



THE PASSWORDLESS DECADE



INTRODUCTION

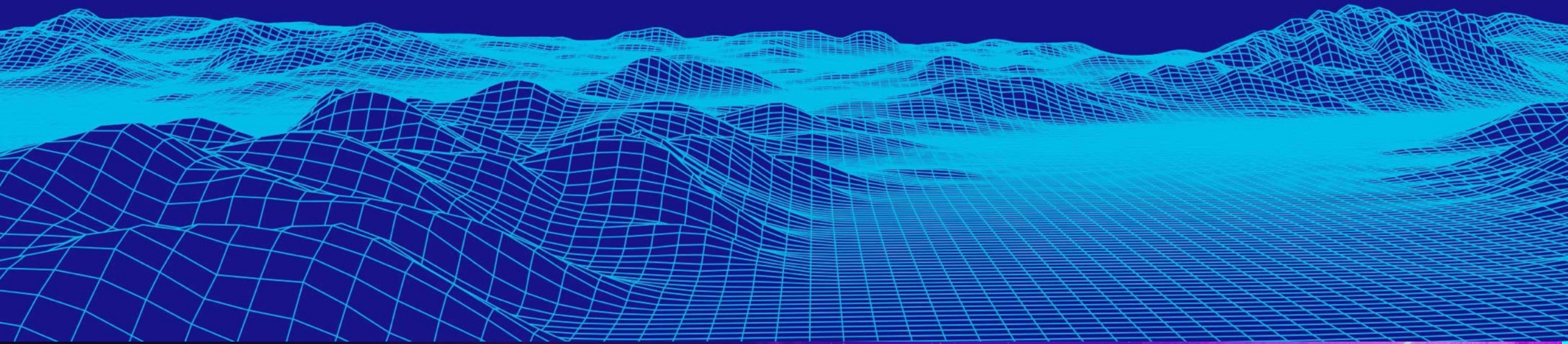


George Avetisov
CEO & Co-Founder of HYPR

Email: george@hypr.com

WHAT THIS TALK IS ABOUT

- Why is Credential Reuse at All-time Highs?
- How has Authentication Evolved?
- Why this is the Passwordless Decade



CREDENTIAL REUSE IS AT ALL TIME HIGHS

\$1.7B

Account Takeover (ATO) Fraud
Costs have Doubled Since 2015

+56%

Of Consumer Banking Traffic
are Malicious Login Attempts

+30B

Login Attempts in 2018 were
Credential Stuffing Attacks

"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."

JAVELIN

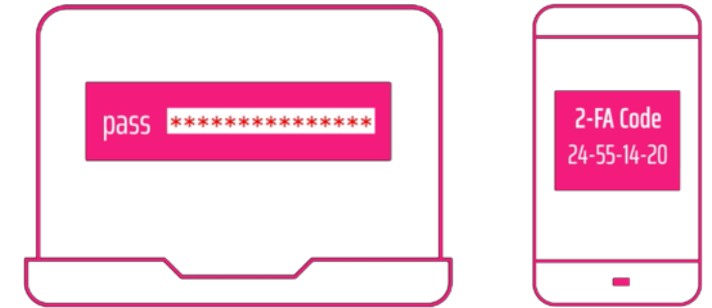
COST OF THESE ATTACKS HAS DECREASED FOR THE ADVERSARY AND INCREASED FOR THE ENTERPRISE



Cloud Transformation has
Increased the Attack Surface



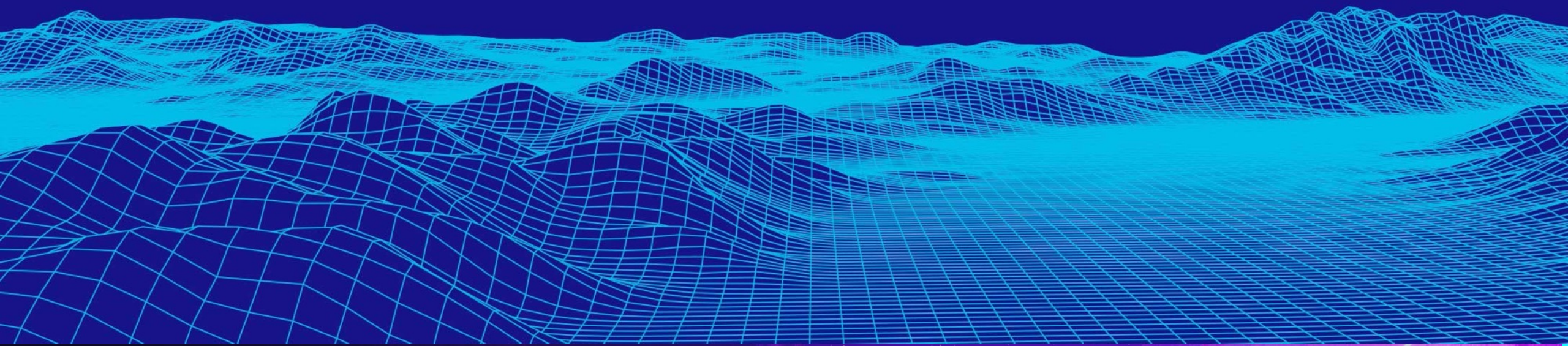
Tools Like SNIPR and Modlishka
Are Easy to Use



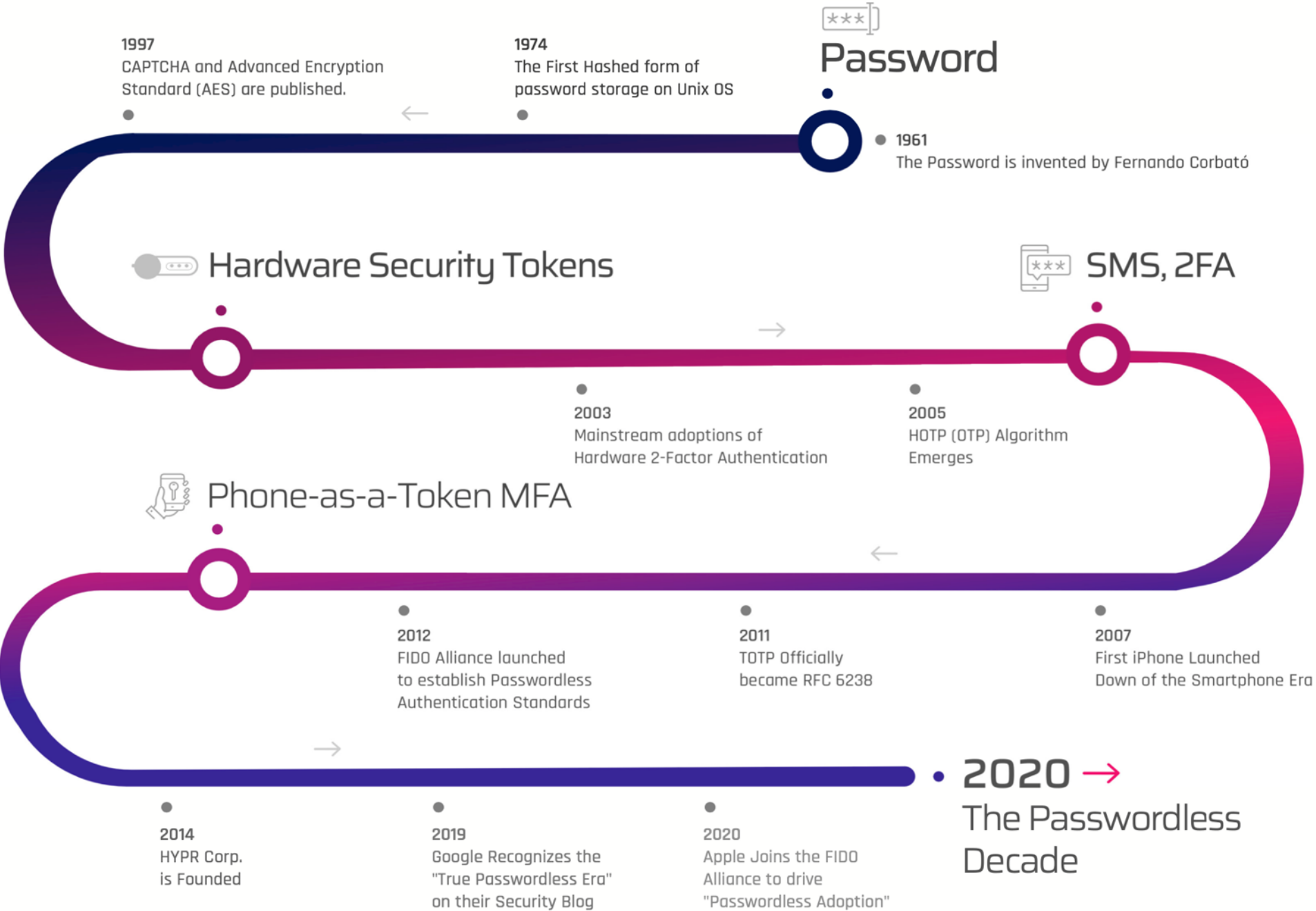
Despite Millions Invested,
MFA Adoption has **Stagnated**
Since 2015

HOW

DID WE GET HERE?

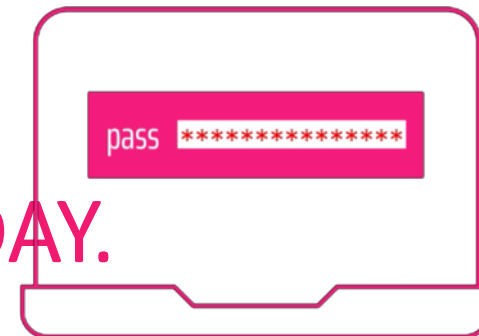


A BRIEF HISTORY OF TRUST



PASSWORDS

INVENTED IN 1961..... STILL USED TODAY.

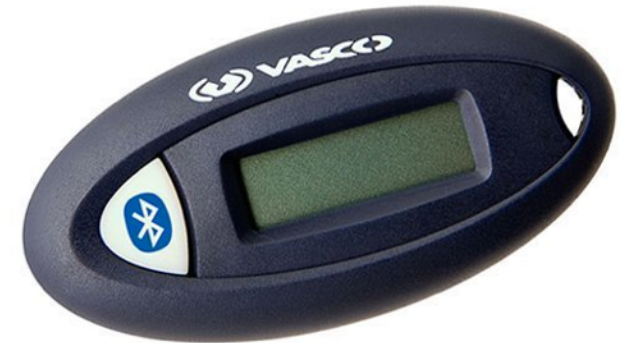
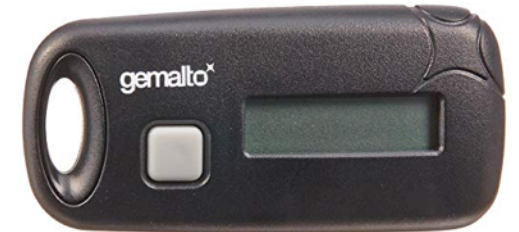


Charlie Ciso



HARD TOKEN 2-FA

HIGH FRICTION - LOW ADOPTION - OFTEN SHARED



SMART CARDS

POPULARIZED PKI - NICHE ADOPTION



SMS 2FA

BROUGHT MFA TO THE MASSES - DEPRECATED BY NIST

IN 2016

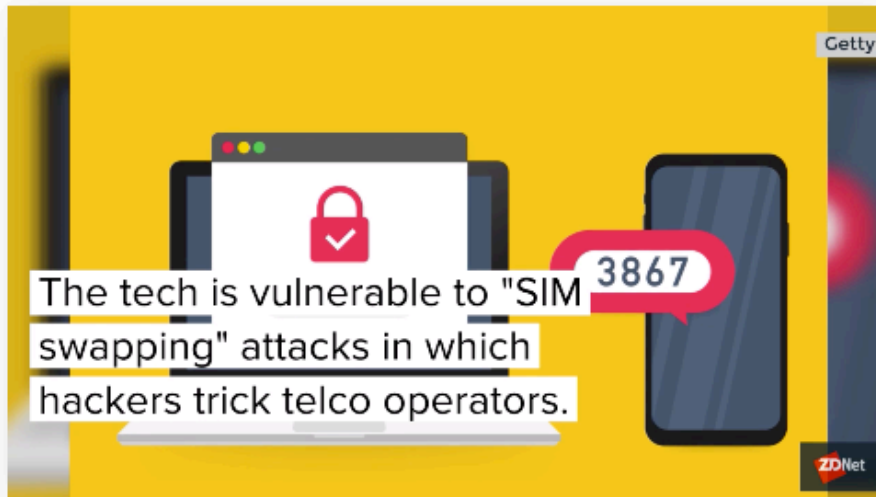


German banks are moving away from SMS one-time passcodes

New EU legislation might help kill SMS 2FA / 2SV / OTP.



By [Catalin Cimpanu](#) for [Zero Day](#) | July 11, 2019 -- 12:28 GMT (05:28 PDT)
| Topic: [Security](#)



Schneier on Security

[Blog](#)

[Newsletter](#)

[Books](#)

[Essays](#)

[News](#)

[Talks](#)

[Academic](#)

[Blog](#) >

NIST is No Longer Recommending Two-Factor Authentication Using SMS

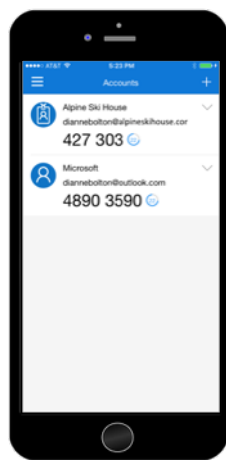
09.04.19

Twitter just disabled its SMS tweet feature after CEO Jack Dorsey got hacked

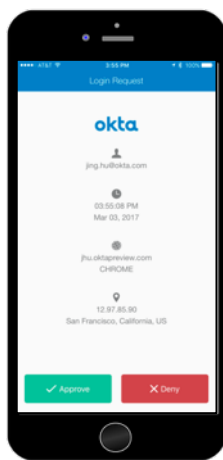


PHONE AS A TOKEN MFA

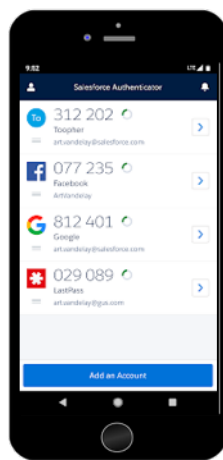
REPLACED HARDWARE TOKENS – HOW FAR DID IT GET?



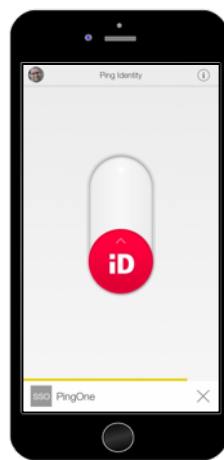
Microsoft



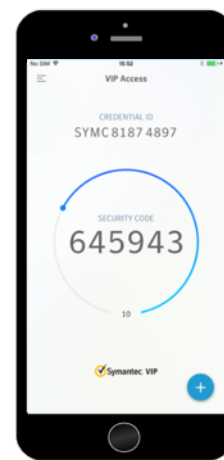
okta



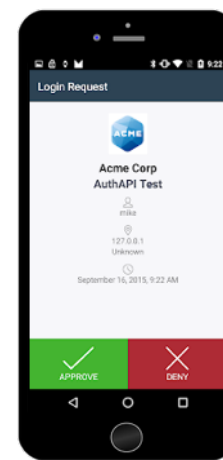
salesforce



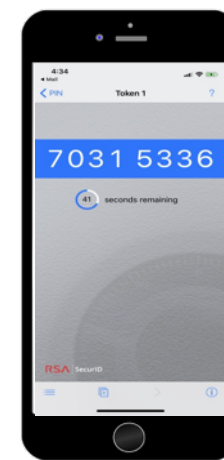
Ping ID



Symantec VIP



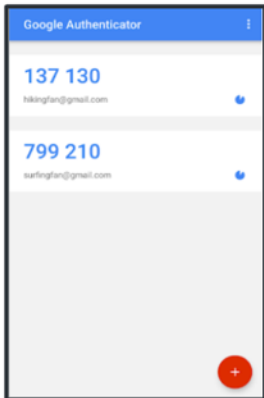
DUO



RSA

GLOBAL MFA ADOPTION HAS STALLED IN THE LOW 50% RANGE

2-Factor Authentication = Incomplete Adoption Limits Effectiveness

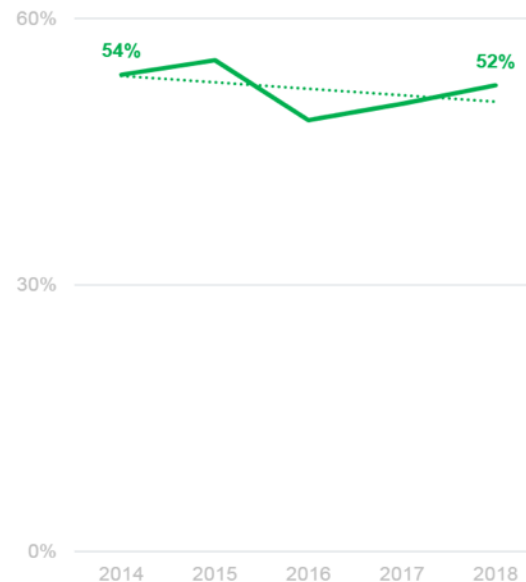


Security experts have seen a significant uptick in the number of clients securing their VPN or remote access infrastructure with multi-factor authentication.

However, there is frequently a lack of multi-factor authentication for applications being accessed from within the internal corporate network.

FireEye Threat Research, 4/19

% Sites Supporting 2-Factor Authentication, Global*



2019 INTERNET TRENDS REPORT



- Despite adoption for VPN/Remote Login **Desktop MFA is rarely used.**
- Users claim the combination of **Password + MFA is too slow.**

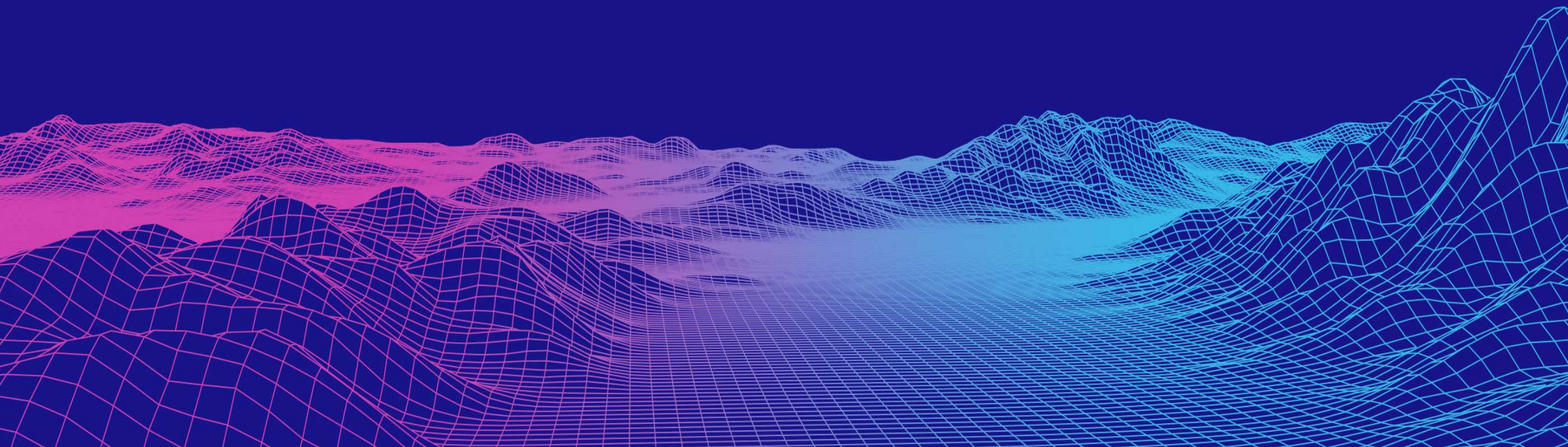
WHERE WE'RE AT TODAY

- **Customer and Desktop MFA Adoption has Stalled**
- **Everybody is Still Using Passwords**
- **A 12-Year Old can Launch Large Credential Stuffing Attacks**



WHERE

IS AUTHENTICATION GOING?

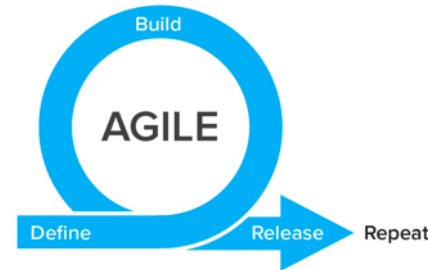


CYBER SECURITY HAS NOT YET EXPERIENCED TRANSFORMATION



MOBILE

Transformed
Consumer Experiences



AGILE

Reimagined Software
Engineering




CLOUD

Revolutionized
IT & Infrastructure

PASSWORDLESS IS THE TRANSFORMATION YOU'VE BEEN



MICROSOFT, GOOGLE, HYPR ANNOUNCE THE “TRUE PASSWORDLESS” ERA



Google Cloud


Blog Menu ▾

IDENTITY & SECURITY

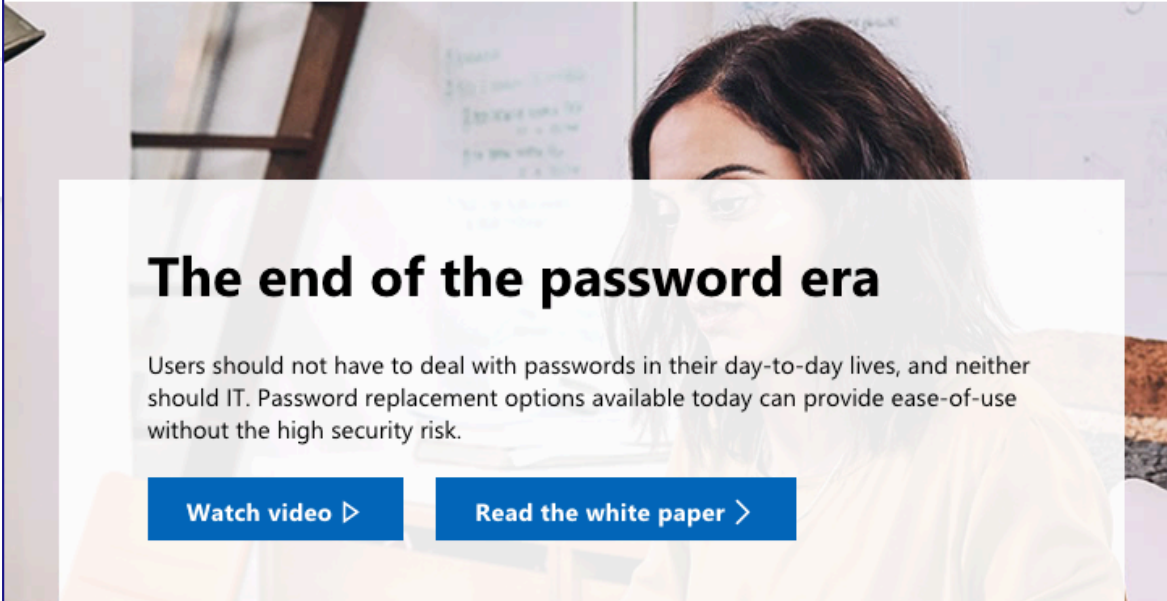
Security trends to pay attention to in 2019 and beyond

We'll see broader strides toward a true “passwordless” era, due to mainstream adoption of new standards.

We will see secure passwordless login experiences start appearing in the mainstream in 2019. This will mark the start of a broader “passwordless” era, enabled by W3C and FIDO APIs which will appear in major browsers




Microsoft | Cloud platform Products ▾ Solutions ▾ Support ▾ More ▾



The end of the password era

Users should not have to deal with passwords in their day-to-day lives, and neither should IT. Password replacement options available today can provide ease-of-use without the high security risk.

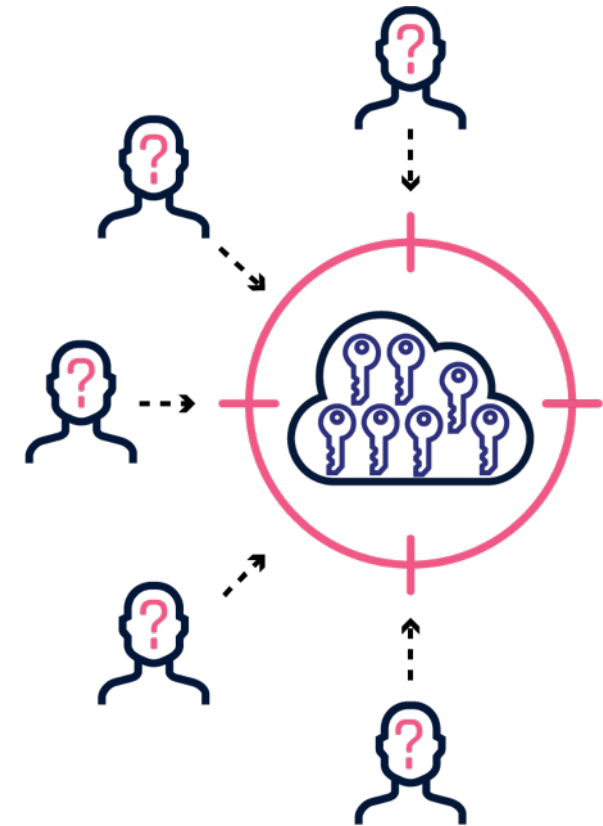
[Watch video ▸](#) [Read the white paper ▸](#)



TRUE
PASSWORDLESS SECURITY

LEGACY MFA : PASSWORDS, PINS, OTP

- Shared Secrets Stored Inside Enterprise
- Hackers' Favorite Target
- Expensive to Defend, Difficult to Use
- **Customer and Desktop MFA Gap Unsolved**



PASSWORDS & SHARED SECRETS

TRUE PASSWORDLESS MFA

- No Shared Secrets Stored in the Enterprise
- Passwords Replaced with Public-Key Encryption
- Expensive to Attack, Easy to Use
- **Addresses Customer and Desktop MFA Gap**

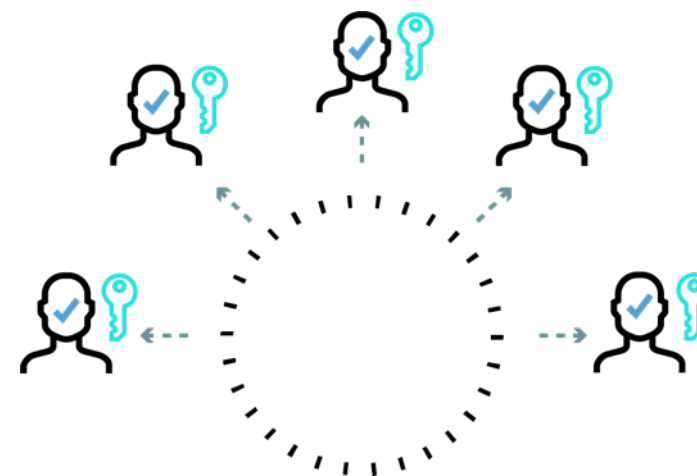


TRUE PASSWORDLESS MFA

“TRUE PASSWORDLESS” MEANS EVOLVING BEYOND SHARED SECRETS



EXPENSIVE TO DEFEND
EASY TO ATTACK



EXPENSIVE TO ATTACK
EASY TO DEFEND

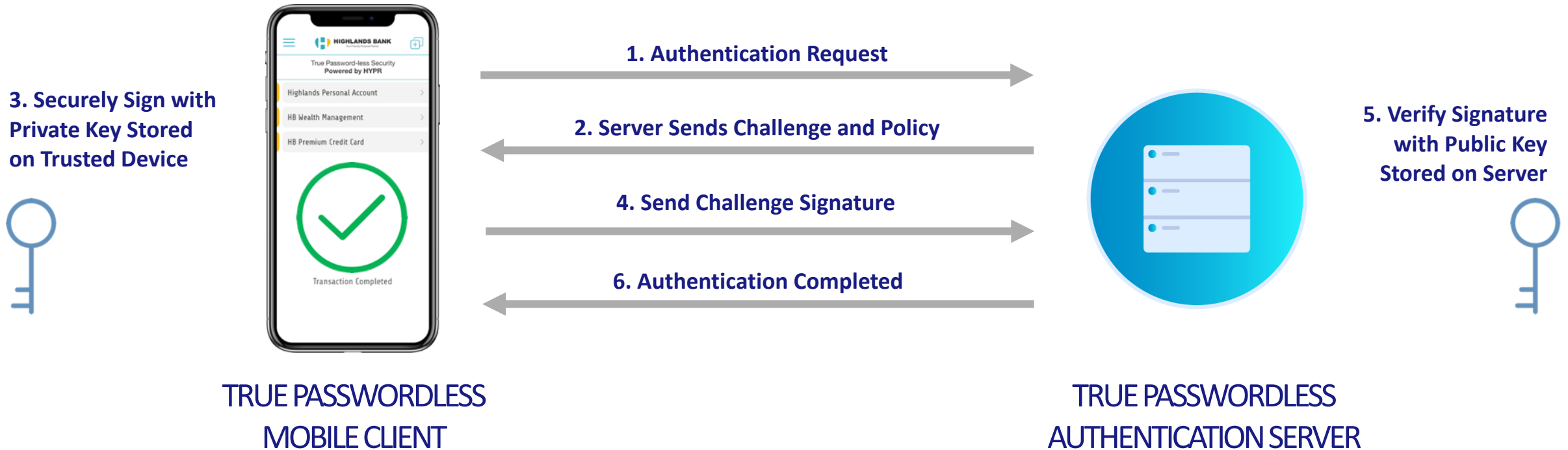
HOW DO I EXPLAIN TRUE PASSWORDLESS MFA?

IT'S LIKE A SMART CARD IN YOUR SMART PHONE



HOW DOES IT WORK?

OPEN STANDARDS + PUBLIC KEY ENCRYPTION + MOBILE AUTHENTICATION



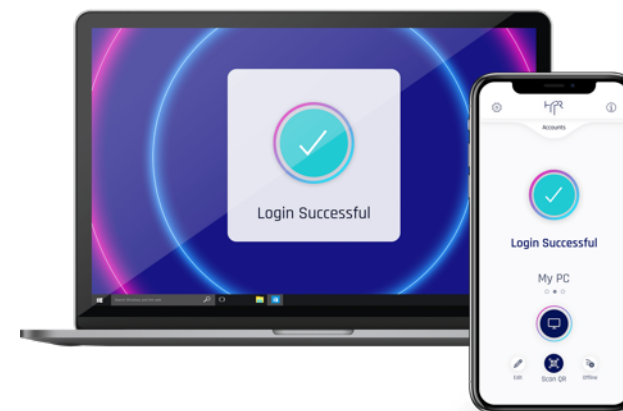
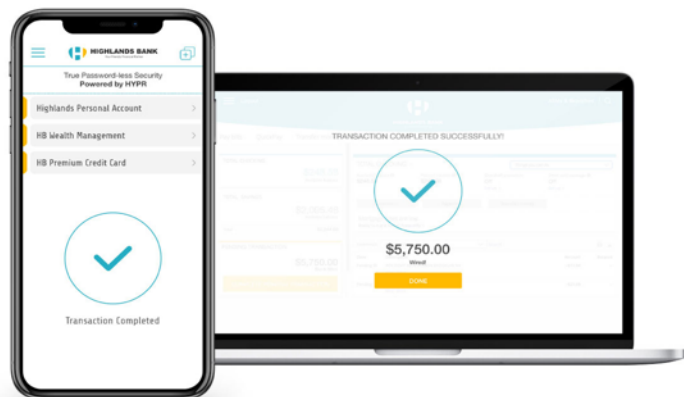
WHO IS ADOPTING TRUE PASSWORDLESS MFA?



By 2022, Gartner predicts that 60% of large and global enterprises, and 90% of midsize enterprises, will implement passwordless methods in more than 50% of use cases — up from 5% in 2018.”



PRIORITY USE CASES FOR PASSWORDLESS



PASSWORDLESS SCA
STRONG CUSTOMER
AUTHENTICATION IMPROVING
USER EXPERIENCE & SECURITY

PASSWORDLESS MFA
ENTERPRISE WORKFORCE
ADDRESSING THE
DESKTOP MFA GAP



Reduction of
Mobile
ATO Fraud



Secure & Easy
Transactions



PSD2
SCA Compliance



Passwordless
Transformation



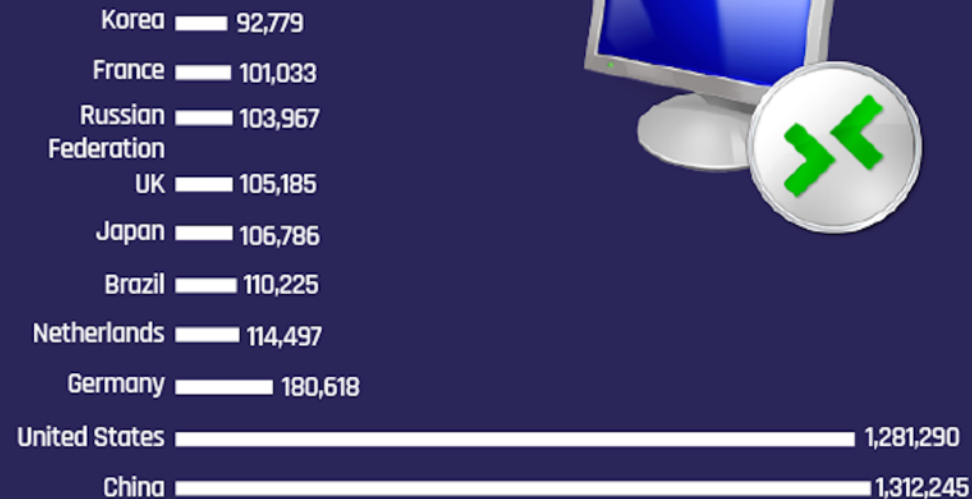
Saving \$\$\$ of
password costs



Elimination of
Phishing

HOW IS PASSWORDLESS TRANSFORMING REMOTE

RDP attacks are at an all time high with the Number of RDP Ports Exposed to the Internet skyrocketing in April 2020.



Historically speaking, the administrator user experience has not been a top priority.

Passwordless RDP Login is gaining traction among admins and remote workers, by allowing them to emulate smart cards to enhance the user experience for administrators.



HOW IS PASSWORDLESS TRANSFORMING REMOTE

WORK

VPN usage has spiked 54% IN 2020

MFA use has not.

What has skyrocketed are password resets – overwhelming IT and helpdesk teams as remote workers are asked to re-authenticate more often than ever before.



Passwordless VPN eliminates the headaches of password resets and frees up time for your IT team to attend to more critical issues.



Gartner **70%**
of organizations will implement biometric authentication for workforce access via smartphone apps by 2022.

WHY 2020 IS THE PASSWORDLESS DECADE

IT'S READY FOR ENTERPRISE SCALE



MAJOR BROWSERS SUPPORT
FIDO



OPERATING SYSTEMS INCLUDE
FIDO CLIENTS



FIDO AUTHENTICATORS ARE
BUILT INTO MOST HARDWARE

HOW CAN I GET STARTED?

EXPERIENCE TRUE PASSWORDLESS MFA NOW



HYPR.COM/FREE-TRIAL



THANK

Q&A?

YOU