
VansonBourne
HYPR
THE STATE OF
PASSWORDLESS
SECURITY
2023
VOLUME 3

Contents

Foreword

It's no secret that passwords and other weak authentication methods remain a primary cause of data breaches. Simple, secure authentication continues to be a challenge for many organizations; a constant tug of war between security and the need for users to easily access digital resources. But it doesn't have to be.

This was the impetus behind the founding of the FIDO Alliance 10 years ago – to develop standards for simpler, stronger user authentication. From the beginning, we recognized that user experience and security are interdependent. That is why the authentication protocols that became known as the FIDO standards were developed with equal focus on phishing-resistance, user acceptance and scalability.

HYPR's 2023 State of Passwordless Security report captures an interesting juncture, where we see that organizations are eager for change yet still reticent in action. However, as the study findings show, the consequences of that inaction are becoming impossible to ignore, both in terms of security risks and business impacts. Into this milieu has entered passkeys. With the industry at an inflection point, passkeys promise to be the vehicle to tip us over by finally presenting the world with a phishing-resistant, user friendly and scalable alternative to passwords as a primary authentication factor. It also marks a time where service providers have options for all use cases – for example, while the syncable nature of passkeys is a win-win for consumer services, enterprise security teams can opt for device-bound passkeys on a security key or dedicated mobile app for employee authentication.

It won't be your security teams driving the change, it will be your employees and customers expecting the same simple login they experience in their daily lives. Change won't happen overnight but I believe when we look back at this period, we will mark it as the beginning. Like any new technology, passkeys will benefit from market response – which will lead to beneficial iterations and the development of implementation best practices. Organizations that understand this, and begin the transition to these phishing-resistant systems now will be the ones in the strongest position in the coming years. Not just from a security standpoint, but from the efficiency gains brought by a simplified UX.

— Andrew Shikiar

Executive Director & CMO, FIDO Alliance

Andrew Shikiar is the Executive Director and Chief Marketing Officer at FIDO Alliance, a global consortium working to create and drive adoption of open standards for simpler, stronger user authentication. Shikiar has been involved in the identity industry for 20+ years.

Introduction

The annual State of Passwordless Security Report offers organizational leaders as well as those in the trenches a way to stay informed on one of the most rapidly evolving, expanding and VISIBLE fields in IT and security. The methods used to log in touch everyone, in almost every aspect of their professional and personal lives.

At the time of publication of the first State of Passwordless Report, only a fairly narrow band of security folks and tech geeks had even heard of passwordless technology. Insecure passwords were an accepted burden, and OTP codes, push notifications and other additional authentication layers seemed a viable, albeit clunky, solution to keep organizations safe.

That illusion was all but shattered last year with the high-profile breaches of Uber, Cisco, Twilio and a string of others, all which had multi-factor authentication deployed. Attackers don't need to break in, they can flash their credentials and walk through the door; MFA or not. Frankly, we're at a point in time where we're witnessing the wholesale collapse of traditional authentication methods.

In October of 2022, the Cybersecurity and Infrastructure Security Agency (CISA) issued guidance urging organizations to deploy phishing-resistant passwordless MFA based on FIDO standards. Around the same time, passkeys entered the picture, offering a secure, consumer-friendly password replacement. What a difference a few years make. Or does it?

Our third annual State of Passwordless Security report digs deeper into the issues than previous volumes, with a detailed, expanded survey that crosses regions and industries. This research and analysis – conducted independently by Vanson Bourne and sponsored by HYPR – is based on interviews of 1000 IT security decision makers with knowledge and/or responsibility for cybersecurity. These IT security decision makers were from organizations in EMEA, Asia-Pacific and Japan (APJ) and the US, ranging in size from 50 employees to large enterprises.

This report explores the full results, including the following:

- **Cyberthreats and their impact on organizations**
- **Current authentication practices and shortcomings**
- **Perceptions and misconceptions about authentication security**
- **The impact of passwordless authentication**

Key Findings

3 in 5

organizations had authentication-related breaches in the last 12 months

$2.95M

average cost of authentication-related cyber breaches in the last 12 months

28%

of organizations were hit by push notification attacks (MFA bombing), more than double the number reported in last year's study

Only 3%

of organizations that use passwordless authentication for employees are using phishing-resistant passwordless methods

Four

different systems of authentication are being used by employees daily, on average

32%

of IT helpdesk spend is related to password issues, costing organizations an average of **$375 per employee annually**

86%

believe that passwordless authentication provides the highest level of authentication security

86%

believe that passwordless authentication is needed to ensure user satisfaction

Authentication Weaknesses Are Leaving Organizations Exposed to Cyberattacks and Breaches

1

Organizations Face a Range of Cyberthreats

For anyone following the news over the past year, it won't be a surprise that the vast majority (88%) of organizations suffered a cyberattack in the last 12 months, with phishing the most prevalent form reported (43%). However, let's be frank, it's more than likely all organizations suffered a cyberattack, but only 88% of them noticed.

Close to three quarters (74%) of organizations acknowledged authentication-related attacks in the last year, suggesting cybercriminals are looking to capitalize on weak and insecure technologies. In fact, three out of the top four attack vectors are connected to authentication.

In particular, push notification attacks (28%), whereby the user receives multiple push alerts to their device requesting account access, pose a substantial threat. Also termed MFA bombing, these types of attacks have skyrocketed compared to past years' studies — The State of Passwordless 2022 and 2021 reports found push notification attack rates to be 12% and 9%, respectively. This type of attack is now easily available to attackers and was used by Lap$us, 0ktapus, and the teenager who breached Uber.

The financial services and energy/utilities sectors face the heaviest bombardment, with a full third of organizations in each of these industries hit by push notification attacks, making them targeted at a rate nearly 20% higher than average. While these sectors were more likely to report an attack in general (see Section 4 for breakdowns by industry), this figure far exceeds that which can be accounted for by greater attack volume as a whole, indicating attackers are specifically targeting the MFA processes in these sectors.

Types of Cyberattacks Faced in the Last 12 Months

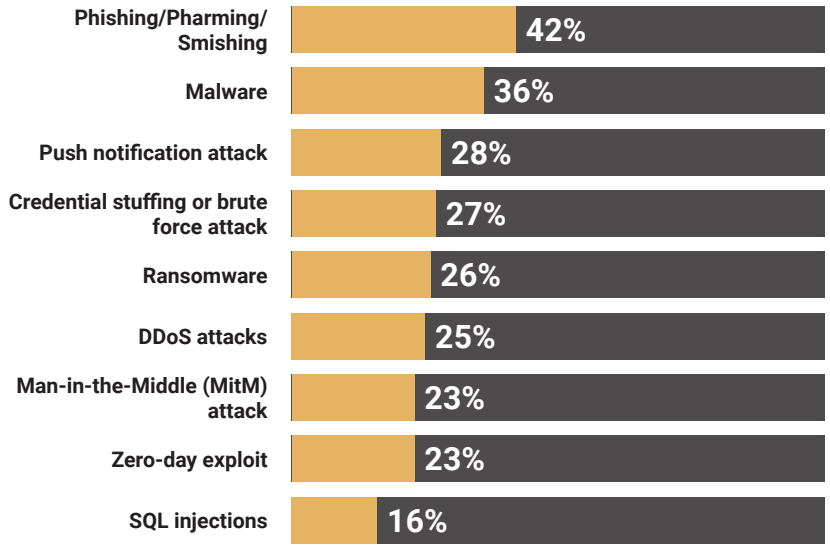


Figure 1: What, if any, types of cyber-attack has your organization faced in the last 12 months? [1,000], omitting some answer options

Insecure Authentication Plays a Primary Role in Cyber Breaches

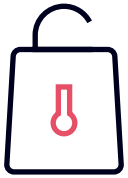
Organizations are not as secure as respondents perceive them to be (see Section 3), with 74% admitting they were breached in the last 12 months. Moreover, the majority were breached on multiple occasions – at an average of three times – indicating not only are current security measures inadequate, but organizations are also slow to identify and react to the threat with mitigating controls.

Authentication processes present a clear breach target; 82% of organizations that were breached name credential misuse or authentication weaknesses as a root cause. In other words, 3 out of 5 organizations were breached last year through their authentication processes. Furthermore, just over a fifth of respondents (22%) experienced two or more authentication-related breaches.

These findings expose significant security gaps in the authentication protocols currently used by most organizations and underscore the urgent need for methods that can combat the modern, evolving threat landscape.

74%

of all organizations report that they experienced a cyber breach in the last 12 months



82%

of those breached organizations attribute credential misuse or authentication weaknesses as a root cause

3 in 5

organizations were breached due to credential misuse or authentication weaknesses

Authentication-Related Breaches Are Impacting Organizations' Bottom Line

On average, cyber breaches caused by insecure authentication cost each organization a staggering $2.95 million in the last 12 months.

Unsurprisingly, larger organizations (500+ employees) experience higher costs than smaller organizations (50-499 employees), with $3.4 million being attributed to breaches due to authentication weaknesses, compared to $2 million respectively.

These sums would include the direct financial costs of cyber breaches, such as regulatory fines, legal costs, investigation costs and business disruption. However, over the coming months, or even years, organizations will likely face additional financial impact due to lost business, long-term remediation work, cyber insurance premium increases or reputational damage.

$2.95M

average cost of authentication-related cyber breaches in the last 12 months

Impact of Cyber Breaches over the Last 12 Months

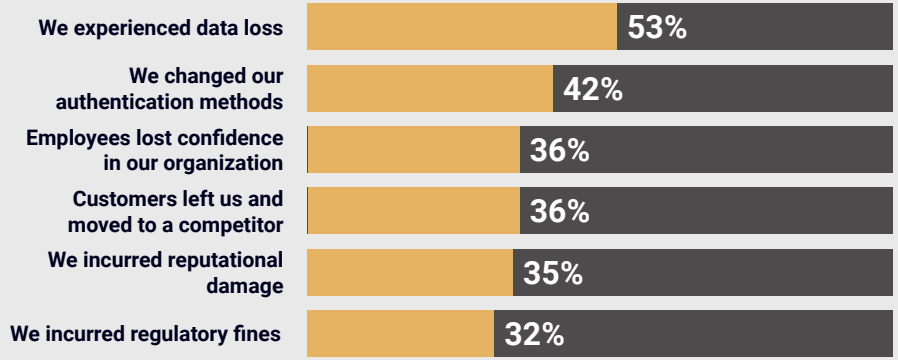


Figure 2: What was the impact of the cyber breach(es) that your organization experienced in the last 12 months? [737] omitting some answer options, only asked to those from organizations that have been a victim of a cyber breach in the last 12 months, omitting some answer options

Nearly all (95%) organizations that experienced a cyber breach suffered negative impacts to their business as a result. Over half (56%) experienced a financial impact, with over a third (36%) losing customers to a competitor and nearly that many (32%) reporting that they incurred fines. The majority (53%) of organizations also experienced the loss of data and more than a third suffered reputational damage (35%).

So, what are organizations doing about it? We are starting to see a shift in willingness to take action. While the majority (58%) still did nothing, 42% changed their authentication methods after a breach. This is up from the 2022 State of Passwordless Security survey, where only 36% reported that they made changes.

Outdated Authentication Methods Still Common

2

Organizations Use Multiple Insecure Authentication Methods

Until fairly recently, traditional two-factor/multi-factor authentication (MFA), which uses a password plus another factor, was the recommended best practice for authentication. However, attackers have developed techniques to crack these methods, leading the United States Cybersecurity and Infrastructure Security Agency (CISA) and other industry bodies to strongly urge all organizations to adopt phishing-resistant MFA.

This message, however, hasn't trickled down into practice yet. While organizations are using a range of authentication methods for their workforce, the majority use insecure legacy methods, with **a shocking 57% using only a username and password for some systems**. More than half (54%) use traditional MFA. Encouragingly, more than a quarter state they employ a more modern passwordless authentication approach – although as we'll see in Section 3, there seems to be confusion as to what a passwordless solution actually entails.

Organizations also face challenges from the sheer variety of authentication systems used on a daily basis — four on average. This means multiple, varying sign-on requirements that employees must remember and use, adding friction and frustration in their day-to-day work.

Four

different systems of authentication are being used by employees daily, on average

Workforce Authentication Methods Currently in Use

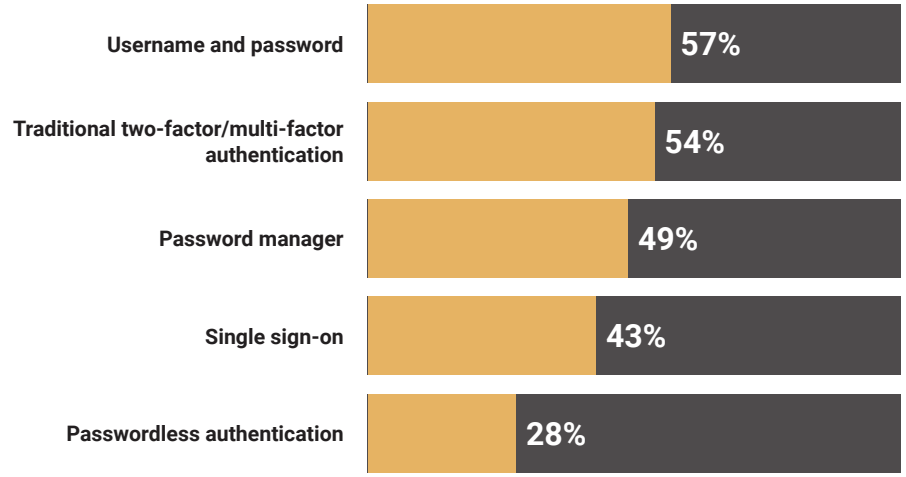


Figure 3: Which of the following authentication methods does your organization currently use for its employees? [1,000], omitting some answer options

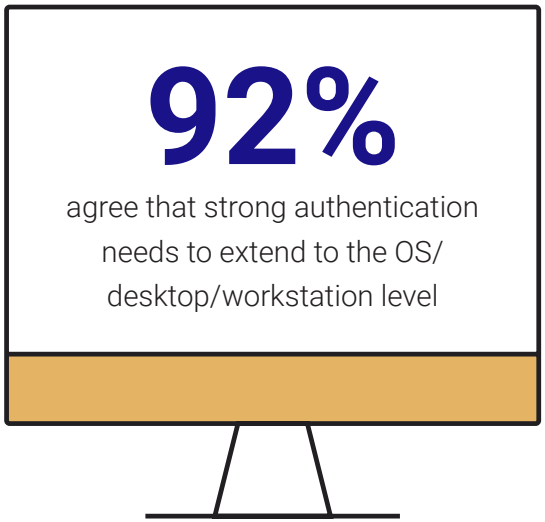
Customer Authentication Practices Equally Insecure

While this report is primarily concerned with workforce authentication, we took a pulse on the customer side and found many organizations using insecure methods for their customers as well. Over half (53%) require only a username and password, 49% use traditional MFA, and 39% rely on social identity credentials.

Username and Password Remain a Common Method for Accessing Laptops/Desktops, Despite Risks

As the first point of login, desktop authentication holds a critical position for the security of the organization. Unauthorized access can grant cyber criminals an array of profitable information such as the corporate directory or user accounts, to name a few. It is therefore concerning that nearly all organizations (97%) allow at least a portion of their employees to access their laptop/desktop with only a username and password.

Encouragingly, most (92%) agree that strong authentication needs to extend to the OS/desktop/workstation level. The problem may lie in the authentication technologies we see currently in use by those organizations – most sit at the application level and cannot support desktop-level authentication.



What About Passkeys?

Notably absent from the types of authentication we've discussed is the newest authentication method on the scene, passkeys. Passkeys replace passwords with a cryptographic key pair and on-device authentication to make user login easier and more secure. The most commonly discussed form of passkeys, the multi-device passkeys announced by Apple, Google and Microsoft, generally are meant for consumer use and lack certain security and management capabilities that would make them suitable for enterprise deployment. It will be interesting to see how passkey adoption in the market influences future authentication practices in enterprise IAM systems.

Many Organizations Remain Unaware of Their Authentication Security Risks

Fact:
The majority of organizations were breached in the last 12 months due to weaknesses in their authentication technologies and processes.

Fact:
Insecure authentication practices remain pervasive.

Conundrum:
The majority (87%) of IT and security leaders consider their organization's approach to authentication to be completely or mostly secure.

There's a clear dissonance between facts on the ground and the perceived security of organizations' approach to authentication. This becomes even more blatant upon closer investigation – those organizations that consider their authentication completely secure were actually the most likely to report an authentication-related breach (66%). Conversely, those that consider themselves only somewhat secure recorded the fewest (51%).

We explore possible sources of this mislaid trust throughout the rest of this report.

Perceptions of Authentication Security Level in Organizations

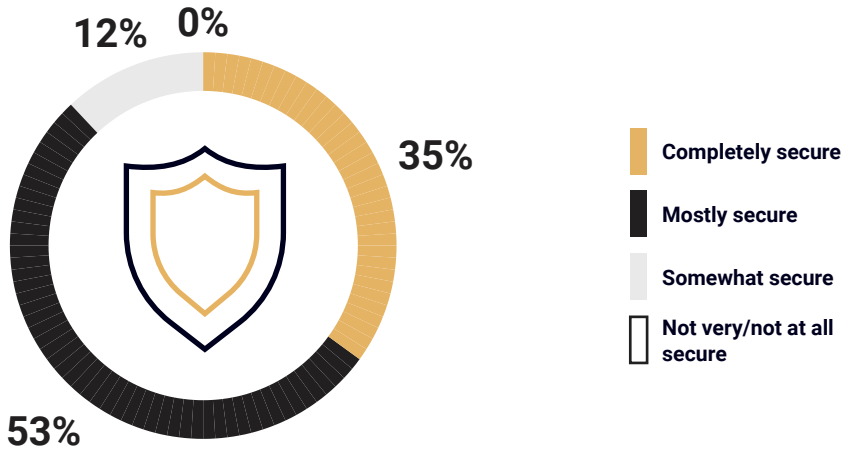


Figure 4: How secure do you consider your organization's approach to authentication to be? [1,000], omitting some answer options

Current Authentication Practices Create Significant Challenges for Organizations

Although IT and security leaders voice confidence in the security of their organization's authentication approach, that optimism is less evident when we dig into specifics. Nearly all (96%) find inadequacies with their current authentication methods, with challenges being seen across the business.

In fact, two thirds (67%) experience challenges with their organization's security, with securely authenticating remote workers (36%) and third-party devices (35%) among the top issues named. User experience is also a major pain point for organizations (64%). Around a third (31%) report resistance from employees in using authentication technology and a similar proportion (29%) cite password/credential resets as a problem. This serves as a stark reminder that user experience holds a role as important as security when it comes to adoption of authentication technology.

Authentication approaches take a toll on IS and IT teams too. More than half (56%) face IT-related obstacles, including management complexity (34%) and integration difficulties (31%).

Pain Points of Current Authentication Methods

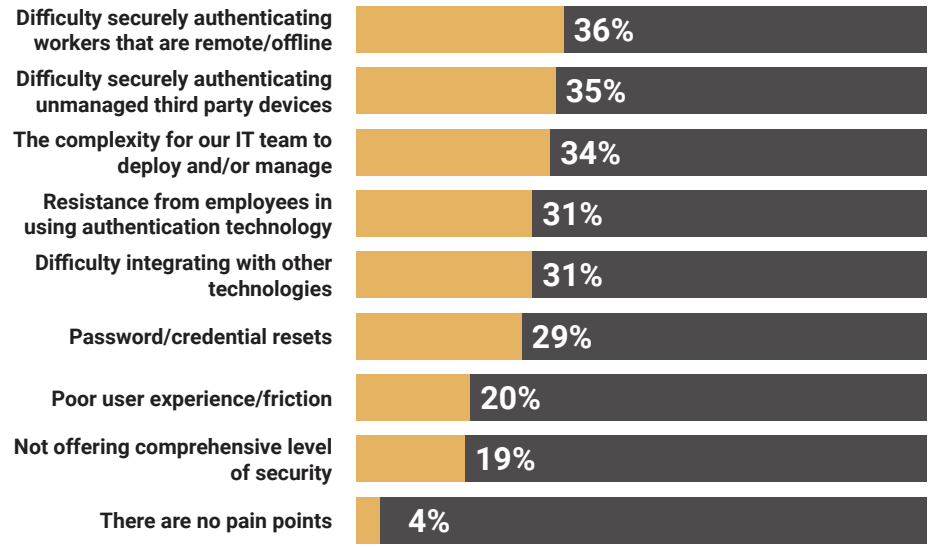


Figure 5: What are the pain points associated with your organization's current authentication methods? Combination of responses ranked first, second and third [1,000], omitting some answer options

Pain Points are Impacting Multiple Areas:

56%
IT-related

64%
UX related

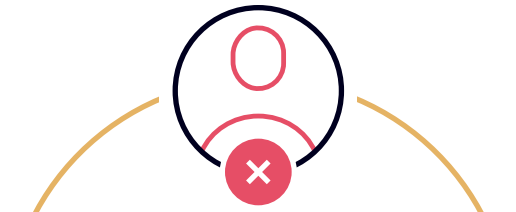
67%
security related

Passwords Take a Toll on Productivity and IT Help Desks

Around eight in ten (81%) respondents report that they've been unable to access critical information due to forgetting their password – a considerable increase from the 63% who responded in the same way for the State of Passwordless Security 2022 study.

This not only harms employee productivity, it creates a tremendous help desk burden. Just over three quarters (76%) of organizations have seen an increase in their number of help desk requests regarding password resets or other authentication issues in the past 12 months, registering an average increase of 13%.

What does this mean for their balance sheet? On average, organizations spend 32% of their IT help desk budget on password resets and password-based authentication issues. This equates to $465,645 annually, or $375 per employee per year, wasted on password issues.



81%

could not access work-critical information because they forgot a password

$375

per employee per year is wasted on password issues

Passwordless Authentication and Phishing-Resistance

3

Passwordless Authentication Can Improve Conditions for Users and IT Teams as Well as Security

It's encouraging to see IT and security decision makers acknowledging the benefits that passwordless authentication can bring to their organization. Nearly all (98%) respondents believe that organizations will benefit from implementing passwordless methods.

The top stated passwordless benefit is improved user experience to increase productivity (45%). This stands to reason given that respondents named poor user experience and impacted job performance as challenges with their current authentication practices (Section 2). Similarly, four in ten (42%) believe they can increase workforce adoption of MFA by turning to passwordless authentication, thereby solving the issue of employee resistance observed earlier. The security benefits of passwordless are also top of mind for practitioners including reducing breach risk (43%) and moving away from insecure legacy technologies (36%).

Benefits of Passwordless Authentication

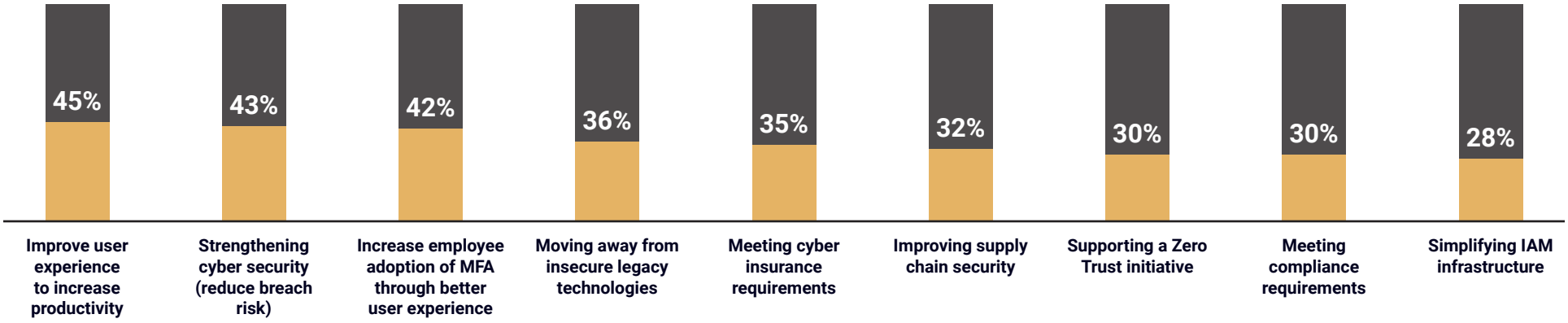


Figure 6: In general, what are the benefits to organizations using passwordless authentication methods? [1,000], omitting some answer options

Passwordless Gaining Traction

Organizations are clearly ready for a change. With authentication-related breaches costing an average of $2.95 million per year and help desk costs adding another $465K, companies spend over $3.4 million annually on troubles stemming from their authentication processes.

Respondents overwhelmingly see passwordless authentication as the fix to the security and usability problems posed by passwords and traditional MFA. The vast majority (86%) state it provides the highest level of authentication security. The same proportion say organizations need to fully embrace passwordless in order to ensure user satisfaction (86%).

In fact, on the surface, it appears that passwordless authentication is already part of the authentication strategy for a sizable number of organizations. As we saw, 28% of respondents believe that their organizations use passwordless technology for at least some systems. If that's the case, why do we still see an alarmingly high number of authentication-related breaches?

86%

state passwordless authentication provides the highest level of authentication security

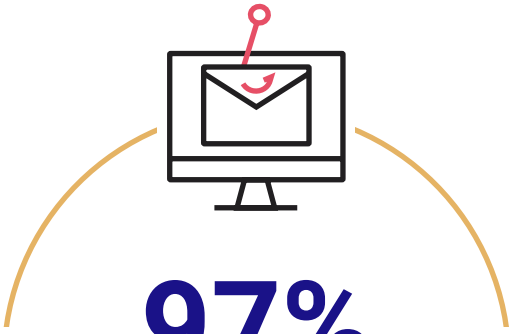
86%

say organizations need to fully embrace passwordless in order to ensure user satisfaction

Misconceptions About Passwordless Authentication Place Organizations at Risk

Despite increased advocacy for passwordless authentication from all quarters, it appears serious misunderstandings linger. The majority of respondents from organizations currently using passwordless solutions report that their solution includes the use of one-time passwords (OTPs) via a mobile authenticator app (58%), OTP hardware tokens such as RSA tokens (54%), push notifications (53%) or stored passwords that are unlocked with biometrics and relayed on the backend (50%).

In fact, nearly all these respondents report that their organizations' ostensibly "passwordless" solutions include the use of at least one technique that requires a password, shared secret or other phishable technique — to the extent where only 3% are using a truly passwordless solution. This means that the vast majority can be bypassed at scale through push fatigue and other MFA attacks – techniques that are surging as noted in Section 1.



97%

of the "passwordless" solutions deployed are susceptible to phishing and push attacks

Education Still Needed About Passwordless, Phishing-Resistant Multi-Factor Authentication

The glaring misconceptions about what and what doesn't constitute passwordless MFA start to make sense when looking at respondents' understanding of the different types of multi-factor authentication.

There appears to be ongoing confusion between the capabilities of traditional MFA and the more secure, passwordless, phishing-resistant approach. Despite extensive published guidance, around two thirds (65%) could not correctly identify the differences between the two methods. Instead believing that you can still use OTPs, SMS or even passwords as an authenticating factor and still be considered phishing resistant.

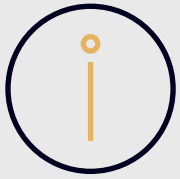
With this in mind, it's understandable, yet highly concerning, that most of those surveyed (82%) believe that traditional MFA can provide complete or high levels of security. It's not that organizations are ignoring the threat from attacks; it's that they think they're covered.

65%

could not correctly identify traditional vs. phishing-resistant MFA

82%

feel that traditional MFA provides complete/high security



Phishing-resistant multi-factor authentication is based on public-key cryptography and uses secure, on-device factors to verify identity.

It doesn't use any type of credential that could be phished or intercepted by attackers including: passwords, one-time passwords (OTP), SMS messages, push notifications, phone calls, and security questions.

For an extensive explanation, see the CISA fact sheet.

FIDO Standards Are Critical to Passwordless Adoption

Perceived hurdles in the implementation of newer approaches may also be slowing down authentication modernization in organizations. A significant portion (38%) of IT security leaders believe it would be difficult to integrate passwordless authentication into their current technology stack). A similar number (36%) report concerns regarding a lack of internal knowledge on how to adopt the technology.

However, the use of a standards-based approach such as Fast Identity Online (FIDO) has the potential to overcome these barriers. FIDO defines an interoperable set of phishing-resistant passwordless authentication protocols that can work seamlessly across platforms and IdPs. By deploying an independent authentication solution, organizations can reduce their IAM complexity as authentication is decoupled from their existing IdP and technology suites.

IT security leaders decidedly acknowledge this, with nine in ten (90%) agreeing that a standards-based approach such as FIDO is important when planning a journey to passwordless authentication.

FIDO-based passwordless is considered the gold standard for phishing-resistant authentication by CISA, the US OMB and other regulatory bodies. So it's encouraging to see that most organizations not only concur on their marching orders to move forward, but it's aligned with the latest regulatory guidance.

fido™ CERTIFIED

90%

agree that leveraging a standards-based approach such as FIDO is/would be important when planning a journey to passwordless authentication

What About Industries and Geographies?

Authentication remains an issue for all companies regardless of industry, geography or size. However, interesting insights emerge when digging into sector and regional differences. Are finance organizations the most targeted? Is EMEA really doing a better job of stopping authentication-related breaches? We take a look in the sections that follow.

Industries

4

Financial Services and Energy/Utilities Hit The Hardest

Looking at the data industry by industry, we see some notable differences between sectors, both in terms of the threat landscape and authentication approach.

Organizations in the financial services and energy/utilities sectors are far more likely to sustain attacks and breaches than those in other sectors. Nearly all (95%) of financial services organizations and 91% of those in the energy/utilities sectors reported cyberattacks while only 72% of healthcare organizations acknowledged an attack. Specifically, these industries face greater authentication-related threats. More than 8 in 10 (81%) of organizations in financial services and 77% in energy/utilities were targeted by attacks on their authentication processes – globally the average was 74%. These organizations are also the most likely to be breached, with almost 9 in 10 (87%) from the energy/utilities sector and 83% of those from the financial services sector reporting cyber breaches.

Experienced an Attack on Authentication in the Last 12 Months

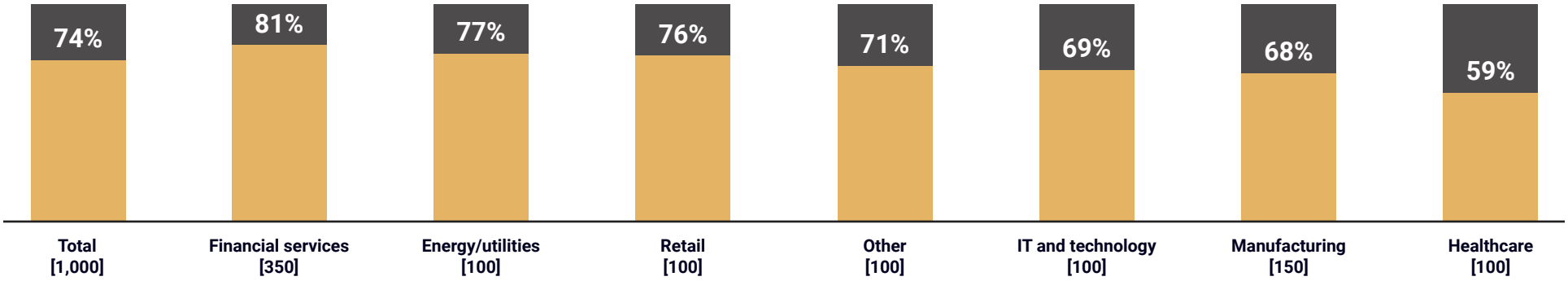


Figure 8: What, if any, types of cyber-attack has your organization faced in the last 12 months? [base sizes in chart], split by industry, omitting some answer options

There's Cross-Industry Support for Passwordless Technology but Expertise is Uneven and Plans Vary

Our research confirms that the most regulated industries are also the most savvy about authentication. IT security professionals in the healthcare (50%) and financial services (45%) sectors far outperformed their counterparts when it comes to understanding the differences between traditional MFA and phishing-resistant authentication methods. Ironically, only 13% of those from the IT and technology sector displayed a correct understanding of the concepts.

No matter their grasp of specific terms and definitions, IT security leaders across all industries (98%) acknowledge the benefits brought by passwordless authentication. However, some sectors plan to incorporate passwordless technology in their IAM strategy sooner than others. Around 4 in 10 financial services firms (39%) and retail organizations (41%) plan to adopt or use passwordless authentication in the next 1-3 years. By contrast, only 19% in the energy/utilities sector include passwordless authentication in their IAM plans over the next three years. We should note, however, that the blitz of press coverage and consumer interest in passkeys may cause organizations to accelerate their passwordless plans.

Planning to Use Passwordless Authentication in the Next 1-3 Years

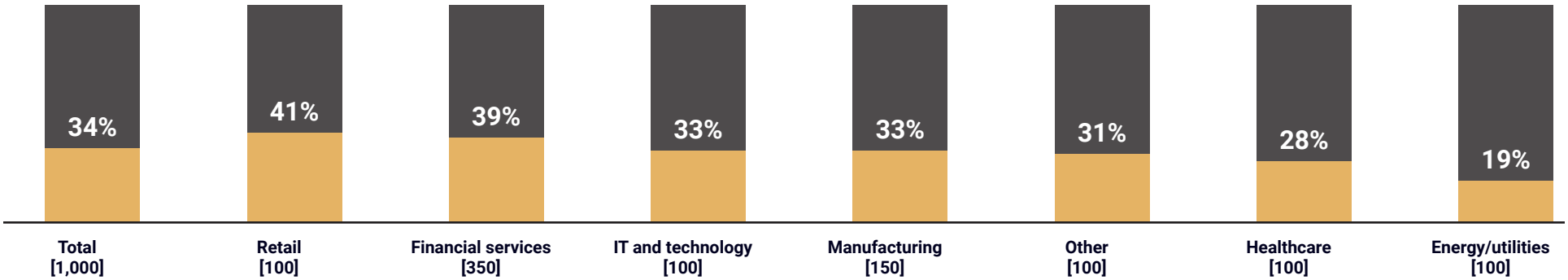


Figure 9: Which of the following authentication methods does your organization plan to adopt, or use/continue to use in the next 1-3 years? [base sizes in chart], split by industry, only showing responses to passwordless authentication

Geographies

5

Authentication Is a Global Issue

We see the same general story play out across geographical regions: attacks on authentication; the will but not necessarily the knowledge to address. What are the consequences from a geographical perspective?

Organizations in France are most likely to have experienced a cyberattack on their authentication methods in the last 12 months (81%) and also are the most likely to register cyber breaches associated with authentication weaknesses (70%).

Looking across regions, organizations in APJ (84%) and the US (85%) are most liable to report authentication weaknesses as the cause of breaches. Those in APJ, however, contend with much higher associated costs. Breaches caused by authentication weaknesses cost organizations in APJ a shocking $6.3 million per year on average, compared to $2.4 million in the US and $2.95 million globally.

Experienced a Breach as a Result of Authentication Weaknesses

Figure 10: Were any of the cyber breaches that your organization experienced related to credential misuse or authentication vulnerabilities? [base sizes in chart], split by region, only shown to those who experienced a cyber-attack in the last 12 months

APJ and the US Heading the Passwordless Pack

While the APJ and the US hold the dubious honor of the highest rates of breaches due to authentication weaknesses, they also are actively seeking to address this. Organizations in these regions (tied at 37%) are the most likely to be looking to implement passwordless authentication in the coming years. Increased security is one obvious driver of this change. Approaching nine in ten (87%) from APJ and even more in the US (91%) agree that passwordless authentication provides the highest level of authentication security.

However, user experience plays an equally important role in the adoption of passwordless authentication. This makes sense as it's an area where many organizations are experiencing pain points (as highlighted in section 2). Those in the US are most likely to recognize benefits in this area (70%), while around two thirds of those in APJ (66%) and EMEA (65%) say the same. Interestingly, organizations in the US place a higher priority on user experience in general. Nearly all organizations in the US (96%) say user experience needs to be prioritized when considering authentication but this drops to 87% for those in EMEA.

Planning to Use Passwordless Authentication in the Next 1-3 Years

Figure 11: Which of the following authentication methods does your organization plan to adopt, or use/continue to use in the next 1-3 years? [base sizes in chart], split by region, only showing responses to passwordless authentication

Conclusion

The inescapable verdict from this report is that, at nearly 65 years old and doing a job it was never meant for, it's time for the password to retire. Passwords are a fundamentally flawed part of any authentication system, and systems built on top of them, including almost all MFA solutions, are destined to fail. Most organizations' authentication security crumbles in the face of today's threats, leading to breaches that cost them nearly $3 million annually, on average. What's more, their approaches create friction and frustration for their users and IT teams.

While this study was started before passkeys became a household term, we hope that the market attention they receive will accelerate passwordless adoption. Only then can we overcome some of the concerning issues highlighted in these pages.

Migrating away from legacy authentication technologies toward phishing-resistant passwordless MFA must now be a priority for organizations; however, buy-in from employees will be essential to a successful transition. A good user experience and smooth deployment are as important as the security of any system.

A Passwordless Future is Here

The good news is that it is already being done. Organizations large and small are ridding themselves of passwords. One multinational corporation was able to transition nearly their entire workforce in less than five months. The key is not only the right technology, but a partner well-versed and ready to support the change management required.

HYPR True Passwordless™ MFA delivers security assurance and frictionless experience, with phishing-resistant login that begins at the desktop and extends to the cloud. Designed to deploy rapidly into existing infrastructure, it turns an ordinary smartphone into a FIDO security key, delivering hardware-grade security with software-grade flexibility. HYPR is deployed at scale in organizations across the globe for both employee and customer scenarios.

Research Scope/Methodology:

HYPR commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this whitepaper is based. A total of 1,000 IT security DM respondents were interviewed in December 2022 and January 2023. Respondents were targeted in the US (300), UK (250), France (100), Germany (100), China (100), Australia (75) and Japan (75), and were from organizations with 50+ employees across a range of private and public sectors. Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated the results discussed are based on the total sample.

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

Learn more at www.vansonbourne.com

HYPR fixes the way the world logs in. HYPR's True Passwordless™ MFA combines phishing-resistant multi-factor authentication with an intuitive and simple user experience so that organizations decrease their risk of attack, improve user experience, lower operational costs and ensure regulatory compliance. HYPR is an industry leader, securing organizations globally with proven deployments at scale in some of the most complex and demanding environments.

See how HYPR helps secure your workforce and customers

Visit: hypr.com/demo