device, Anytime

VHI ensured that passwordless authentication would be fully interoperable and that all devices would be covered, even legacy smart phones.

Steep Drop in Password Reset Costs

The company enjoys less password resets and by extension they are seeing a steep decline in the number of customer service requests. In an industry where password resets can send service costs sky-high, VHI remains many steps ahead.

It's Time to Decouple Authentication From Identity

As businesses move to the cloud they must choose between adopting a single identity platform or having to maintain multiple fragmented identity systems. Resource-constrained IT teams are forced to stitch together multiple IdPs while end-users juggle numerous multi-factor login methods with increasingly complex and inconsistent user experiences.

The abundance of commoditized MFA products has failed to solve the password problem. Legacy IAM products have married businesses to the use of passwords, making it difficult to progress to next-gen authentication. Information Security teams still struggle to close gaps in MFA coverage; and despite having more ways to log in than ever before, businesses remain heavily reliant on passwords.

It's time to move authentication forward.

Decoupling authentication has allowed leading IAM teams to neutralize this identity turmoil. By insulating themselves from the cloud wars they are finally able to acclerate digital transformation, solve MFA gaps, and deliver on the promise of passwordless.

Such businesses are providing their users a consistent authentication experience that is fast and easy to use. Their IT teams have the ability to support constantly evolving identity initiatives without the headache of managing a multitude of fragmented identity and MFA products. They have unified consistent authentication with a continuously evolving identity strategy.

To Learn more:

PASSWORD ELIMINATION GUIDE

www.hypr.com/password-elimination

PASSWORDLESS REMOTE WORK GUIDE

www.hypr.com/passwordless-remote-work-force-guide

NOT ALL FIDO IS THE SAME

www.hypr.com/not-all-fido-is-the-same-white-paper

HYPR is the Passwordless Company backed by Comcast, Samsung, and Mastercard.

Passwords and shared secrets remain the #1 cause of breaches despite billions of dollars invested in cyber security. The HYPR Passwordless Cloud makes it easy to go Passwordless across the enterprise by combining the convenience of a smartphone with the security of a FIDO token.

With HYPR, businesses are finally able to solve the MFA gap, eliminate customer passwords, and deliver lightning-fast login experiences their users love.

Go Passwordless Now at www.HYPR.com