DECOUPLING AUTHENTICATION FROM IDENTITY PROVIDERS

Introduction

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.

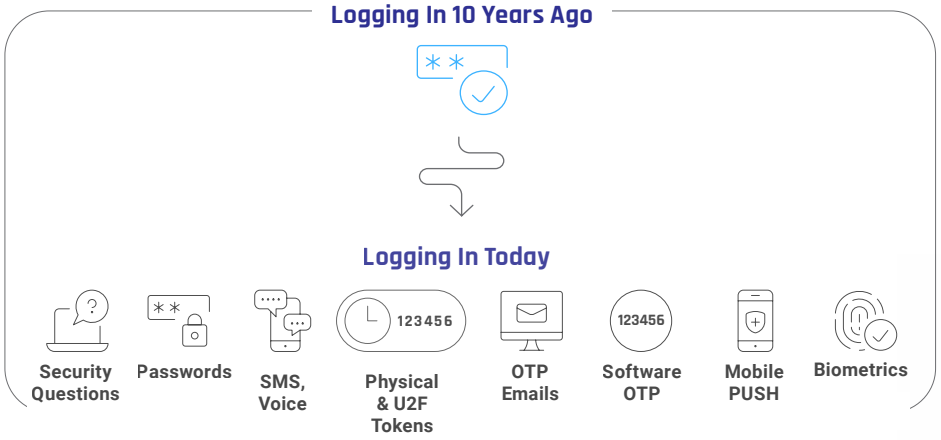
Cloud Wars and Identity Turmoil

Authentication has Become Too Complicated

There was a time when 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 smartphones became ubiquitous across the enterprise, the identity platforms saw an opportunity to merge MFA with their products. Soon everyone had a dedicated MFA app baked into their Identity suite. Today there are over 300 authentication vendors. Now, the drawerful of RSA tokens has been replaced by a smartphone full of MFA apps.



Users Struggle with MFA Fatigue and Password Pain

Fast forward to today. People use multiple methods 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 find it difficult to maintain a consistent user experience. Complaints about password complexity, a sense of reduced productivity and "MFA fatigue" abound.

MFA has been commoditized and increasingly mandated, yet most businesses still meet resistance from 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. A 2021 report by Twitter found that only 2.3% of its active accounts use multi-factor authentication and Microsoft recently admitted just 11% of its enterprise cloud users enabled MFA.

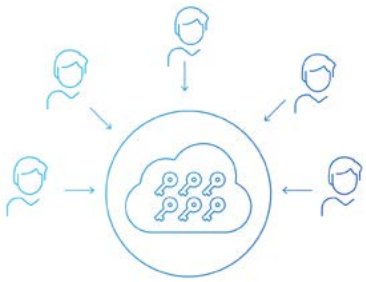
Businesses have more MFA options than ever and yet still have gaps in user adoption. The worst part? Everyone still uses passwords.

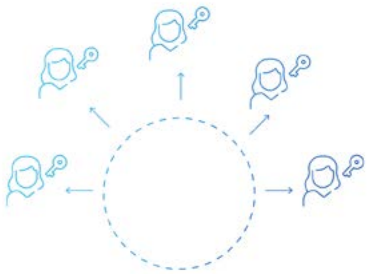
Looks familiar?
MFA Fatigue is a growing problem

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 addressed the compliance checkbox. Most mainstream push, OTP, SMS, or soft token products utilize a similar combination of passwords with symmetric cryptography to provide a multi-factor authentication experience.

In the late 2010s "True Passwordless" authentication gained traction. Unlike legacy MFA, such passwordless 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. However, the same approach that made it easy for Identity products to commoditize MFA is the reason many 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 Simplified, Fast User Experience
- Replaces Passwords with Public-Key Encryption
- Stops Credential Stuffing, Fraud and Phishing
- Solves Customer and Desktop MFA Gap

Passwordless MFA Demands a Different Approach

As organizations became aware of the problems with the password-based MFA that incumbent identity vendors provide, they focused their attention on next-gen solutions such 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 tools are really only adding a single extra factor"
> **- Gartner**

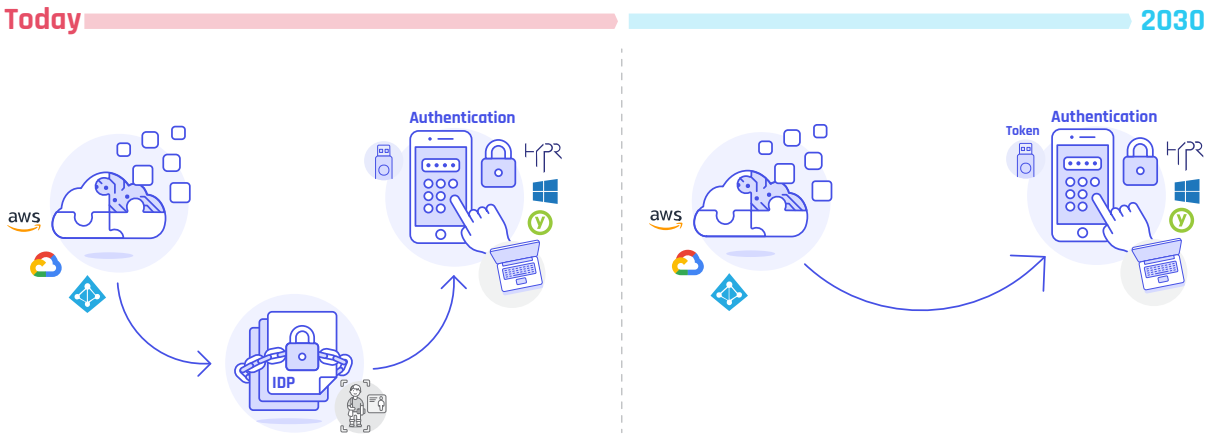
Legacy MFA products were prone to silos and vendor lock-in while the new school of authentication focuses on interoperability. Bringing together open standards such as FIDO2 and SAML, they emphasize interoperability and integration with identity platforms rather than working to displace them. This new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

Analysts have also taken note. Gartner, for example, separates "User Authentication" from the broader Identity Access Management category. In their 2020 Market Guide for User Authentication, Gartner states, "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."

Identity Is Now Being Commoditized by the Cloud

The cloud wars rage on with Amazon, Microsoft and Google building more and more identity and access management features into their massive platforms. Microsoft claims that Azure AD manages more than 1.2 billion identities and processes over 8 billion authentications every day. Identity is a core component of the cloud story and as these industry titans continue to expand their offerings, third party identity providers (IdPs) risk being commoditized.

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 resource-constrained IT teams. And while SMBs and new products born in the cloud may never encounter the need for a third party IdP, they too suffer from 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 applications 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 large number of organizations have realized that they cannot solve their authentication challenges by continuing to rely on the password-based MFA provided by their incumbent IAM vendors.

3 key drivers stand out:

1 Decoupling Allows You to Leverage True Passwordless MFA

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 alike. Businesses that stick with the password-based MFA products of their identity providers are married to a password-based infrastructure that at best can tack a passwordless experience on top. Leading IAM teams realize that they must decouple from legacy IAM to enable their next-gen authentication initiatives. Rather than wait for product roadmap promises, they are accelerating the elimination of passwords on their own terms. Decoupling gives them quick time to value and a decisive win for IT leaders who can definitively state, "We solved the password problem."

2 Decoupling Mitigates Identity Turmoil and User Disruption

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.

Savvy businesses are investing in next-gen authentication platforms that are distinct from their identity providers for a consistent, secure authentication experience. By decoupling from the broader Identity stack, they ensure user authentication works with their cloud initiatives — not against them. IT teams can accelerate their cloud transformation and future-proof the organization against user disruption caused by an always evolving Identity strategy.

3 Decoupling Satisfies New Regulatory & Compliance Requirements

How do you know a space has gotten big? Standards and regulatory bodies take notice. Several significant 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" 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 MFA is insufficient to secure consumer transactions — especially MFA that relies on shared secrets (e.g. OTP) or lacks a separate execution environment for key storage.
- 2021 FFIEC Guidance on Authentication and Access to Financial Institution Services and Systems calls for MFA as part of layered security, citing the above NIST standards as reference sources for implementers.

Equally telling? Cyber insurers are now demanding similar authentication standards in order to obtain coverage.

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. Leadership changes, mergers and acquisitions and evolving IT strategies meant that the IT org was supporting multiple identity providers, while more than 10,000 employees had to utilize three separate MFA apps in addition to 14-character complex passwords.

Solution: Unifying Identity Experiences with True Passwordless SSO

The 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 unified passwordless login across all identity products and services. Most importantly, user login speeds increased by 300%

- **Fast, Consistent Login Experiences:** They replaced three 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 accelerated the rollout of passwordless authentication, hitting their milestones faster than scheduled — without the pain of managing a crowd of fragmented MFA apps, flows, and experiences.
- **Future Proof Authentication:** They offset any user disruption by future-proofing the user authentication experience against the constantly evolving IT initiatives.

CASE STUDY

CVS Health

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.

Security leadership needed the organization to move away from passwords since they were the target of credential-based attacks, account takeover (ATO) and phishing. Moreover, costly password resets were impacting the company's bottom line.

Solution: ATO Fraud and Password Reset Costs Plummet

CVS integrated True Passwordless authentication across customer-facing iOS and Android apps. Today, more than 10 million users benefit from a frictionless passwordless login experience that keeps them safe from credential-based attacks.

- **Strengthened Security:** The security and risk teams decreased Account Takeover (ATO) fraud by more than 98% and reduced incident response costs that had totaled millions of dollars.
- **Sharp Reduction in Password Resets:** Password resets fell drastically, resulting in direct ROI. The annual cost in password resets had been a top expenditure for the security team.
- **Fast Time to Value and the Ability to Scale:** Along with authentication speed and security gains, the year-over-year mobile engagement rates increased. By focusing on authentication, CVS can quickly scale passwordless across a growing user base.

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

CASE STUDY

Challenge: New Regulation for Strong Authentication

VHI Healthcare, Ireland's largest health insurer, needed to satisfy PSD2 Compliance requirements, specifically, 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 two-factor authentication were no longer sufficient 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 needed passwordless authentication that would be intuitive for their customers, many of whom are senior citizens. The security team also wanted users 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, presenting a unique challenge. For example, legacy iPhones, which lack a Secure Enclave, would need to be supported as well.

> "The ability to deliver strong passwordless authentication to our customers who are using the VHI App is critical for a secure digital health experience. HYPR's passwordless authentication has simplified and improved the experience for our customers without compromising on security."
>
> **- Damien Mullan**
> IT Manager, VHI Healthcare

Solution: Straight to PSD2 Compliance

VHI decided on True Passwordless authentication as a fast and simple way to meet PSD2 compliance, eliminate fraud, and enhance user experience. 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 smartphones.
- **Steep Drop in Password Reset Costs:** Along with authentication speed and security gains, the year-over-year mobile engagement rates increased. By focusing on authentication, VHI can quickly scale passwordless across a growing user base.

It's Time to Decouple Authentication From Identity

As businesses move to the cloud they must choose between adopting a single identity platform or maintaining 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 handcuffed 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 businesses remain heavily reliant on passwords.

It's time to move authentication forward.

Decoupling authentication has allowed leading IAM teams to accelerate digital transformation, solve MFA gaps, and deliver on the promise of passwordless. Such businesses are providing their users a consistent, simple, secure authentication experience while enabling their IT teams to support a continuously evolving identity and security strategy.

THE PASSWORDLESS COMPANY

Contact: 1-866-GET-HYPR [US]

Learn more: www.hypr.com

HYPR reimagines multi-factor authentication to protect workforce and customer identities at the highest level of assurance. With HYPR True Passwordless™ MFA, you can change the economics of attack, improve your security posture, and enhance digital engagement with every login experience.