2021

Cybersecurity INSIDERS

PRESENTED BY

HYPR

The State of PASSWORDLESS SECURITY

Overview

Passwords have been a weak link in the security chain for decades. Aside from their reuse, they suffer from problems ranging from poor user experience to costly overhead. Passwordless authentication aims to eliminate the use of passwords, passphrases, and other shared secrets in authentication when verifying users and authorizing payments.

In May 2020, Microsoft proclaimed that more than 150 Million people use passwordless login on Windows every month. To better understand how this trend is accelerating, Cybersecurity Insiders and HYPR compiled this report based on the feedback of security professionals across the globe. We set out to learn how businesses are adopting this technology.

Where most research has focused on passwords and their many challenges, this first-of-its-kind report addresses the rapidly growing field of passwordless security. Overall, we were surprised to find just how many people understand their password problem and are actively working to solve it – with more than half of respondents already using a passwordless technology.

Key Findings Include:

1 | Passwordless MFA Secures Users and Reduces Costs

2020 brought a sharp increase in attacks on systems using legacy and password-based multi-factor authentication (MFA). These include account takeover (ATO) fraud, Remote Desktop Protocol (RDP) attacks, push attacks, phishing, and credential stuffing attacks. Survey respondents revealed that 90% of them had experienced phishing attacks against their organizations in 2020 which also incurred significant helpdesk costs from password resets. Those that choose to go passwordless can reduce the costs and risks associated with password-based MFA. This includes savings tied to avoiding the high costs of purchasing, maintaining, and replacing hardware.

2 | User Experience and Security Are Interdependent

To maintain a strong security posture and a competitive edge, organizations must prioritize ease of use and speed as core ingredients of a superior user experience. Sixty-four percent (64%) cite user experience as a top reason for going passwordless, with 73% of respondents stating that a mobile-first passwordless MFA solution is preferred over traditional factors, such as passwords, push-based MFA, or hardware tokens. Its ease of use helps consumer-facing businesses increase revenue, while corporate workforces also benefit from increased productivity through simple and secure login across use cases, starting at the computer.

3 | Passwordless Solutions Reduce Complexity

Identity systems and infrastructure inevitably become more complex and disparate over time. A combined 95% of respondents stated the importance of passwordless MFA to be interoperable with multiple identity providers. By decoupling authentication from single-identity systems, organizations can unify their authentication mechanism with a single, consistent, and fast login experience that promotes productivity and customer engagement.

This **2021 State of Passwordless Security** report is produced by Cybersecurity Insiders, the 500,000-member community for information security professionals. We would like to thank HYPR for supporting this important research. We hope you find this report informative and helpful as you continue your efforts in protecting your IT environments against cyber threats.

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

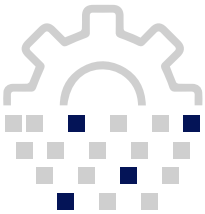
The #1 Priority for Passwordless MFA is Stopping Credential Reuse

Stopping credential-based attacks is the number one reason people say passwordless MFA is important, with 91% of respondents saying it is the primary reason. Sixty-four percent (64%) cite user experience as a top reason. It has been said that usability often takes a backseat in the security industry – and yet a majority of respondents have prioritized improved user experience as a key driver of their security initiatives.

Why is passwordless MFA important to you? Choose all that apply.

91% Stop credential theft and phishing

64%
User Experience



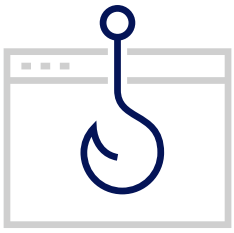
21%
Achieve digital transformation

14%
Cost savings

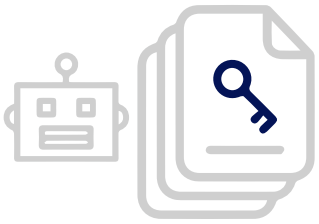
Push Attacks Are on the Rise in Remote-Work Environments

Password-related attacks continue to dominate attacks on enterprises. Respondents revealed that 90% of them experienced phishing attacks against their organization, and 29% saw credential stuffing in 2020. Other attacks respondents noted include RDP attacks (14%) and push/push fatigue attacks (9%). Once praised as the method that took MFA mainstream, push notifications are being increasingly weaponized by malicious actors.

What kinds of cyber attacks has your organization seen this year since remote work has become more common? Choose all that apply.



90% Phishing



29%

Credential stuffing and brute force

14%

Remote Desktop Protocol (RDP) attack

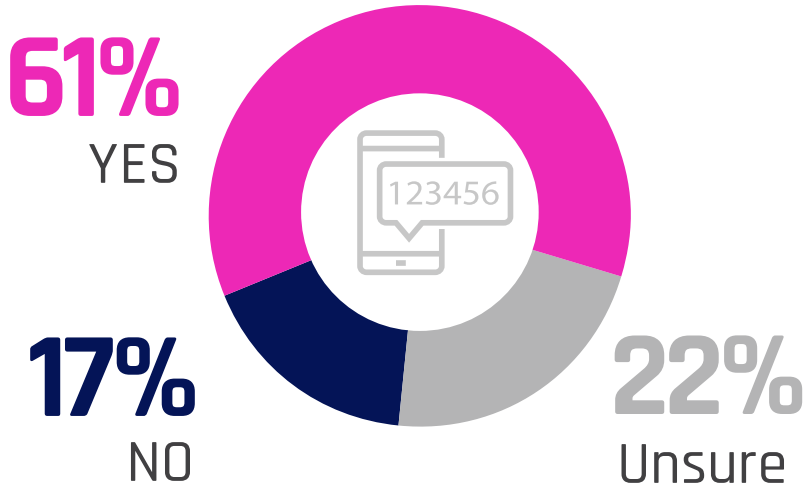
9%

Push or push fatigue attack

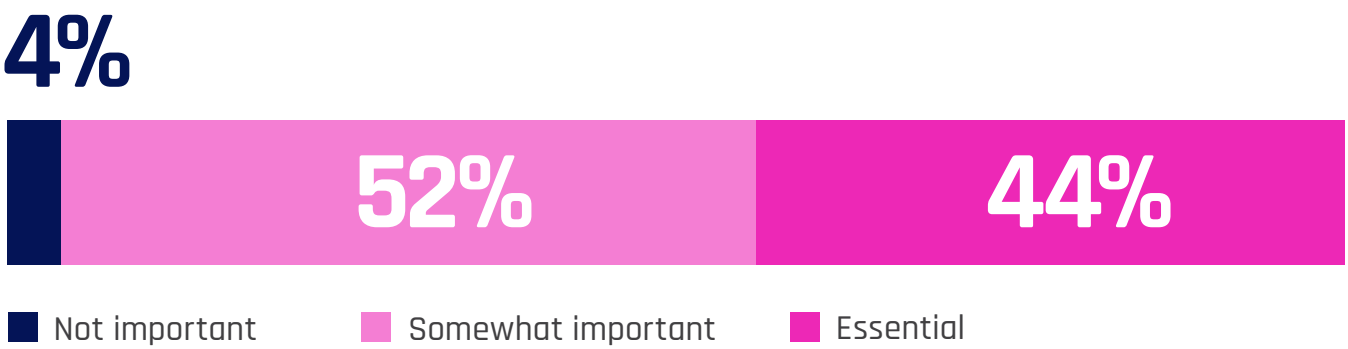
Most 'Passwordless' Solutions Still Rely on Passwords

Sixty-one percent (61%) reveal that their organization's "passwordless" MFA solution requires a shared secret, such as an underlying password, one-time password (OTP), or SMS code. This is despite 44% considering it "essential", and 52% considering it "somewhat important" to eliminate shared secrets for authentication. In addition, 22% are unsure, suggesting there is more education to be done on the definition and benefits of passwordless MFA, including offline and account recovery use cases.

- **Some MFA solutions provide a passwordless experience. Does your "passwordless" MFA solution require a password or other shared secret (e.g., OTP, SMS code)?**



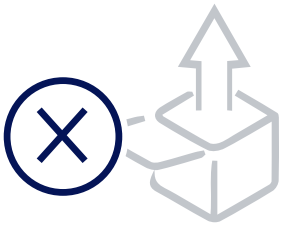
- **How important is it for your passwordless solution to not use any kind of shared secret, specifically during account recovery and when offline?**



Smartphones Lead the Way for Passwordless Adoption

Forty-eight percent (48%) of respondents say their organization lacks a passwordless solution (here, loosely defined as authentication in which the user is required to provide a username but not a password to gain access). Thirty-six percent (36%), however, are passwordless, using smartphones as FIDO tokens. This supports the trend in mobile-first solutions among passwordless technologies.

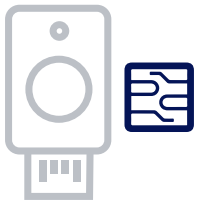
What passwordless technologies does your organization provide today? This is defined as authentication in which the user is required to provide a username but not a password to gain access. Choose all that apply.



48% None – we don't have any passwordless technology deployed

36%

Smartphone as a FIDO token



17%

Hardware security key where no password is required

(e.g., Yubico Yubikey, Google Titan, or smartcard)

17%

Built-in authenticators

(e.g., Windows Hello)

User Experience - High Priority, Low Expertise

Enhanced user experience (UX) is a key benefit of passwordless technology. Sixty-seven percent (67%) of enterprise respondents say their security organization lacks UX expertise. Although proficiency in this department plays a more significant role in B2C use cases, we are seeing a convergence of UX requirements for both workforce and consumer users. Seventy-three percent (73%) say that, from a UX perspective, smartphones are the most convenient MFA method whether they are accessing resources at work or remotely.

Does your security organization have a UX team?

From a UX perspective, whether remote or in-office, which MFA method is more convenient?

73%
A smartphone

17%
Built-in authenticator
(e.g., TouchID, Windows Hello)

5%
A smart card

5%
A U2F security key
(e.g., YubiKey)

Remote Work is the #1 Use Case for Passwordless Adoption

For organizations with a passwordless solution in place, internal users are the dominant user population, with remote employees (86%) and onsite employees (73%) leading, followed by external contractors and partners (43%). It's both exciting and unsurprising to see that organizations have made remote login the clear winning use case for passwordless security.

Who is the primary user base for passwordless authentication in your organization? Choose all that apply.

86% Remote employees

73%

Onsite employees

43%

Contractors/ partners

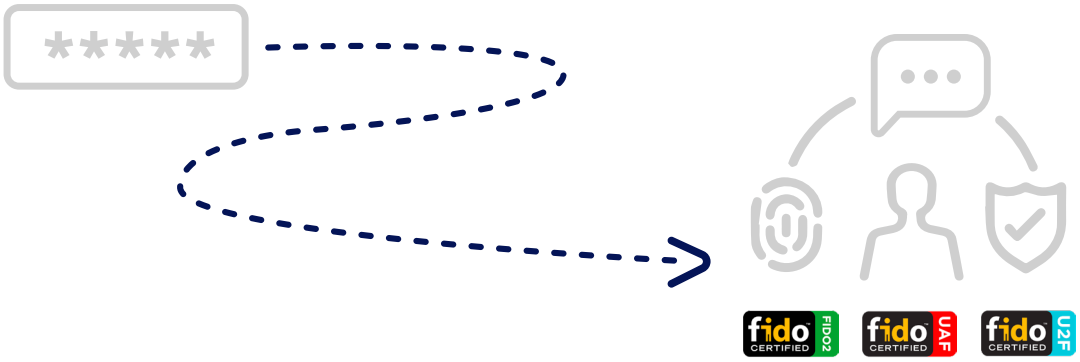
24%

Customers/ consumers

The Standards-based Approach Remains Top of Mind for Security Professionals

Of those who are planning their journey to passwordless authentication, a combined 94% said it is "essential" (58%) or "somewhat important" (36%) to leverage a standards-based approach such as Fast Identity Online (FIDO) standards. Standards ensure a solution is enterprise-ready, future-proof, and integrates seamlessly into existing IT environments.

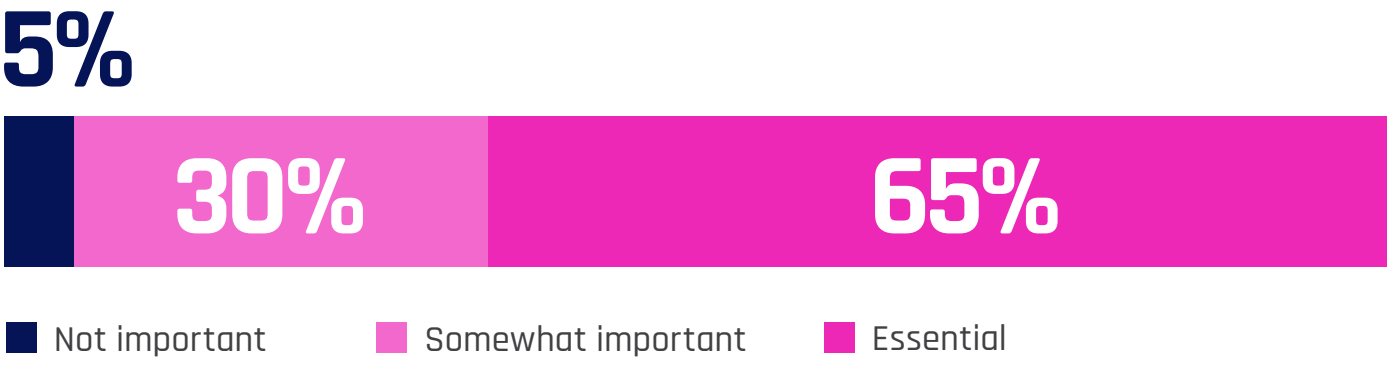
When planning your journey to passwordless authentication, how important is it to leverage a standards-based approach such as FIDO?



Interoperability with Multiple Identity Providers is Key

Identity and Access Management (IAM) is a component that must work well with an organization's existing infrastructure and systems. Identity platforms are a key consideration when choosing an authentication solution as nearly two-thirds (65%) of respondents said it is important for a solution to be "seamlessly interoperable" with multiple identity providers. It is interesting to see that most respondents already use or expect to have multiple sources of verification for user identity, rather than the traditional approach of using one siloed MFA product per identity system.

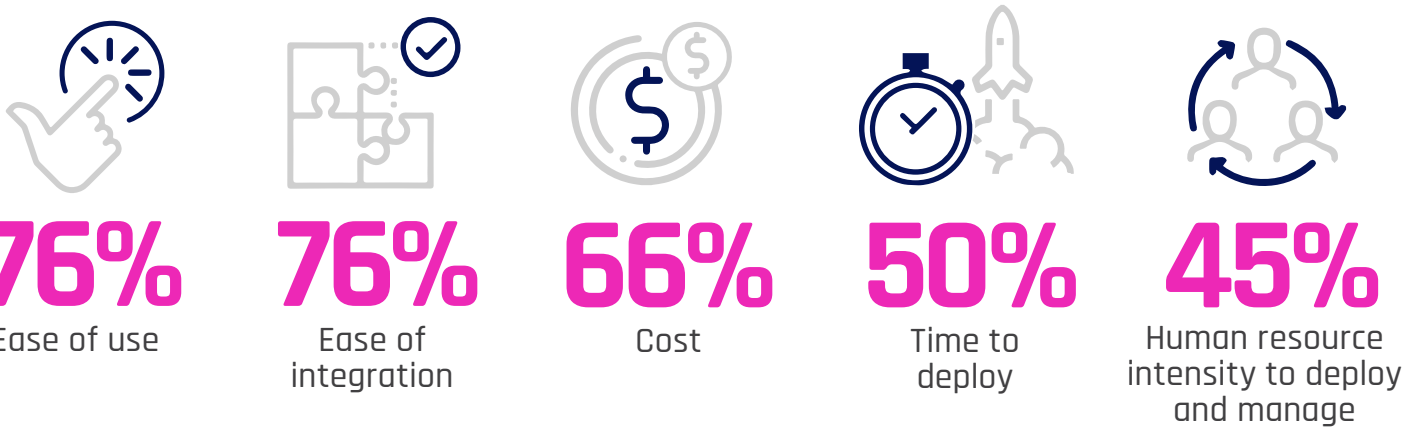
How important is it for your passwordless MFA solution to be seamlessly interoperable with multiple identity providers?



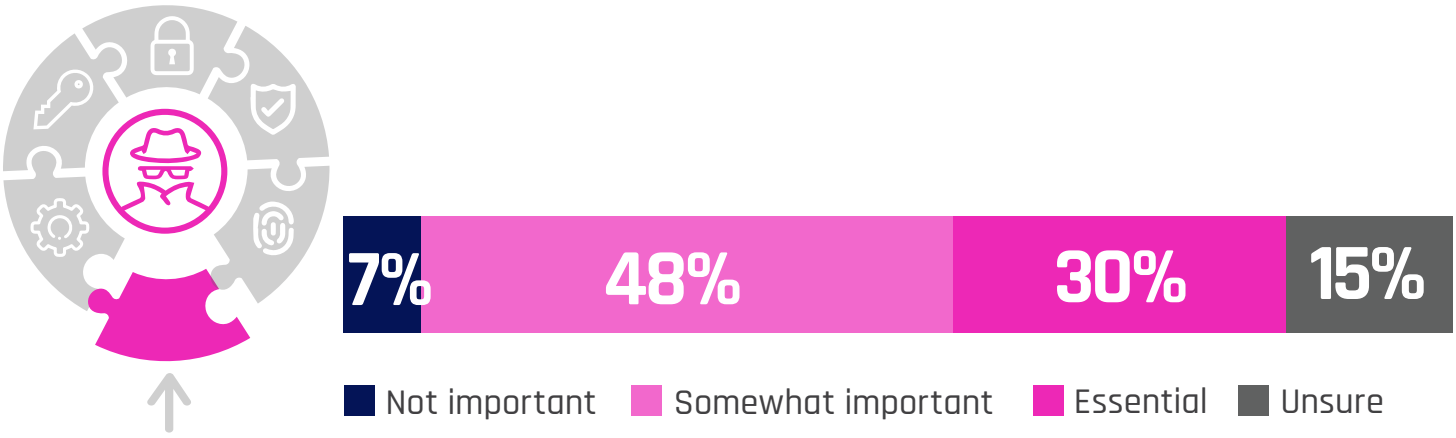
Ease of Use and Integration are Top Deciding Factors

We asked what factors organizations prioritize when choosing a passwordless solution. Seventy-six percent (76%) of respondents cited "ease of integration" as an important factor. Almost a third of organizations (30%) confirmed that a passwordless MFA solution should have the ability to integrate with fraud and risk engines, while 48% said it was "somewhat important".

When choosing a passwordless solution, what factors are most important? Choose all that apply.



How important is it for your organization to have the ability to integrate fraud and risk engines alongside your passwordless MFA solution?



Hardware Keys Carry High Costs and Helpdesk Hurdles

Enterprise respondents consider hardware security keys to be costly – and they see costs at all stages of security token deployments. As the biggest drivers of these costs, respondents cite the initial costs of hardware (66%), helpdesk-related costs (60%), maintenance and service (55%), and hardware token replacement costs (52%).

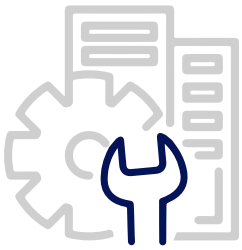
What are the biggest drivers of the high costs associated with hardware security keys? Choose all that apply.

66%

Initial costs of the hardware

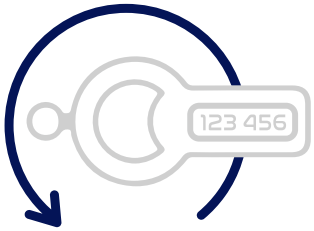
60%

Helpdesk costs (onboarding, training, and deployment)



66%

Maintenance and service agreement costs



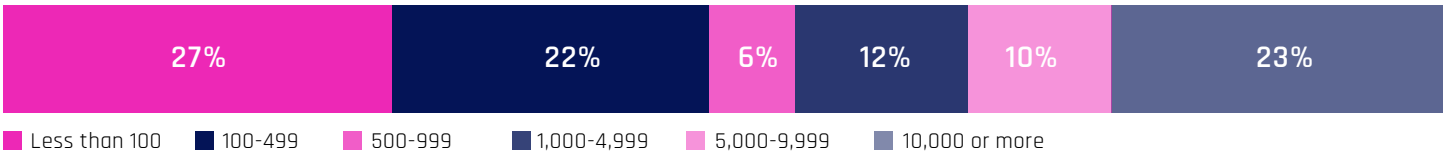
52%

Hardware replacement costs

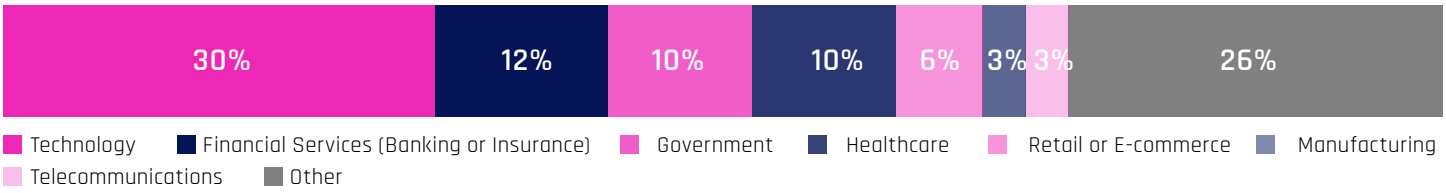
Methodology & Demographics

The 2021 State of Passwordless Security report is based on a survey of 427 information technology professionals that explored the state of passwordless authentication, the key drivers and barriers to adoption, and organizations' technology preferences. The respondents range from technical executives to IT security practitioners, representing a cross-section of organizations of varying sizes across multiple industry verticals.

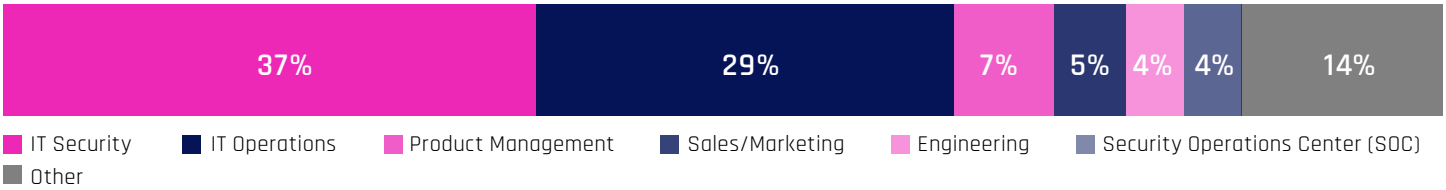
Company Size



Industry



Department



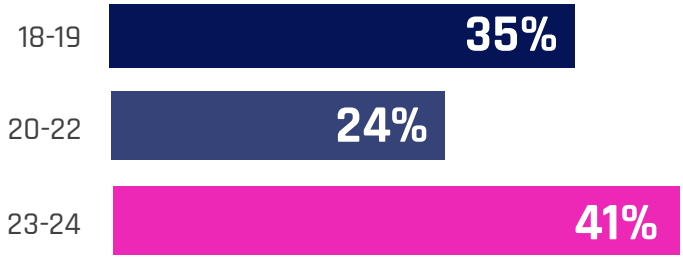
Computer OS

Type of Smartphone OS Used

Addendum: Password Manager Usage is Declining Among Gen Z

While Generation Z has a reputation for being quick adopters of new technology, password management apps are surprisingly less popular with this age group when compared to other age groups. Only about a quarter (24%) of Gen Z respondents say they are using a password management app. The most popular password management apps for this group include Google Chrome (27%), utilizing Chrome's password feature, Apple Keychain (13%), and LastPass (8%).

GEN-Z
Age group



Password management app usage

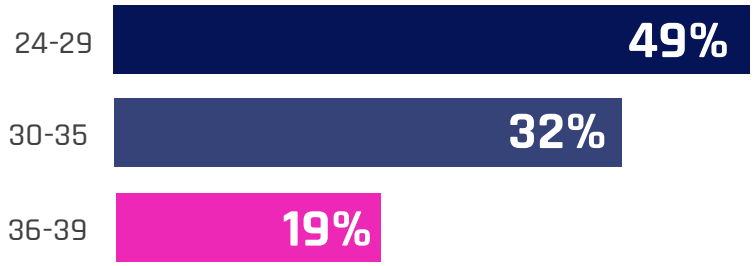
App popularity

Keeper 1% | RememBear 1% | NordPass 1% | Other 44%

Addendum: Password Manager Usage Among Millennials

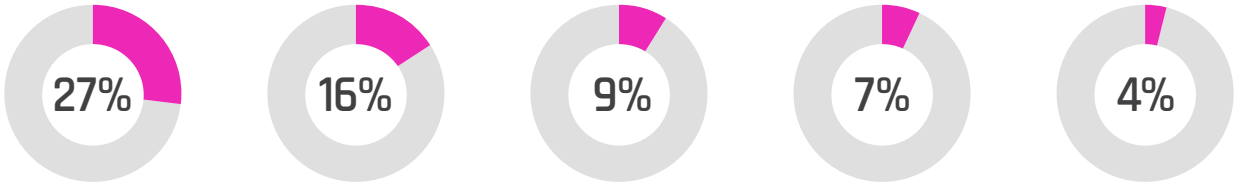
Millennials are more likely to use a password management app (39%), when compared to Gen Z. The most popular password management apps for this group include Google Chrome (27%), LastPass (16%), and 1Password (9%).

Millennials
Age group



Password management app usage

App popularity

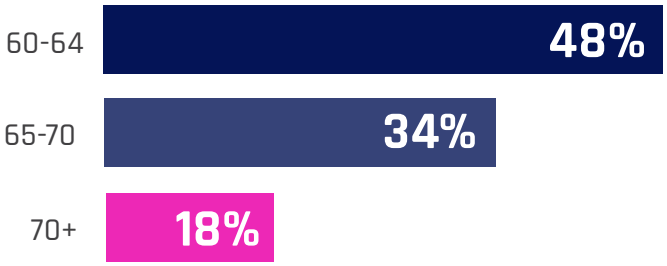


Keeper 1% | NordPass 1% | Other 34%

Addendum: Older Adults Prefer Passwordless Authentication

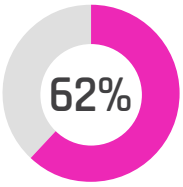
Among older adults (60 and up), a majority (54%) prefer passwordless authentication technologies; 62% of people in this age group say they already access banking and healthcare via mobile and web apps.

Older adults
Age group

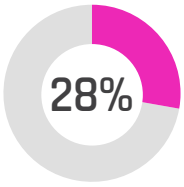


Preference for passwordless authentication

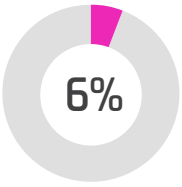
How they access healthcare and banking apps



Mobile and website



Website only



Mobile only

Other 4%

Summary

There is a common notion among technologists, analysts, regulators, and the media that passwords aren't going anywhere. This report tells a very different story from the practitioners' point of view. Not only have a meaningful number of organizations already deployed passwordless technology, but they also demonstrate a clear understanding of its impact and use cases.

The State of Passwordless Security report tells a story that mainstream adoption is upon us. The proliferation of passwordless technology is further along than we think and may be happening faster than once predicted.

Key Takeaways:

- **Credential reuse attacks remain the leading driver for the elimination of passwords.**
- **The shift to remote work has accelerated urgency for passwordless authentication.**
- **Ease of use and integration are the deciding factors for choosing a product.**
- **96% of respondents want to stop using shared secrets for authentication.**
- **Smartphones are leading the way in driving adoption of passwordless MFA.**

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

Passwords and shared secrets remain the leading cause of breaches despite billions of dollars invested in cybersecurity. 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 that their users love.

Cybersecurity
INSIDERS

PRESENTED BY