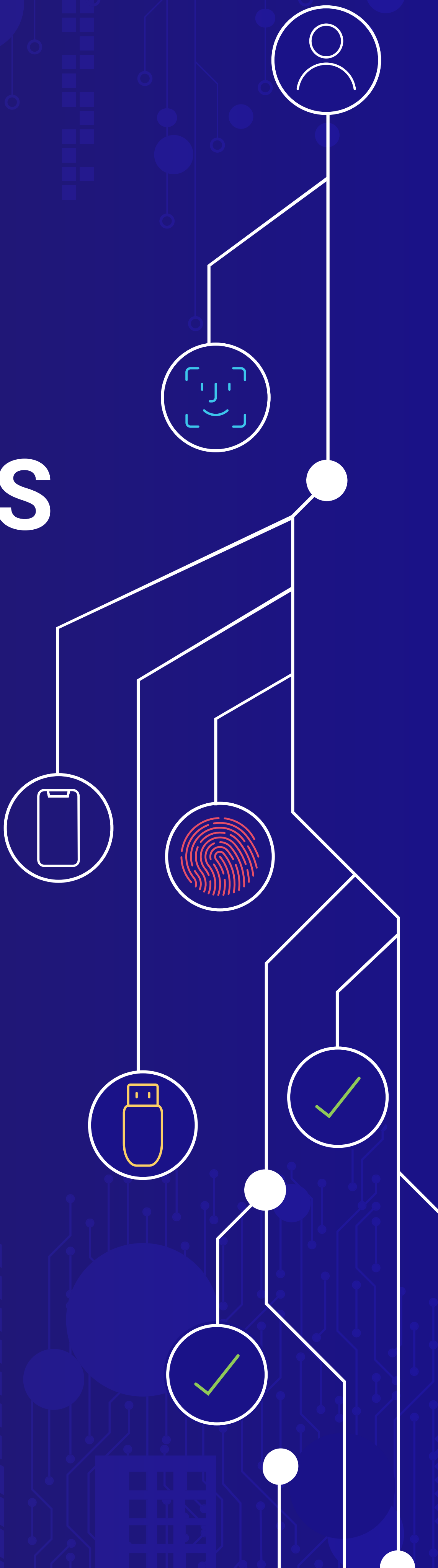
THE STATE OF

PASSWORDLESS SECURITY 2022



Cybersecurity INSIDERS | HYPR

_EXECUTIVE SUMMARY

The long-standing, oft-deferred security threat posed by password-based authentication is now front and center. Some of the most damaging cyberattacks in the past year were caused or enabled by weak password protection. For example, the Colonial Pipeline breach that shut down fuel supply operations to the eastern United States was traced to a single compromised password.

This untenable risk, along with growing regulatory pressures such as the the 2021 Executive Order on Cybersecurity's Zero Trust mandate, are prompting more organizations to turn to passwordless options. There's growing recognition that passwordless security approaches can provide significantly better protection and user experience as well as cost savings.

To further clarify the state and direction of passwordless authentication, we conducted our second annual survey among IT and security professionals across the globe.

The data we collected reveals several significant trends:

- Traditional multi-factor authentication (MFA) methods are increasingly under attack. These include Remote Desktop Protocol (RDP) attacks, account takeover (ATO) fraud, phishing, man-in-the-middle (MitM) attacks, credential stuffing and push attacks.
- Remote work continues to be the main driver for passwordless authentication, especially against the backdrop of the significant increase in phishing attacks in recent years.
- Organizations face serious security gaps due to insecure authentication methods based on secret-sharing.
- A decoupled, standards-based approach that provides interoperability helps organizations reduce complexity and is key to future passwordless adoption at scale.

We hope you find this report informative and helpful as you continue your efforts in protecting your IT environments against cyberthreats.

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity INSIDERS

This 2022 State of Passwordless Security Report has been produced by Cybersecurity Insiders, in conjunction with HYPR, to explore the latest authentication security trends, challenges, gaps and priorities.

_ KEY FINDINGS

Our findings underscore that IT and security professionals face escalating authentication security challenges as attacks rise and traditional MFA proves problematic. Passwordless solutions let organizations reduce these risks as well as the high costs associated with password-based MFA.

Traditional MFA methods are increasingly under attack.

33%

Rise in push attacks, with 12% of organizations reporting attacks using weaponized push notifications.

34%

of organizations reported credential stuffing attacks, up 17% from the previous year.

89%

of organizations experienced a phishing attack in the past year — indicating phishing is still at an all time high.

There are major gaps in authentication security.

65%

of respondents believe their company's authentication is not secure.

16%

of organizations with passwordless technology use phishing-resistant methods; the remaining still have shared secrets or are uncertain.

Remote work remains the top driver in the move to passwordless.

86%

of organizations reported remote work as their number one passwordless use case, unchanged from last year.

_ CREDENTIAL ATTACKS ARE ON THE RISE

Given the vast troves of stolen passwords on the dark web, easily available automated attack tools, and people's penchant for password reuse, it's unsurprising that credential stuffing attacks continue to grow — 34% of respondents reported credential stuffing attacks, a 17% increase over last year. On top of that, phishing remains at an all time high with 89% of respondents revealing that their organizations experienced at least one phishing attack.

Remote Desk Protocol (RDP) attacks (14%) also continue to afflict enterprises. Moreover, push notifications are being increasingly weaponized with a 33% spike in push attacks since last year.

NOTEWORTHY

Attackers continue to target remote workers as evidenced by the sharp increase in push attacks and ongoing pressure from RDP and MitM attacks.

What kinds of cyberattacks has your organization seen this year? Select all that apply.

89%
Phishing

34%
Credential stuffing and brute force

14%
Remote Desktop Protocol (RDP) attack

12%
Push or push fatigue attack

9%
Man-in-the-middle (MitM) attack

_ AND MOST ORGANIZATIONS AREN'T EQUIPPED TO HANDLE THEM

Despite the high rates of phishing and other authentication attacks, the majority of organizations still lack sufficient authentication security controls.

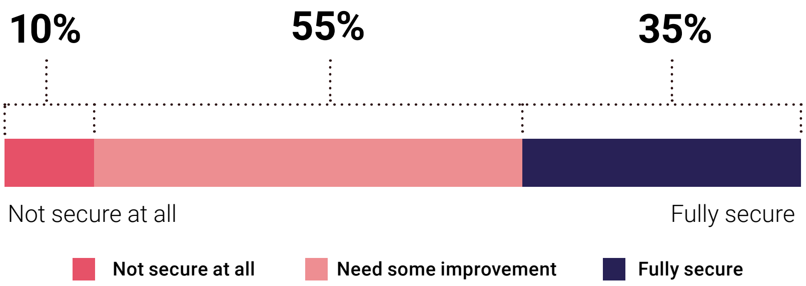
NOTEWORTHY

Multi-factor authentication at the desktop remains a serious security gap. Analyst firm Forrester estimates that more than 55% of organizations today rely on passwords as the primary authentication method.[1]

Authentication Improvements Needed

Only 35% of IT and security professionals believe their current authentication solution is fully secure.

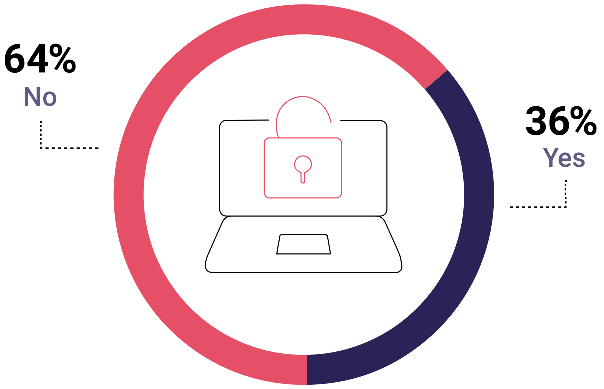
How secure do you believe your current authentication solution to be?



The Status Quo Reigns

Even after an attack, most organizations retain the same password-based approach.

If your organization experienced any of these attacks, did it change how it manages passwords or protects corporate resources?



[1] Using Zero Trust To Kill The Employee Password, Forrester Research, Inc., August, 2021

_ TRADITIONAL MFA IS FAILING

Why is there apparent widespread unpreparedness when it comes to passwords and security? Challenges to deployment and adoption of traditional MFA, from both a user and systems point of view, may hold the answer.

NOTEWORTHY

The Open Web Application Security Project (OWASP) includes "Identification and Authentication Failures" in its OWASP Top 10 as one of the biggest application security risks.

Obstacles to Traditional MFA Adoption

When asked about challenges in deploying conventional multi-factor authentication solutions, nearly half (49%) named poor user experience. This was closely followed by difficulty to integrate with current systems (48%).

What do you see as the primary obstacles to deploying a traditional MFA solution? Select all that apply.

49%
Poor user experience

48%
Difficult to integrate with current systems

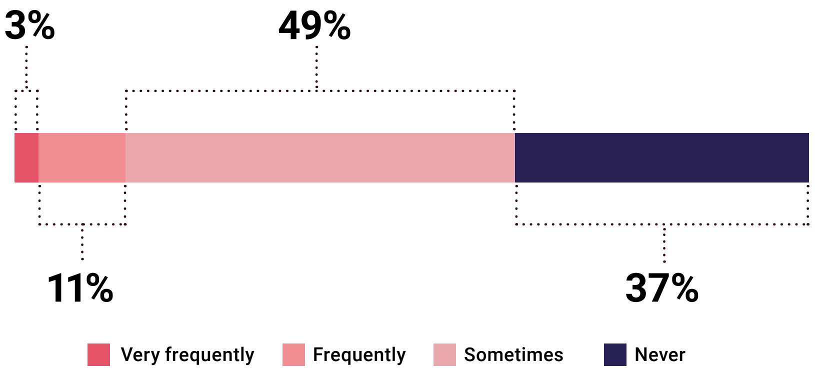
42%
Cost

26%
Requires too many resources to deploy and manage

Password-Based MFA Harms Productivity

63% of those surveyed could not access work-critical information because they forgot a password.

Have you ever needed access to critical information for your work but were unable to because you forgot the password?



_ WHY PASSWORDLESS MFA IS IMPORTANT

With this chaotic landscape, it’s unsurprising that passwordless authentication is gaining traction. The overwhelming majority of those surveyed (82%) say stronger security is the number one reason passwordless MFA is important. Improved user experience comes in at a strong second, at 67%. This is up 5% from last year, indicating a mounting awareness of usability’s importance to the success of security initiatives.

Regulatory factors are also a strong driver of passwordless adoption, with nearly 40% citing compliance as a priority.

NOTEWORTHY

People are starting to get the message that passwordless can also bring cost savings. While it still comes in last place at 21%, this represents a 50% increase over last year.

What do you believe are the key benefits of passwordless Multi-factor Authentication (MFA)? Select all that apply.

82% Increase Security

67% Improve User Experience

39% Comply with regulations

29% Achieve digital transformation

21% Cost savings

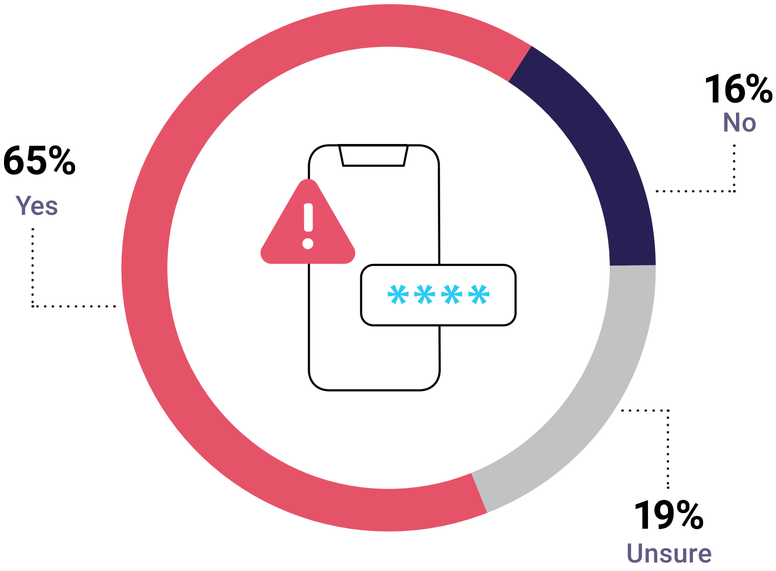
_ CONFUSION BETWEEN PASSWORDLESS EXPERIENCES AND PASSWORDLESS MFA

Although stronger security was named as the top priority for passwordless adoption, the majority of organizations that employ passwordless login use insecure methods. At least 65% are using “passwordless” solutions that just mask the password — such as biometrics that unlock an underlying password, an OTP or SMS code — leaving them vulnerable to credential-based attacks. And the number is potentially much higher as 19% did not know if their solution was vulnerable. This also suggests that more education is needed on the definition and benefits of passwordless MFA.

NOTEWORTHY

Many regulations, including the 2021 Executive Order on Cybersecurity, specifically require phishing-resistant MFA, which means SMS and OTPs must go.

Some solutions provide a passwordless experience but are not fully passwordless. Does your “passwordless” MFA require a password or other shared secret (e.g. One-time password (OTP), SMS code)?



_ FINANCE SECTOR LEADS IN PASSWORDLESS ADOPTION

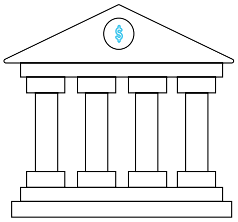
Unsurprisingly, the industries that are the most regulated and the most under attack are the ones the quickest to turn to strong passwordless security. Of small-to-medium businesses (defined as 500 or fewer employees) that started passwordless projects in 2021, 25% were in the finance and insurance sector. For larger enterprises, this figure was even higher at 34%. The next strongest showing on the enterprise side was the manufacturing sector at 13%.*

This closely mirrors recent cyberthreat trends. According to the IBM Security X-force Intelligence Index 2021, the finance and insurance industry was the most-attacked industry for the fifth straight year. The big shift was manufacturing, which moved from eighth place in 2020 to the second most targeted industry last year.

NOTEWORTHY

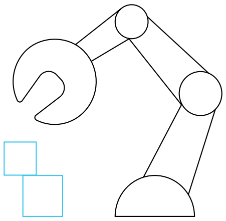
Many of the top financial institutions are not just adopting passwordless, they are leading the charge. Mastercard, Bank of America, American Express, Visa, USAA, PayPal and Wells Fargo are all board members of the FIDO (Fast IDentity Online) Alliance, which works to define passwordless security standards.

Breakdown by industry of enterprises (>500 employees) that started passwordless projects in 2021.



34%

in finance and insurance sector



13%

in manufacturing sector

* This research was conducted separately by HYPR using a different set of data.

_ REMOTE AND HYBRID WORK CONTINUES TO DRIVE PASSWORDLESS ADOPTION

For organizations with a passwordless solution in place, remote employees (86%) are the predominant user population, followed by onsite employees (73%), suggesting that most organizations employ a significant hybrid workforce. Adoption of passwordless technology for customers (23%) continues to lag behind the workforce.

NOTEWORTHY

As discussed earlier, attackers capitalize on security gaps in remote and hybrid workforces. Organizations quick to evolve their authentication strategy are able to eliminate this risk.

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

86%
Remote employees

74%
Onsite employees

23%
Contractors/ partners

21%
Customers/ consumers

_ HARDWARE KEY-BASED PASSWORDLESS CARRIES A HIGH PRICE TAG

Security and IT professionals consider hardware security keys to be costly — both at deployment and as an ongoing expense. As the biggest drivers of these costs, they cite initial costs of hardware (66%), help desk related costs (59%), maintenance and service (56%), and hardware token replacement costs (51%).

NOTEWORTHY

Secure distribution of hardware keys poses a particular challenge in the case of a remote workforce.

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

66%
Initial costs of the hardware

59%
Help desk costs (e.g. resources dedicated to onboarding, training, and deployment)

56%
Maintenance and service agreement costs

51%
Replacement costs of the hardware

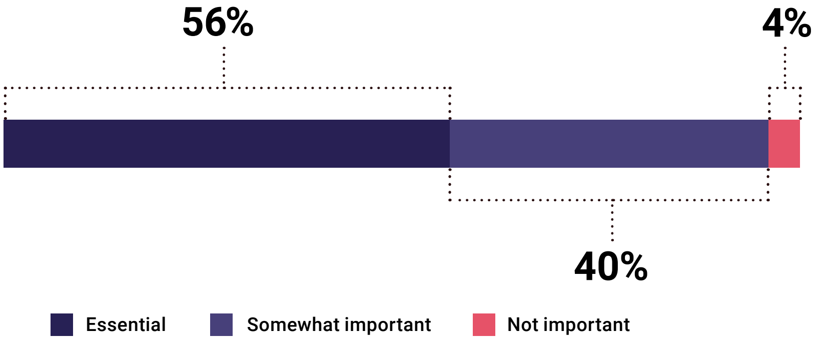
_ A DECOUPLED, STANDARDS-BASED APPROACH IS KEY TO REDUCE COMPLEXITY

Of those who are planning their journey to passwordless authentication, a combined 96% say it's important to leverage a standards-based approach such as Fast Identity Online (FIDO), with 56% stating it's essential and 40% that it's somewhat important. Only 4% believe a standards-based approach is unimportant — down by 33% from last year.

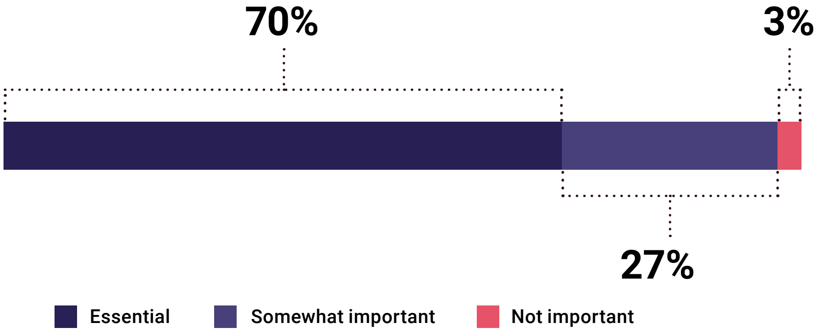
This goes hand-in-hand with the nearly unanimous support for passwordless technology that is independent from identity and access management (IAM). A full 70% of respondents (up from 65% last year) say it's essential for a solution to be seamlessly interoperable with multiple identity providers and an additional 27% say it's somewhat important. It is interesting to note the strong trend toward decoupling authentication, rather than locking into a single vendor.

NOTEWORTHY

FIDO standards have emerged as the most widely adopted standards in the passwordless industry, supported by Mastercard, Apple, Microsoft, Samsung and many others.



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



How important is it for your passwordless Multi-factor Authentication (MFA) provider to be seamlessly interoperable with multiple identity providers?

_ SUMMARY

As these findings corroborate, the need for strong authentication has reached the point of urgency at the same time that traditional MFA has hit a wall.

Strong password policies are difficult to enforce. Passwords are hard to remember and cumbersome to type. Hidden costs from resets, lost productivity and other problems of conventional MFA add up to a very tangible price. Most importantly, centralized credential stores will always be an attacker's favorite target.

The risks affect organizations of all sizes. Historically, small organizations experienced fewer than half the number of data breaches of large enterprises. The 2021 Verizon Data Breach Investigations Report found that it's now above 85%.[1]

With the ubiquity of automated hacking tools and massive password leaks, attacks will continue to rise unless organizations evolve their strategies. Legacy MFA – and any authentication that relies on shared secrets – is vulnerable. Fortunately, this report shows a growing consensus among IT and security practitioners that passwordless multi-factor authentication technologies hold the answer.

TAKEAWAYS

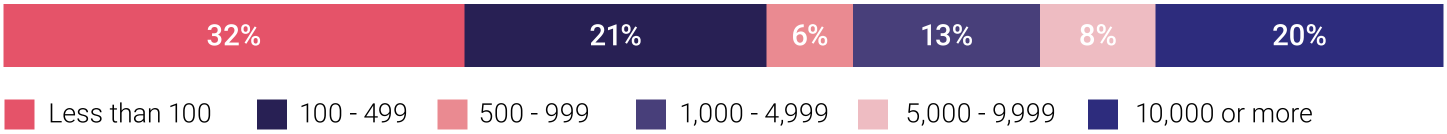
- Traditional MFA methods are increasingly under attack
- Remote and hybrid work continues to be a driving force in passwordless adoption
- The majority of solutions deployed to date provide a passwordless experience, not passwordless MFA
- There's a clear need for strong passwordless authentication that does not require dedicated experts and extensive resources to deploy and manage
- Organizations are looking to passwordless security to bridge a disparate identity ecosystem and unify their authentication mechanism
- The financial services industry is taking the lead in the move to a passwordless world

[1] https://www.verizon.com/business/resources/reports/dbir/2021/smb-data-breaches-deep-dive/

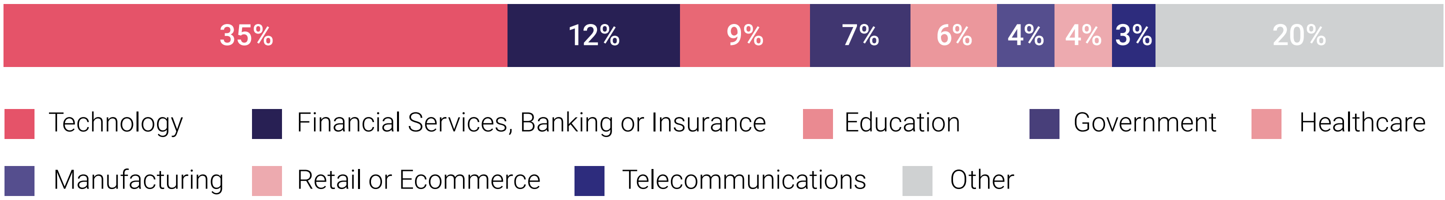
_ METHODOLOGY AND DEMOGRAPHICS

The 2022 State of Passwordless Security Report is based on a comprehensive survey of 411 technology professionals to explore the state of conventional and passwordless authentication, key drivers and barriers to adoption, and organizations' technology preferences. Respondents range from technical executives to IT security practitioners, representing a cross-section of organizations of varying sizes across multiple industries.

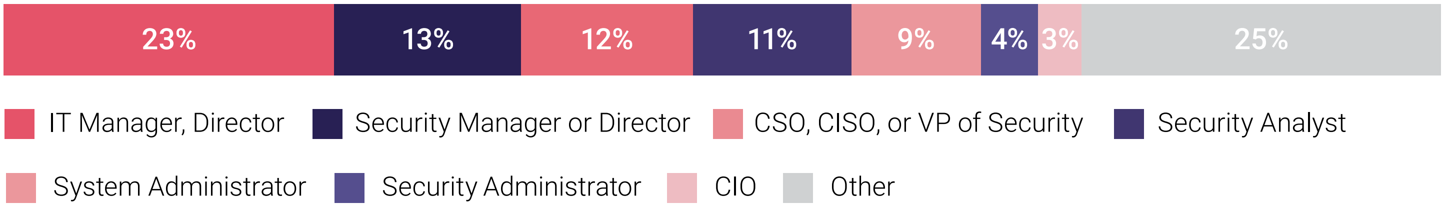
Company Size



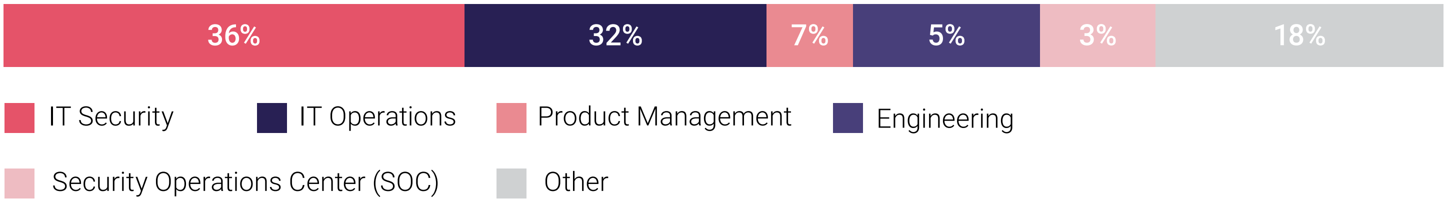
Industry



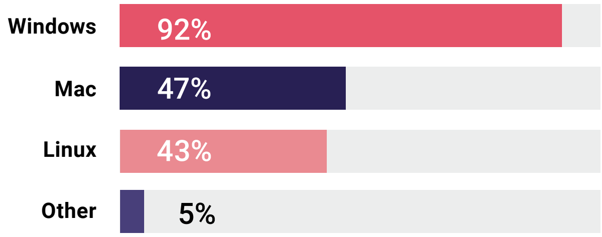
Primary Role



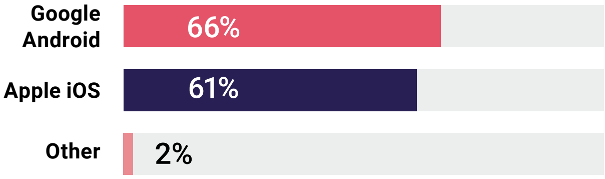
Department



Type of computer OS for work (all that apply)



Type of smartphone OS (all that apply)



_ ABOUT HYPR

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.

See how passwordless MFA can secure your workforce and customers
Visit: hypr.com/demo

Cybersecurity INSIDERS