THE EVOLUTION OF

AUTHENTICATION

This white paper from Goode Intelligence & HYPR explores the evolution of authentication over the last 50 years. From passwords and 2-Factor Authentication to True Passwordless Security and the era of Zero-Trust, we review how user authentication has changed over the years and where it is headed.

HYPR

AUTHENTICATION IS EVOLVING BEYOND SHARED SECRETS

Account Takeover Fraud (ATO) costs have doubled in the past 2 years.

Malicious logins account for more than 90% of eCommerce traffic.

Credential stuffing attacks are at all-time highs, costing the US banking industry $50 million on a daily basis.

More than half of all companies in the UK fell victim to phishing attacks in the past 2 years.

Between passwords, multi-factor authentication, security tokens and biometrics, internet users have more ways than ever before to secure their digital identity. And yet, these statistics tell a story of a digital identity problem that worsens every year.

Passwords were invented in the 1960's. Fast forward to 2019 and much of the world is still dependent on a 50-year-old technology for securing access to online services and IT resources Stronger 2-Factor Authentication solutions are widely available but they are not widely adopted – with estimates suggesting deployment to less than 10 percent of internet users. In fact, the 2019 Internet Trends Report by Mary Meeker estimated that global adoption of 2FA has actually stalled in the low 50% range.

With so many authentication methods you would think that Account Takeover stats would be getting better, not worse.

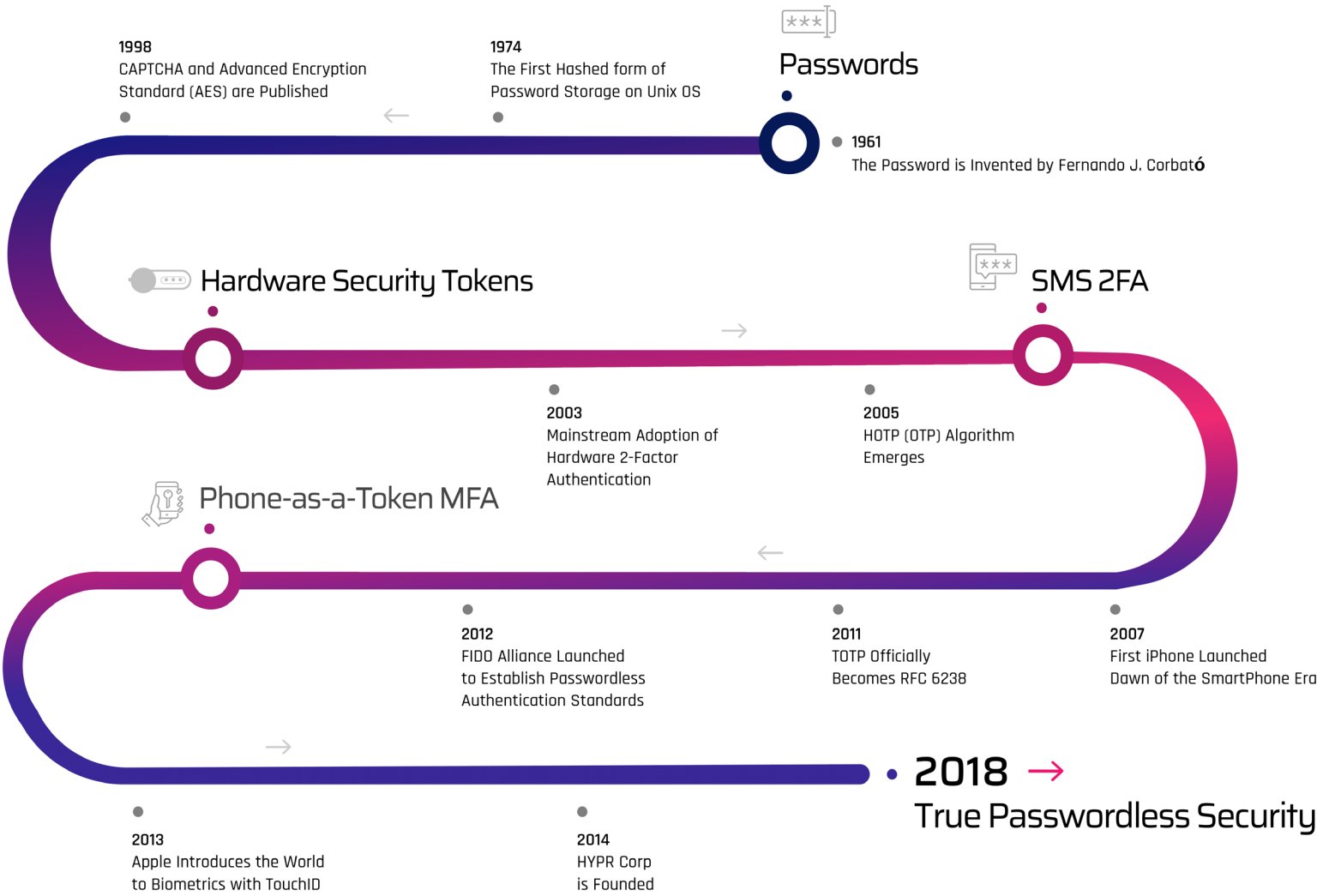
Shared Secrets Have Always Been the Problem.

The problem is that passwords, 2FA and legacy multi-factor authentication solutions have one thing in common – they rely on shared secrets. That means that a user has a secret, and a centralized authority holds the same secret. When authenticating, those two secrets are compared to approve user access. If a malicious 3rd party intercepts the secret, they can impersonate the user.

The bad news is that this reliance on shared secrets has kept large populations of users vulnerable to phishing, credential stuffing attacks, and password reuse while contributing to the steep rise in Account Take Over (ATO).

The good news? The Digital Identity landscape is about to change very quickly.

A BRIEF HISTORY OF TRUST...



User authentication technologies have evolved. The world is rapidly moving away from proprietary, monolithic authentication methods that rely on shared secrets to standards-based passwordless solutions that prioritize security and usability.

In order to predict where digital identity is heading, we must first understand how we got here. This paper provides a brief timeline of the history of digital authentication, an overview of various popular authentication methods, and an Authentication Attack Matrix that explores how these approaches stack up against one another.

PASSWORDS

Back in 2014, the inventor of the computer password, Fernando J. Corbató, went on record to say that his invention has become "kind of a nightmare." Corbató invented the password around 1961 when he was working at MIT on the then revolutionary Compatible Time-Sharing System (CTSS). The problem the password was solving was to ensure that these early pioneers of computer engineering were able to log onto "multiple" terminals to ensure they access their own records.

When they spoke of "multiple" the team was referring to only a handful of connected green-screen terminals. Fast-forward nearly 60 years and Corbató's invention is still the dominant login access method – underpinning the vast majority of today's authentication sessions. Passwords authenticate billions of sessions daily on billions of devices ranging from laptops to smart mobile devices with touchscreens and even connected cars – but just how bad is the password problem?

Credential Stuffing has become an epidemic - with malicious logins accounting for more than **56%** of consumer banking traffic.

More than 5 Billion passwords have been stolen since 2016. Weaponizing those stolen passwords has never been easier, with tools like SNIPR making it easier than ever to launch an attack. The cost of an attack has gone down for the hackers, while the cost to defend has drastically increased for enterprises.

Credential stuffing attacks are at all-time highs - with Akamai reporting more than "**30 Billion malicious login attempts** in less than a year." According to SANS Analyst Research, credential reuse attacks can achieve **success rates of up to 1% - 2%**.

Add these trends together and it's no surprise that **ATO Fraud costs have doubled year over year** to more than $1.7B in 2018, according to the 2019 Javelin Strategy "Cloud Conundrum" Report.

"This massive migration of applications from inside the firewall to the cloud, coupled with widespread customer password breaches are key contributors to the steep rise in ATO and its costs. "

Al Pascual, Javelin Strategy
"The Cloud Conundrum" Report

HARD TOKEN 2FA

If you've worked in a large enterprise, chances are you've used one of these. When hardware security tokens became popular they brought the world more security, using time-based one-time password (TOTP) algorithms and tamper-resistant hardware. Hard tokens introduced a "second-factor" to authentication (2FA) and were good at providing additional standards-based security for authentication sessions that needed a higher level of assurance. These devices promised to provide an additional layer of security above passwords – but over the years have been found to possess a number of user experience drawbacks as well as security vulnerabilities.

Token sharing is common practice in corporations, where employees are known to pass around a hard token as if it were a password on a sticky note.

Malicious attacks are also commonplace as hard token OTPs can be captured either by **keyloggers** or **man-in-the-middle attacks**, creating additional security concerns for enterprises.

But the hard token's most challenging aspect remains its usability – with users often responding unfavorably to the **added friction** caused by the mandatory use of an additional device.

As the world moved beyond desktops to the mobile device, hard tokens became even more clunky to use and added significant friction to the user experience. The resulting **lack of adoption among consumers** created another hurdle to mass adoption of hard token-based 2FA.

SMART CARDS

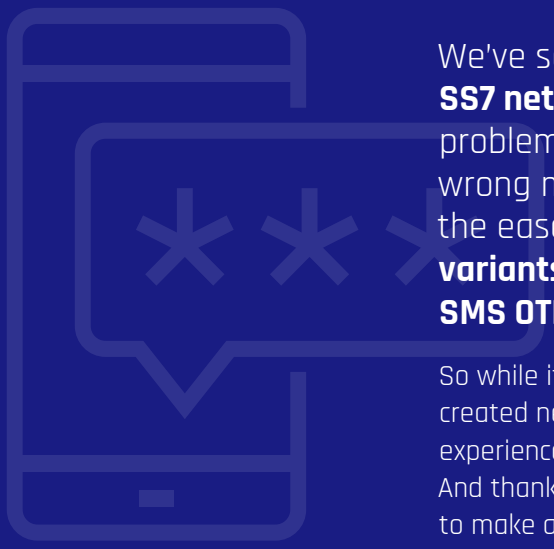
Smart cards are those plastic cards you see in enterprises and government facilities. They contain an embedded microprocessor and are carried or worn by employees for identification, authentication, physical access, and even financial transactions. In the public and financial sectors, smart cards have been successfully deployed in mission-critical settings where the use of mobile phones is unsupported due to security concerns.

Smart cards and hard tokens share similar usability issues, but a key advantage is security. Because they primarily rely on Public Key Infrastructure (PKI), smart card authentication often replaces the use of shared secrets and meaningfully improves security.

SMS 2FA

The mobile era introduced SMS authentication using the TOTP methods that were popularized by hard tokens.

Instead of generating an OTP on a separate piece of hardware, a server generates the code and delivers it to the user via SMS to their mobile device. As most people have a mobile phone of some kind, avoiding the cost of a hardware token has led many service providers to adopt 2FA SMS for large-scale consumer use. It is still the most widely adopted 2FA method in use today and can be considered the "hard token equivalent" of the consumer use case - but SMS based authentication carries significant risks that have all but stalled its growth.

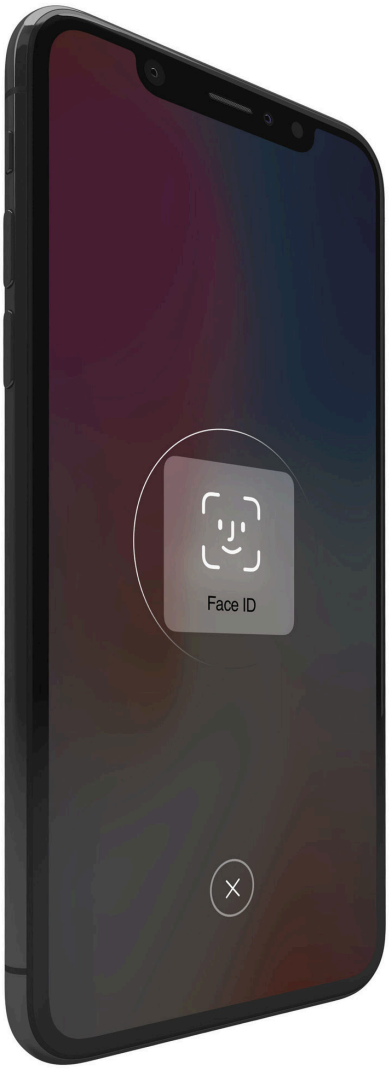


We've seen how easily SMS messages can be intercepted via **SS7 network attacks**, how the commonplace **SIM-Swapping** problem can result in OTP messages being delivered to the wrong mobile phone – usually in the hands of fraudsters - and the ease with which popular **keyloggers and mobile malware variants** such as Modlishka come equipped with **automated SMS OTP stealing** functions.

So while it was less expensive for service providers, the SMS 2FA approach created new security problems while adding noticeable friction to the user experience by having to type in the OTP into the mobile device or web browser. And thanks to a reliance on shared secrets, this approach to authentication failed to make a meaningful impact on user security.

VULNERABILITIES IN SMS 2FA LED TO A TIPPING POINT WHEN THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) STOPPED RECOMMENDING THE USE OF SMS AS A STRONG SECOND FACTOR IN JULY 2016.

PHONE-AS-A-TOKEN MFA



Soft token MFA went mainstream as businesses and their users shifted towards mobile devices. These methods popularized software-based One-Time-Passwords (OTP), and managed to replace a large segment of the hard tokens with PIN, PUSH or biometric based MFA.

Once popular among businesses and developers, there are many known weaknesses in many of the software based two-factor and multifactor authentication (2FA/MFA) systems. Some of the most popular authentication methods that leverage One Time Passwords (OTP) happen to rely on shared secrets - leaving users susceptible to **social engineering, mobile malware and man-in-the-middle (MitM) attacks**.

Phishing sites that impersonate 2FA login interfaces have grown in popularity, with attacks deployed at scale targeting large populations such as Gmail users[1]. Even major MFA providers such as Microsoft have experienced signifcant attacks, **with Hackers bypassing MFA by exploiting IMAP protocols** [2].

A recent study commissioned by Stripe has shown that even soft token MFA is seeing **little adoption among consumer-facing applications -** with merchants citing a fear of increased cart abandonment rates as a key driver for not introducing friction to their customer experience.

TRUE PASSWORDLESS SECURITY

This is the next step in the evolution of authentication. Unlike its predecessors, this approach does not rely on the use of shared secrets. Instead, private keys stored on a user's trusted device are used to access online services and sign transactions.

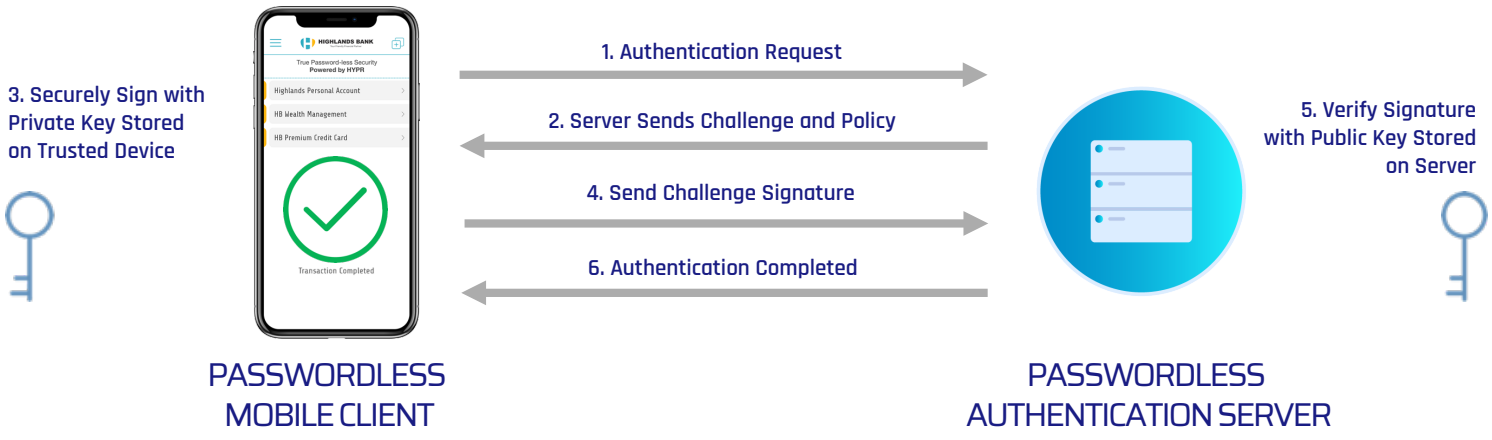
In a true passwordless architecture, the use of shared secrets such as passwords, PINs, SMS codes and OTPs is replaced with public-key cryptography.

Private keys are generated by the user on their device and remain on-device at all times. Biometric sensors such as Apple's Touch ID, Face ID and their Android & 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. This approach has seen significant momentum with adoption both inside and outside the enterprise as well as large-scale deployments across the financial services, payments, healthcare and eCommerce sectors. Many true passwordless deployments leverage open standards such as FIDO (Fast Identity Online), taking advantage of a layer of interoperability and innovation that was previously missing from the IAM space.

How it Works

True Passwordless Security Combines the use of Public Key Cryptography, Open Standards, and Biometric Sensors to create a completely passwordless authentication flow.



THE PARADIGM SHIFT AWAY FROM SHARED SECRETS... WHY NOW?

Adoption of PKC-based Authentication Standards such as FIDO

Security standardization has led to some of the internet's greatest achievements. Would secure eCommerce been achievable without SSL/TLS standards? FIDO Authentication standards are the leading example of what a true passwordless framework should embody and have successfully driven organizations of all sizes to move beyond passwords and shared secrets.

Mainstream Adoption of Mobile Biometric Sensors

Almost every smartphone shipped today is equipped with one or more advanced biometric sensors. The rise of fingerprint, face, iris and voice recognition has made it easier for enterprises to deliver passwordless experiences across large user populations.

Major Browsers Now Support Passwordless Authentication

As of 2018, the FIDO Web Authentication standard (WebAuthn) is supported by major web browsers such as Chrome, Safari, FireFox and Edge. This major milestone brought support for true passwordless security to an even wider web audience - further accelerating adoption.

PSD2 Regulations Are Enforcing Strong Customer Authentication

The European Union's (EU) PSD2 Strong Customer Authentication (SCA) regulation is creating a regulatory framework for payment service providers to adopt the latest strong authentication technology, explicitly supporting the use of passwordless and biometric authentication as one of the supported factors.

Microsoft

Google

Tech Giants Accelerating Large-Scale Passwordless Initiatives

Industry leaders such as Microsoft and Google. Azure Active Directory (Azure AD) simplifies authentication for application developers by providing identity as a service, with support for industry-standard protocols such as OAuth 2.0 and OpenID Connect.

HOW DO THEY ALL STACK UP?

Authentication has evolved beyond monolithic systems that rely on shared secrets to true passwordless technology. A global evolutionary movement to replace passwords is well under way.

The paradigm shift away from shared secrets is happening and organizations should embrace it to avoid an endless cycle that leads to data breach, credential theft and ultimately to costly events such as account takeover and financial fraud. With all that said, how do the various approaches compare to one another? The below table heat-maps many known security threats and advantages, it is offered to arm executives and practitioners with added knowledge on which to base critical authentication sourcing decisions.

	RELY ON SHARED SECRETS				NO SHARED SECRETS	
NIST 800-63B Threat Category	Static Passwords	SMS 2FA	Phone-as-a-Token MFA	Hard Token 2FA	Smart Cards (PKI)	True Passwordless
Security	Low	Low	Medium	High	Very High	Very High
Theft	- Usually Stored In One Place - Users Write Them Down - Can Easily Be Shared	- OTP Easily Stolen and Reused - Only as Secure as Mobile Device - Common SS7 Network Attacks	- OTP Easily Stolen and Reused - Only as Secure as Mobile Device	- OTP Difficult to Steal and Reuse - Not Bound to Particular User	- Card Can be Stolen and Reused - Only as Secure as PIN On Card - Attacks Are Highly Targeted	- Attacks Must Be Highly Targeted - Attackers Must Have Root Access to Mobile OS
Duplication	- Written Down and Duplicated - Backups Are Easily Made	- Backups Are Often Made - Duplicated By Cloning App Data	- Backups Are Often Made - Can be Duplicated By Cloning Application Data	- Seed Backups Are Often Made (e.g. RSA Breach)	- Not Easily Duplicated - Highly Targeted	Highly Targeted and Extremely Difficult Without Physical Access to Silicone On Chip
Eavesdropping	Malware and MITM Commonly Used to Exploit	Can Be Intercepted By Malware, MITM, and Keyloggers	OTP and MPC Can Be Intercepted By Malware and MITM	MITM Commonly Used to Exploit	- PIN Can Be Intercepted Between PC and Card Reader	Extremely Difficult Without Physical Access to Silicone On Chip
Offline Cracking	Hashed / Encrypted Passwords Can Be Cracked Offline	Hashed or Encrypted OTP/HOTP Secrets Can Be Cracked Offline	Hashed or Encrypted Secrets Can Be Cracked Offline	Hashed or Encrypted OTP/HOTP Secrets Can Be Cracked Offline	- Very Difficult, Must Be Able to Decrypt and Exploit Chip	Extremely Difficult Without Physical Access to Silicone On Chip
Side Channel Attacks	Password Size and Complexity Can Be Established Through Side Channel Analytics and Differential Power Analysis	Can Be Sniffed or Intercepted By Other Apps or Malware	- Exposed to Credential Stuffing If Using Passwords as Alias - Can Be Sniffed or Intercepted By Other Apps or Malware	Exposed Using Differential Power Analysis	Possibly Exposed to Differential Power Analysis	Possibly Exposed to Differential Power Analysis by a Very Sophisticated Attacker.
Phishing or Pharming	Passwords Are The Primary Target Of Phishing	Targeted 2FA SMS 2FAPhishing (i.e. Modlishka Tool)	- OTP Susceptible to Phishing - PUSH Attacks Require Social Engineering (See Below)	Targeted 2FA Phishing (Ii.e. Modlishka Tool)	Not Possible Since Each Authentication Request is a Unique Challenge-Response	Not Vulnerable, as Each Authentication Request is a Unique Challenge/Response
Social Engineering	Users and Admins Duped Into Giving Password Through SE Attacks	Attacker Retrieves MFA Code Directly from User	Attacker Convinces User to Authenticate PUSH. Difficulty Depends on Implementation	Attacker Retrieves MFA Code Directly from User	Extremely Difficult as User Does Not Utilize Shared Secrets	Not Vulnerable, User Does Not Have a Shared Secret
Online Guessing	- Passwords Are Easy to Guess - People Reuse Passwords Across Multiple Services	Difficult to Guess a TOTP	- Password-Based Alias Vulnerable to Credential Stuffing & Reuse Attack - Difficult If Based on TOTP Alias.	Difficult to Guess a TOTP	Not Vulnerable to Guessing Due to PKI Architecture	Not Vulnerable as Public/Private Key Pairs Are Used to Perform a Challenge/Response Mechanism
Endpoint Compromise	Vulnerable to Keyloggers, Malware	Vulnerable to Keyloggers, Malware	Vulnerable to Keyloggers, Malware	Vulnerable to Keyloggers, Malware	Not Vulnerable as Private Keys Always Remain On Smart Card	Not Vulnerable as Keys Never Leave Hardware Backed Key Store

HYPR AUTHENTICATION ATTACK MATRIX 2019

ABOUT GOODE INTELLIGENCE

Goode Intelligence is an independent analyst and consultancy company that provides quality advice to global decision makers in business and technology.

Goode Intelligence works in information security, mobile security, authentication and identity verification, biometrics, enterprise mobility and mobile commerce sectors.

Founded in 2007 by Alan Goode and headquartered in London, Goode Intelligence helps both technology providers, investors and IT purchasers make strategic business decisions based on quality research, insight and consulting.

Goode Intelligence works with a cross-section of clients, from global brands that are ranked on the FTSE/ Fortune 100 to start-up technology companies.

www.goodeintelligence.com

ABOUT HYPR CORP

HYPR is the leading provider of True Passwordless Security with millions of users deployed across the Global 2000. Shared secrets are the #1 cause of enterprise breaches, fraud and phishing attacks. HYPR is the first Authentication Platform designed to eliminate passwords and shared secrets - effectively removing the hackers' primary target while eliminating fraud, phishing and credential reuse for consumers and employees across the enterprise.

www.HYPR.com

THANK YOU

HYPR CORP

GETSECURED@HYPR.COM