The State of Passwordless Identity Assurance 2025

HYPR | S&P Global Market Intelligence

Foreword

The Identity Renaissance: From Passwords to People

Anyone who has studied art history knows that the Renaissance wasn't merely a period of artistic achievement, it was a fundamental reimagining of how humans saw themselves and their place in the world. Today, we find ourselves at a similar inflection point in the digital realm: an Identity Renaissance.

In this transformative moment, we must reconsider our relationship with digital identity. As this report clearly demonstrates, the old models of authentication, centered on passwords, knowledge-based verification, and even many forms of traditional MFA, are becoming relics of a bygone era. The data is stark: nearly half of all organizations surveyed suffered a breach in the past year, with an overwhelming 87% of those breaches linked directly to identity vulnerabilities.

The enterprising adversaries of today understand something many organizations have been slow to acknowledge — identity is no longer just about access. It's about verifying the authenticity of a person at every step of their digital journey. Malicious actors aren't breaking in; they're logging in, assuming identities, and exploiting our trust in systems that rely on shared secrets rather than verified identities.

Perhaps most concerning is how quickly these threats are evolving. Nearly 40% of organizations experienced a GenAI-related security incident in the past year alone, and deepfake technology has become a mainstream threat, with 95% of those organizations encountering some form of deepfake attack. The speed with which identity-based threats can move is breathtaking — a reality that echoes what we've seen across the broader cybersecurity landscape.

But this report also reveals promising signs of progress. For the first time in the five-year history of this survey, phishing-resistant authentication methods are projected to surpass traditional methods within the next two years. Organizations that embrace these modern approaches, including FIDO passkeys and advanced identity verification tools, report significantly lower rates of identity-based breaches.

At HYPR, we aren't waiting for the identity landscape to transform itself. We're accelerating our use of advanced authentication and verification techniques to help our customers anticipate and prevent identity-based attacks before they occur. This is the essence of our approach to identity security. Unlike legacy systems, which are still relied upon by organizations globally, we don't sit idle until an attack occurs before we can identify and stop it.

Protecting your digital identities continues to require greater focus with each passing day. You'll find ample evidence of this fact in the data that follows. But you'll also find a roadmap to a future where identity security isn't just about who can log in, but about confidently knowing who is behind every digital interaction.

The Identity Renaissance is here. We must either embrace it, or risk becoming digital security's equivalent of the Dark Ages.

Bojan Simic
HYPR CEO

Contents

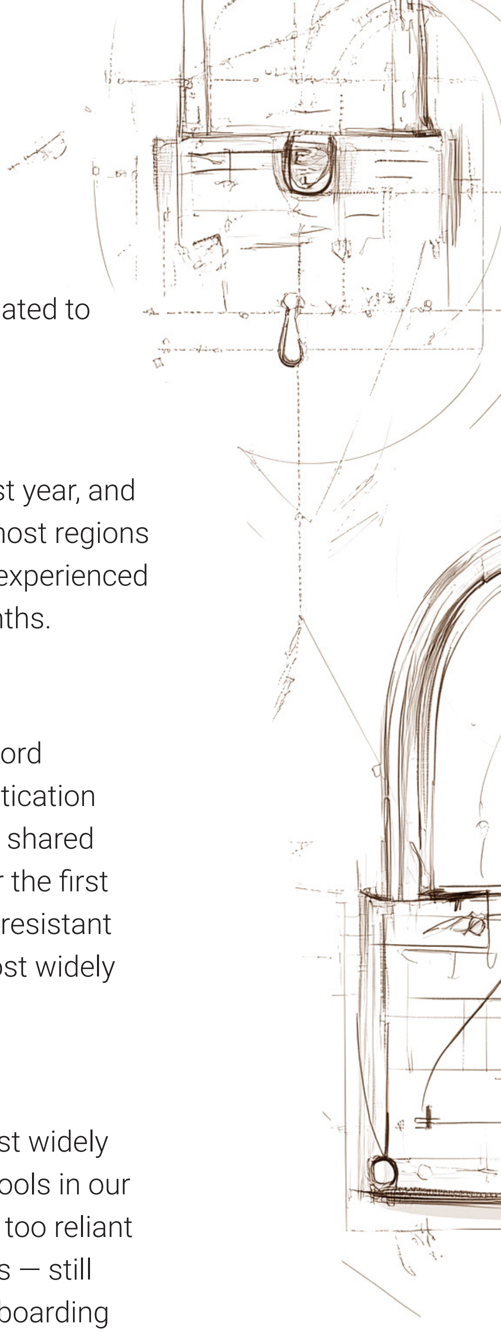
Introduction

It has become common in security circles to warn that attackers no longer break in — they log in.

The fifth annual State of Passwordless Identity Assurance report, commissioned by HYPR and produced by S&P Global Market Intelligence 451 Research, confirms that this adage is more relevant than ever. Identity remains the Achilles' heel of enterprise security, with breaches relentlessly exploiting not just identity assets and infrastructure, but the very processes meant to safeguard them — from credential resets and device replacements to employee onboarding workflows and remote access requests. Our research indicates that identity vulnerabilities play an increasingly critical role in the majority of breaches.

However, there are signs of progress. This year's report reveals that organizations that embrace new phishing-resistant authentication methods (such as passwordless authentication based on Fast IDentity Online (FIDO) passkeys or public-key cryptography) and advanced identity verification tools are less likely to experience an identity breach than those whose adoption lags.

Key Findings



Nearly half of surveyed firms (49%) report they had a breach in the past year alone.

The vast majority (87%) of those breaches were related to identity vulnerabilities.

GenAI is becoming a top identity security concern.

GenAI has garnered numerous headlines in the past year, and it represents the top identity security concern for most regions and industry verticals. Nearly 40% of respondents experienced a GenAI-related security incident in the last 12 months.

Passwordless authentication is poised to surpass traditional authentication methods.

Traditional authentication methods such as password managers (65%) and "standard" multifactor authentication (MFA) tools (52%), such as OTP tokens that rely on shared secrets, remain the most widely used. However, for the first time in the five-year history of this report, phishing-resistant authentication methods are projected to be the most widely deployed methods within the next two years.

Identity verification is broadly used but remains reliant on in-person visits and knowledge-based authentication.

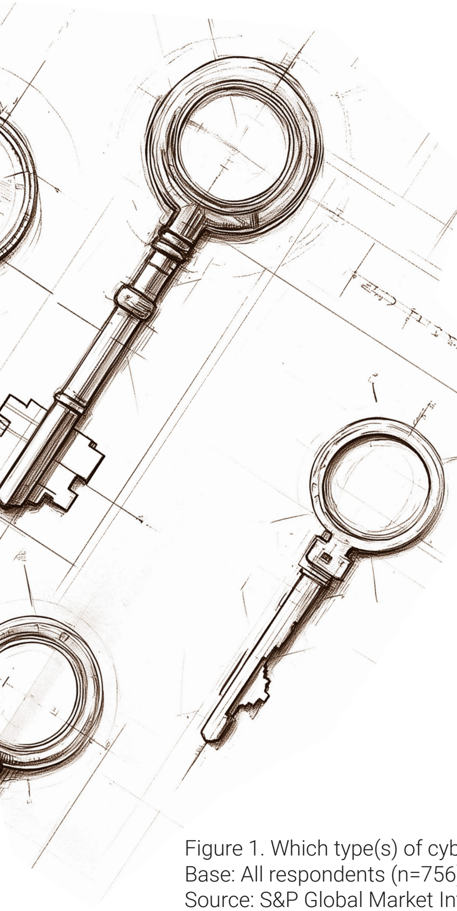
Identity verification (IDV) tools are some of the most widely deployed identity and access management (IAM) tools in our survey overall (63%), and also the top IAM remains too reliant on traditional, manual methods such as office visits — still used by nearly three-fourths of respondents for onboarding new employees — and document-based authentication, both of which are relatively inefficient and insecure.

Threat Trends and Impacts

1

Breaches up sharply due to credential abuse, phishing and remote access rights

Many in the industry have become numb to the reality of an unabating stream of cybersecurity incidents. Nearly half of firms in our survey (49%) have been breached in the past year alone. The vast majority of those successful attacks were specifically related to identity vulnerabilities such as stolen or misused credentials, phishing and inappropriate remote access rights. When we asked respondents whether they were breached due to an identity issue, more than half (52%) answered “Yes, definitely,” while another 35% answered “Yes, probably.” All in, this amounts to nearly nine out of 10 respondents (87%) — a staggering, but sadly no longer surprising, number. Drilling down into the drivers of this phenomenon, we find that the top identity vulnerabilities identified by survey respondents are credential misuse (47%), privileged access abuse (41%), social engineering (36%) and MFA bypass attacks (35%). The most common types of attacks respondent firms have experienced in the past 12 months are phishing, pharming and smishing (43%); malware (41%); and identity impersonation (30%).



Cyber Attacks Experienced in the Past 12 Months

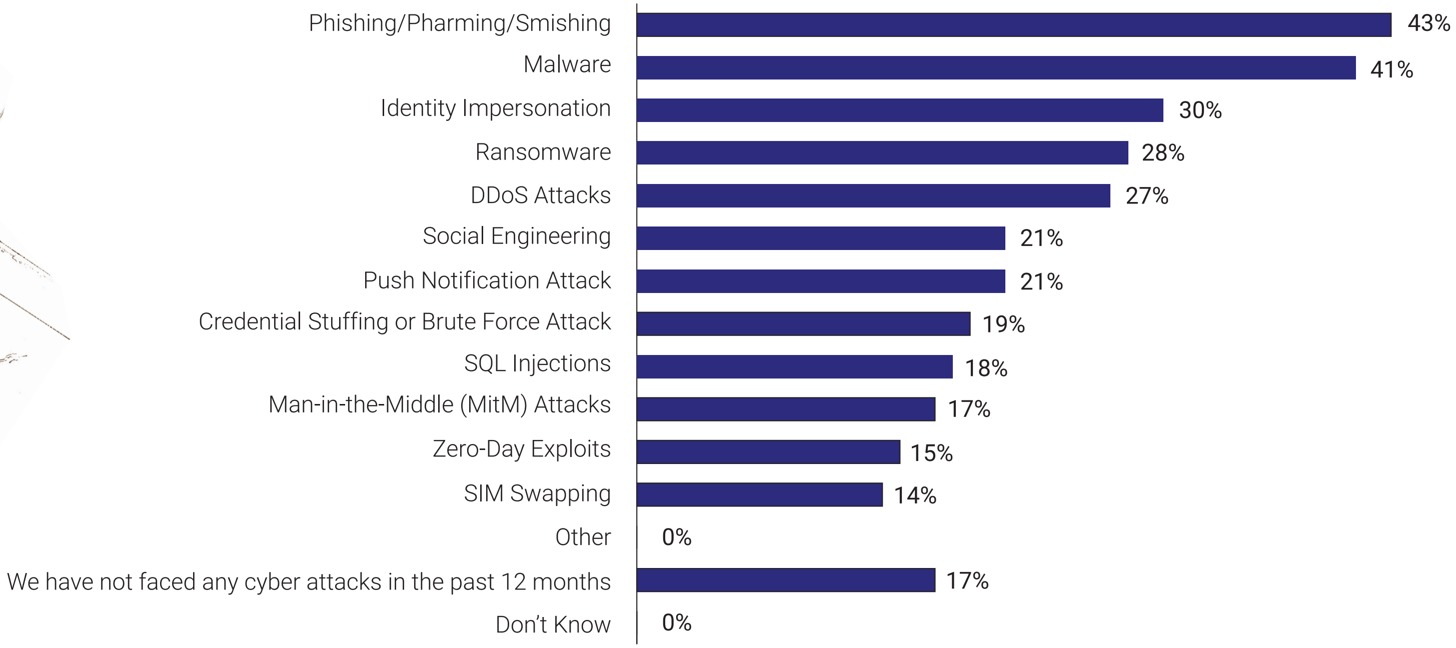


Figure 1. Which type(s) of cyberattack has your organization experienced in the last 12 months (if any)?
Base: All respondents (n=756).
Source: S&P Global Market Intelligence 451 Research custom survey commissioned by HYPR.

Similarly, respondents' top identity security concerns include phishing and credential attacks (46%), managing access for remote employees (46%) and ensuring regulatory compliance (46%). Many of these challenges can be addressed via more secure authentication and identity verification approaches.

Such security challenges contribute directly to the ultimate cost of breaches, as well as to the cost of tools that organizations require to protect against them. Indeed, as the volume and frequency of attacks continue to grow, security spending is rising in tandem. Respondents to 451 Research's Voice of the Enterprise (VotE): Information Security, Budgets & Outlook 2024 survey expected to increase cybersecurity budgets by an average of 30% in the next 12 months.

The largest share of respondents — roughly half — indicate that they spend between 1% and 10% of their overall IT security budgets on identity security, with a weighted average of 14%. Additional data from the same VotE survey shows that IT security budgets rarely decline — less than 5% expect their annual security budgets to fall. Yet, despite steady (and steadily growing) security budgets, breaches still happen, and they carry stiff financial consequences. According to our survey data, the average cost of an identity-related breach in the past year was US$2.5 million, with the most common negative impacts including downtime or business disruption (40%), loss of sensitive data (33%) and reputational damage (33%).

Negative Impacts of Identity-Related Breaches

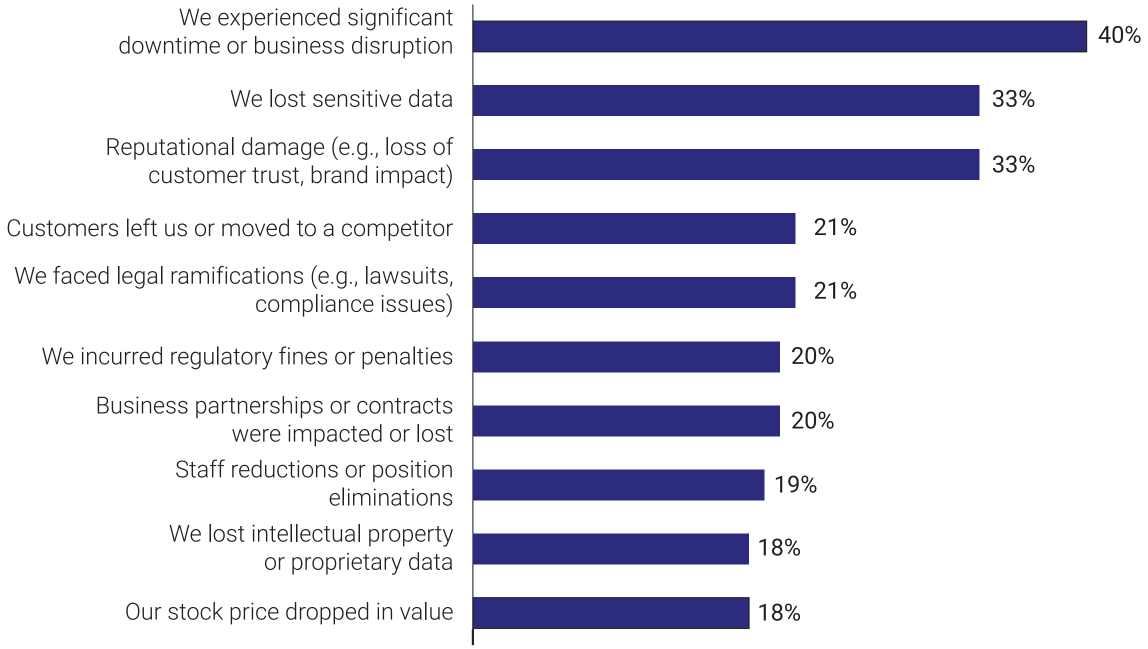


Figure 2. What negative impact(s) has your organization experienced as a result of the cyber breach(es) experienced in the past 12 months?
Base: Respondents who faced a cyber breach in the past 12 months (n=305).
Source: S&P Global Market Intelligence 451 Research custom survey commissioned by HYPR.

33%
experienced
reputational damage
after a breach

21%
faced legal ramifications
such as lawsuits
and compliance issues
after a breach

Common measures that organizations take in response to a breach include increased investment in cybersecurity (61%) and security audit (52%). Half of organizations have changed their authentication methods in response to being breached. Regarding consequences, 33% experienced reputational damage, 21% faced legal ramifications such as lawsuits and compliance issues, 20% incurred penalties or fines, and 18% noted a decline in their stock price.

Improvement Measures Taken in Past 12 Months after Cyber Breach

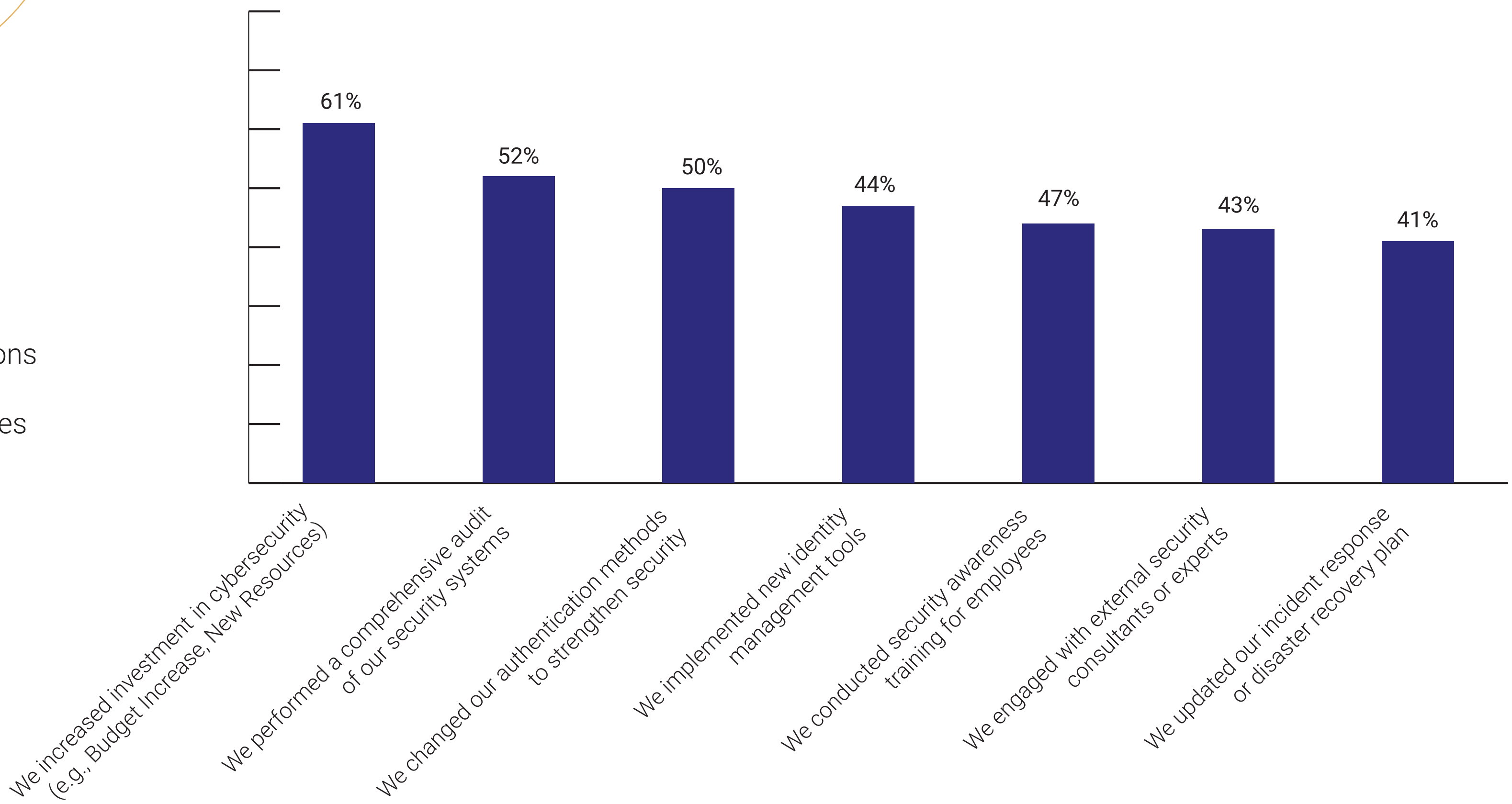


Figure 3. What improvement actions has your organization taken as a result of the cyber breach(es) experienced in the past 12 months?
Base: Respondents who faced a cyber breach in the past 12 months (n=305).
Source: S&P Global Market Intelligence 451 Research custom survey commissioned by HYPR.

While breaches can lead to both direct and indirect costs, a potentially overlooked impact of a breach is lost revenue. For example, breaches can indirectly impact revenue via staff reductions. Nearly one-fifth (19%) of respondents indicated that breaches led to staff reductions, most likely for cost containment. Of those respondents, 34% reported a reduction in executive staff, while 27% (38% in the US) noted a reduction in frontline workers that interact with customers and help drive new business, such as sales and customer service representatives.

In addition to the steady stream of breaches, compliance requirements and industry regulations affect cybersecurity budgets. For IAM specifically, requirements for phishing-resistant MFA from organizations such as the US Cybersecurity and Infrastructure Security Agency and the Office of Management and Budget have provided support for spending on modern authentication methods. Compliance requirements are also moving beyond large, publicly traded companies and prompting smaller organizations to become more proactive with identity controls as regulators move downstream.

Leading categories for projected increases in identity security spending include identity threat detection and response (77% expect to increase spending, 30% "significantly"), customer IAM (70% expect to increase spending, 25% "significantly") and identity governance and administration (66% expect to increase spending, 26% "significantly"). ITDR is a relatively new category that is focused on detection and response capabilities specifically for identity resources, such as directory services (Active Directory, Entra ID, Okta, etc.) or other parts of an organization's IAM estate. When asked about spending plans specifically due to an identity breach, respondents cited IDV (68%), MFA (60%) and, once again, ITDR (52%) as the top three investment areas. As we discuss in more detail later in this report, IDV methods help ensure the accuracy of registered identities, using a variety of techniques such as device verification, background checks, location checks and document verification.

New Identity Management Tool Implemented After Cyber Breach

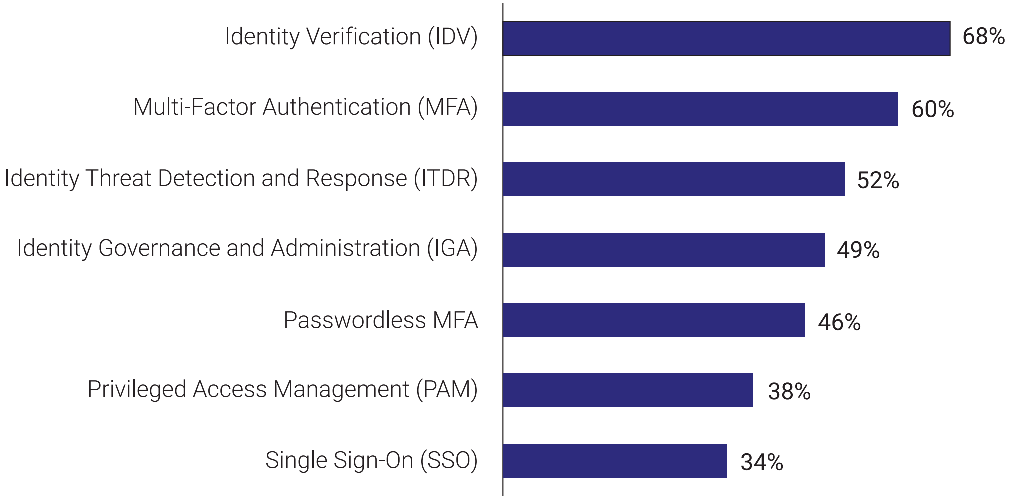


Figure 4. Which new identity management tools did your organization implement as a result of the cyber breach(es) experienced in the past 12 months?
Base: Respondents who implemented new identity management tools due to a cyber breach in the past 12 months (n=142).
Source: S&P Global Market Intelligence 451 Research custom survey commissioned by HYPR.

Ongoing Identity Security Challenges

2

GenAI becoming a top identity security concern

Security threats posed by GenAI have garnered numerous headlines in the past year, so it is understandable that GenAI is respondents' top identity security concern across most regions. Like most advances in IT, GenAI presents both opportunities and challenges for cybersecurity. On the positive side, GenAI makes it much easier for security personnel to automate repetitive or manual processes and obtain faster and more accurate insights. On the flip side, GenAI also makes it relatively easy to spoof messages and create more convincing emails using tools such as ChatGPT. One real-world example is video game maker Activision, which was targeted by a phishing campaign in 2022 that leveraged faked SMS messages to obtain sensitive data.

It follows, then, that the top cited GenAI security concerns are misuse of AI-generated content (54%), vulnerabilities in GenAI systems (53%) and more targeted phishing attacks (49%). Those fears are backed up by our survey data: Nearly 40% of respondents experienced a security incident related to GenAI in the last 12 months alone, and 95% have experienced some form of a deepfake incident. Respondents identified altered static images (50%), manipulated live audio (44%) and manipulated recorded audio (41%) as the most commonly encountered deepfake formats.

GenAI-Related Security Incidents in Past 12 Months

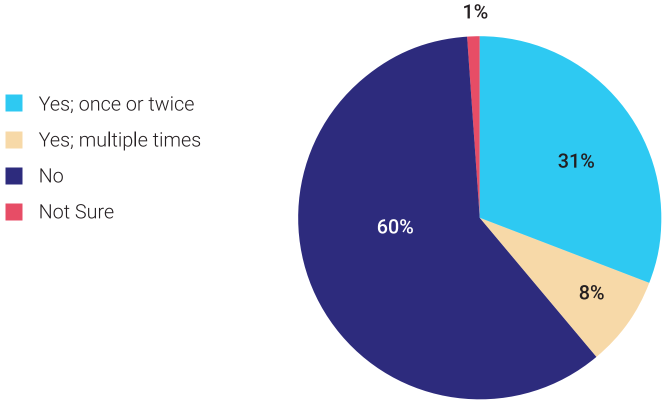
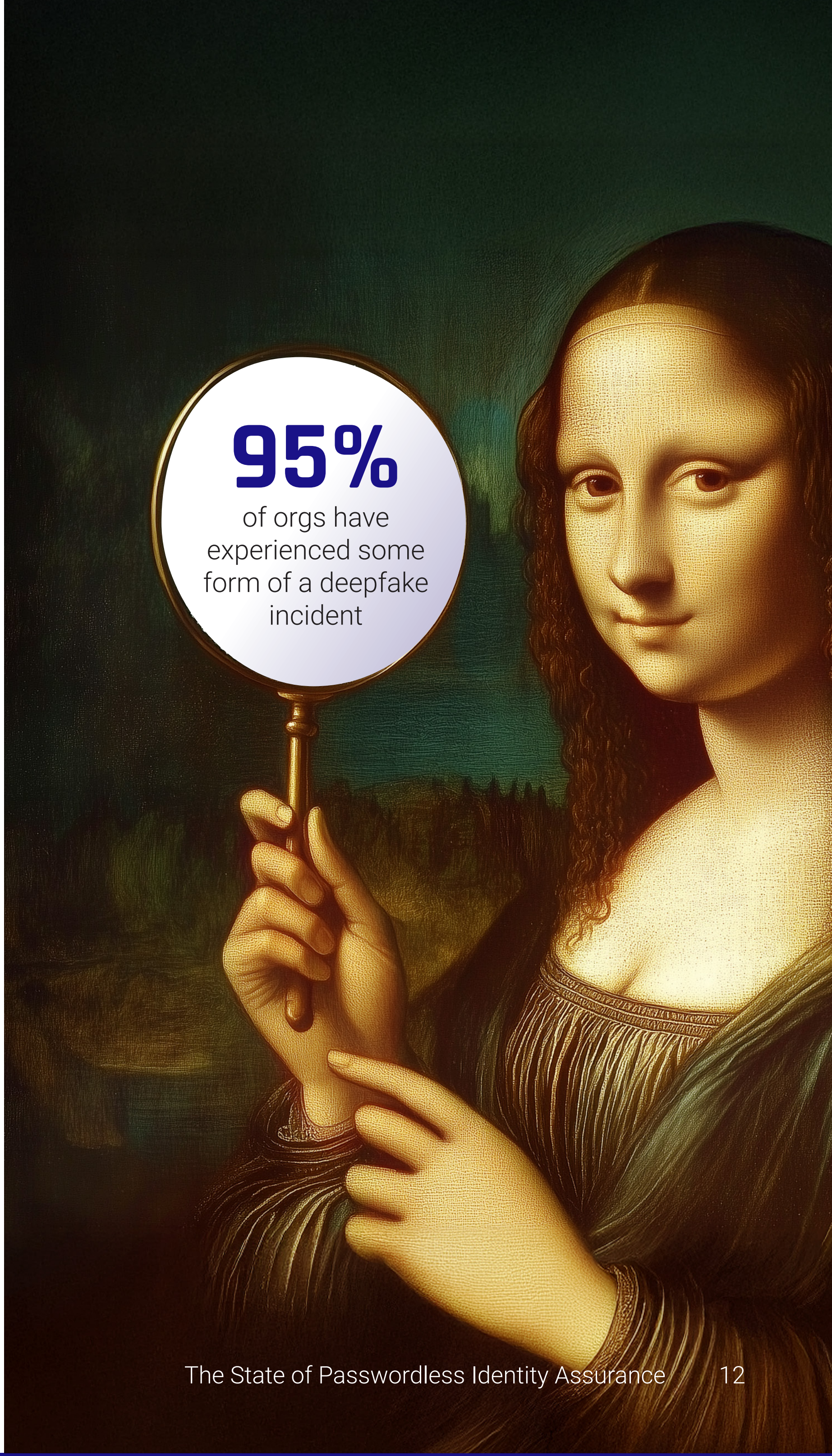


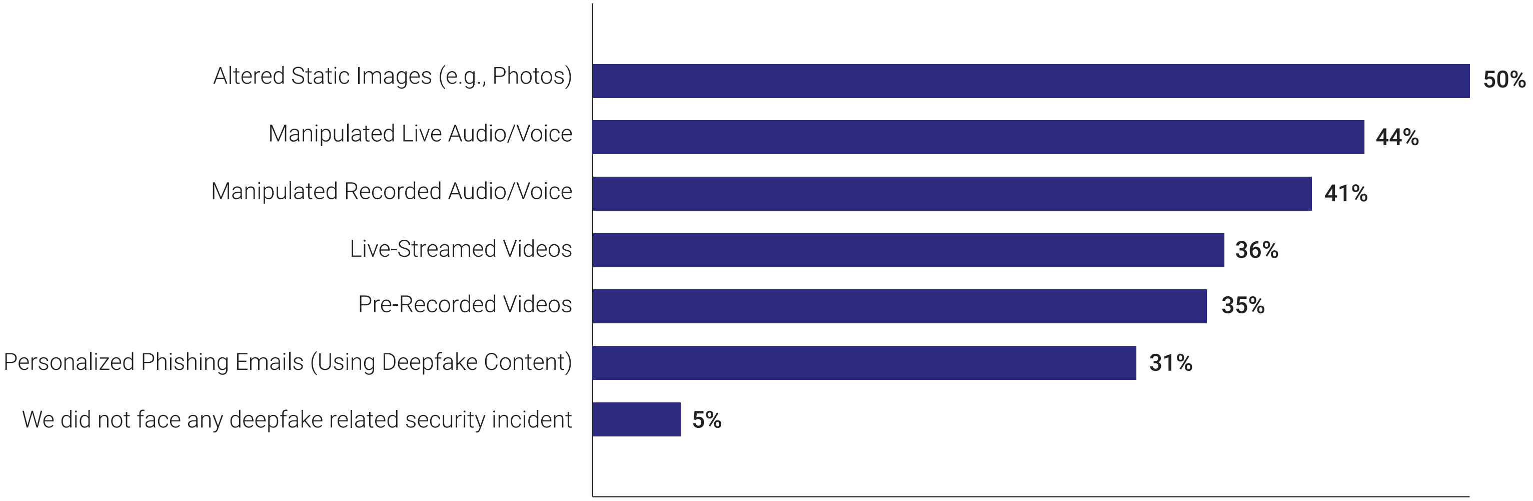
Figure 5. Has your organization experienced any security incidents related to generative AI in the past 12 months?
Base: All respondents (n=756).
Source: S&P Global Market Intelligence 451 Research custom survey commissioned by HYPR.



95%

of orgs have experienced some form of a deepfake incident

Deepfakes Experienced in the Past Year



Passwordless, phishing-resistant authentication on the rise, but market confusion remains an obstacle

Survey data shows that traditional methods of authentication such as password managers (65%) and standard MFA (52%) remain the most widely used, despite being vulnerable to phishing and bypassing, as we discuss below. However, passwordless and FIDO-based authentication methods, which are much more secure, are now in use by nearly half (46%) of respondents. Moreover, for the first time in the five-year history of this report, phishing-resistant authentication methods — such as hardware keys and passwordless (FIDO) passkeys — are projected to be the most widely deployed authentication methods within the next two years.

Further, software-based passwordless/FIDO passkeys are the top-ranked option for authentication methods planned for consumer identity and access management (CIAM) use cases within the next two years. The primary motivations are to reduce fraud (63%) and simplify the user experience (58%), two aspects that are particularly relevant to CIAM purchasers. Account recovery and phishing reduction round out the top choices. User experience is particularly critical in CIAM environments because, unlike employees, customers know that another website, e-commerce site or application is just a mouse click away.

Figure 6. In the past year, which type(s) of deepfake content has your organization experienced?
Base: Respondents whose organizations experienced any security incident related to generative AI in the past 12 months (n=303).
Source: S&P Global Market Intelligence 451 Research custom survey commissioned by HYPR.

CIAM Authentication Methods Currently Deployed Vs. Planned in Next Two Years

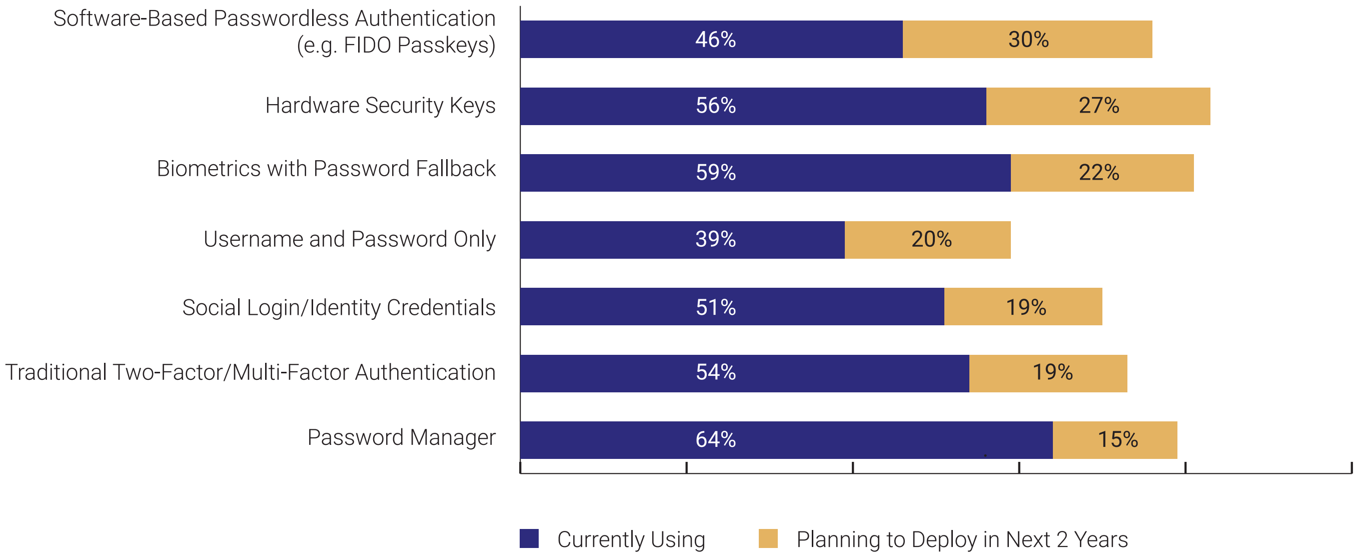


Figure 7. To better understand the consumer identity and access management (CIAM) landscape within your organization, please indicate which authentication methods you currently use for your customers. Select all that apply, noting that different customer interactions may utilize varying methods.
Q. Please indicate which methods of CIAM authentication your organization is planning to deploy within the next two years for your customers. Select all that apply.
Base: Respondents familiar with CIAM (n=736).
Source: S&P Global Market Intelligence 451 Research custom survey commissioned by HYPR.

These increased expectations align with prior survey data from 451 Research, which shows that passwordless authentication is gaining momentum in the enterprise, with usage increasing by 10% compared to the previous year's report.

Biometrics and passwordless multi-factor authentication show largest increases in usage

Authentication Form Factors in Use, 2023 vs. 2024

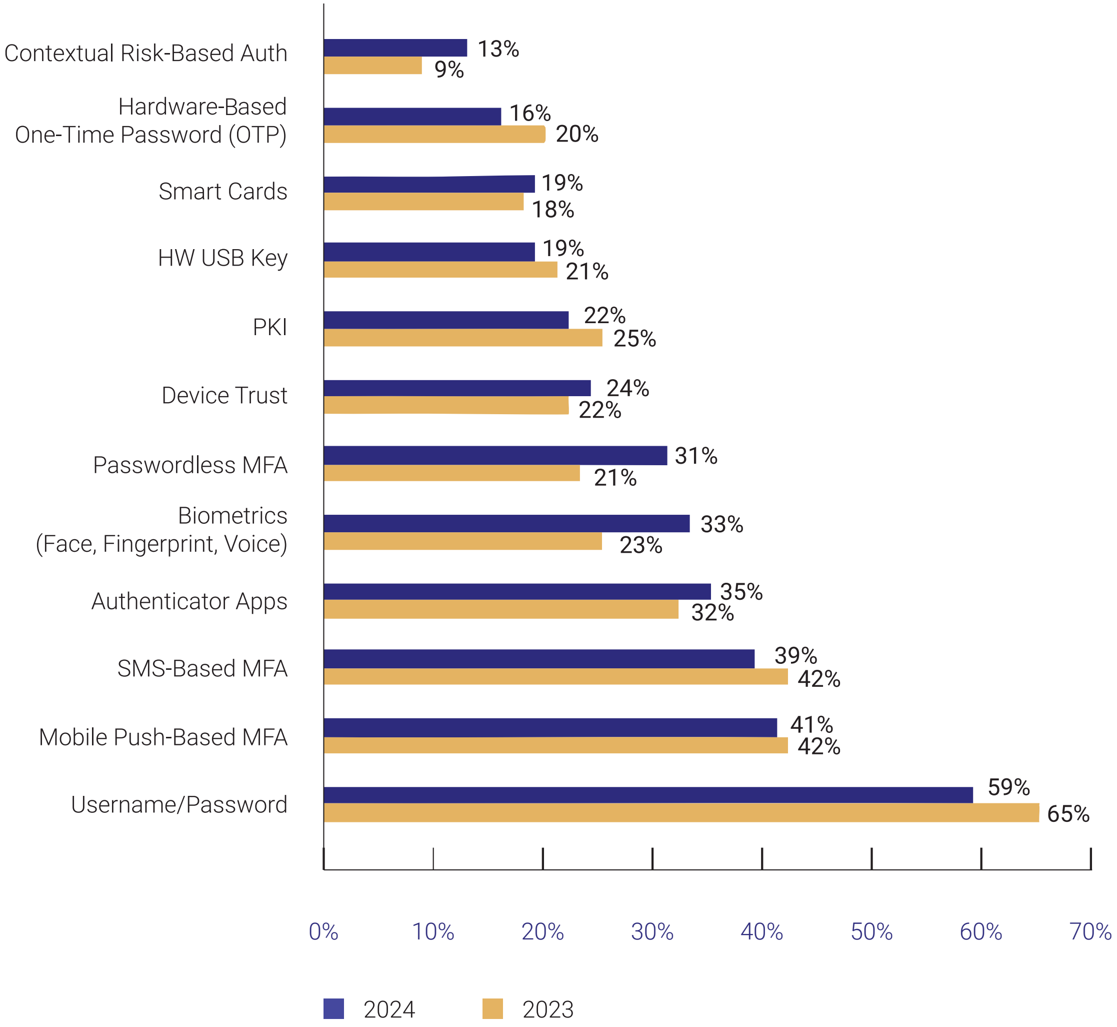


Figure 8. Which of the following authentication form factors does your organization currently use? Please select all that apply.
Base: All respondents, abbreviated fielding: 2023 (n=186); 2024 (n=222).
Source: 451 Research's Voice of the Enterprise: Information Security, Identity Management 2023, 2024.

Despite this, the industry is finding it hard to get rid of passwords completely. While stand-alone username and password methods rank last, 40% of respondents still have systems that rely solely on usernames and passwords. Part of the reason is that many enterprise resources do not yet support MFA or modern authentication protocols. Data from 451 Research's Voice of the Enterprise: Information Security, Identity Management 2024 survey shows that roughly 70% of applications now support MFA, but that leaves nearly one-third of applications unable to use modern and secure authentication.

But perhaps the biggest obstacle to broader adoption of passwordless/FIDO methods is the feeling that existing methods of authentication are "good enough." The issue is not that respondents fail to see the value of modern authentication: When asked about the main reasons why they do NOT deploy passwordless methods, only 12% cited a lack of benefits or business case. The largest proportion of respondents indicated that their existing authentication methods are sufficient (51%), followed by cost and budget concerns (41%) and compatibility with existing IT systems (32%).

One possible explanation is that while firms recognize the limitations of existing authentication methods — and the advantages of newer approaches — they are willing to tolerate some lack of security and inconvenience until they are ready to replace their current methods and newer methods have proven themselves in the field. Breaches can also serve as a catalyst. As noted earlier, roughly half of respondents have changed authentication methods in response to a breach.

Confusion remains about the meaning of 'phishing resistance'

Phishing remains a top security concern for most organizations. Unfortunately, survey responses reflect considerable ongoing confusion about which authentication methods are actually "phishing-resistant" and which are not. This lack of clarity is exacerbated by the absence of a universally agreed upon definition or set of principles. One definition, from the SANS Institute, focuses on removing individual users from the process, and thus their ability to be tricked or "phished."

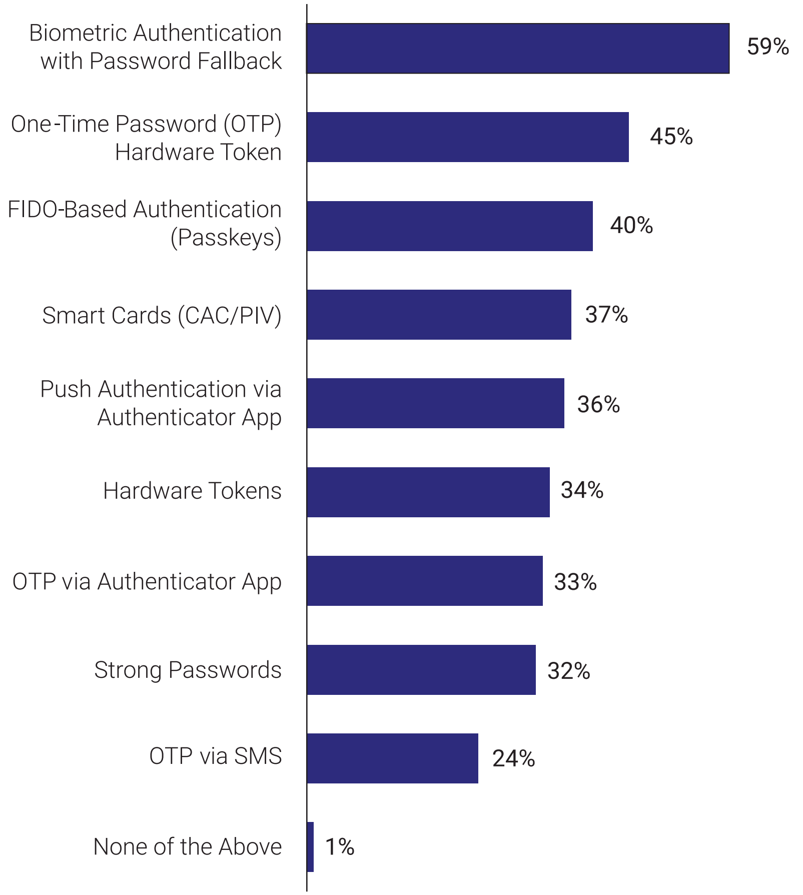
Another way to think of phishing resistance is that it eliminates the exchange of "shared secrets" that may be intercepted by an attacker, such as a password or one-time code. From this perspective, methods such as hardware-based security keys, biometric authenticators (e.g., voice, face or fingerprint recognition) and FIDO-based passkeys are phishing-resistant because they largely eliminate the risk of users compromising a "shared secret" by eliminating the use of secrets themselves. Such methods typically rely instead on public-key cryptography-based certificates and public-private keys.

To illustrate the prevalence of confusion, when respondents were asked to identify "phishing-resistant" authentication methods, the top two responses were biometric authenticators with password fallback (59%) and one-time password (OTP) tokens (45%). While biometric authenticators can be part of phishing-resistant methods, reliance on passwords as a fallback introduces potential for interception.

Similarly, OTP tokens may be intercepted and thus are vulnerable to man-in-the-middle attacks, as are SMS-based codes or push notification apps. FIDO-based passkeys (40%) are third on the list, despite obvious security and user experience benefits relative to the prior choices. FIDO passkeys rely on public and private keys rather than any shared secret and are thus not "phishable." Additionally, smart cards (37%), which are also phishing-resistant because they typically rely on public-key cryptography and public-private keys, barely edged out push notification apps (36%), which are vulnerable to such attacks. In short, the industry must educate end users and decision-makers and promote the advantages of phishing-resistant technologies, both in the workforce and in consumer arenas.

> ...phishing resistance eliminates the exchange of "shared secrets"...

Authentication methods that respondents identify as 'phishing-resistant'



Understandably, the main reason organizations seek to adopt passwordless or FIDO-based authenticators is to prevent password-based attacks (68%), as well as enhance security during device registration (58%) and reduce fraud (52%). A lesser-known benefit of phishing-resistant MFA is that it can also reduce the need for security awareness training. Nearly half of respondents (44%) undertook security awareness training in response to a breach.

Figure 9. Which of the following forms of authentication do you consider to be "phishing-resistant"?
Base: All respondents (n=756).
Source: S&P Global Market Intelligence 451 Research custom survey commissioned by HYPR.

68% of organizations are looking to prevent password-based attacks

However, **32%** still think "strong passwords" are phishing-resistant

For CIAM use cases specifically, reducing fraud (63%) is the top reason to adopt passwordless or FIDO-based authenticators. Other drivers include simplifying the user experience (58%), account recovery (55%) and reducing phishing (52%). Rather unexpectedly, less than one-third (31%) of respondents cite reducing helpdesk costs, which ranks near the bottom, despite years of helpdesk costs being cited as a key concern in adopting MFA and a factor in the continued reliance on passwords. It is also worth noting that the percentage of helpdesk costs attributed to password resets is only about 13% on average, despite being one of the more labor-intensive helpdesk tasks. One plausible explanation is that the costs incurred by helpdesks are often not borne by the security and IAM personnel targeted in this survey, particularly if those initiatives are the purview of broader IT operations teams.

As an aside, there has historically been no single authenticator that can account for all use cases and user preferences. This has led to a trade-off between ease of use and security for most authenticators: Those that are easiest to use and that pose the least user friction tend to be less secure, while those that are more secure tend to be less user-friendly. One of the prime benefits of passwordless authentication is the ability to eliminate this trade-off and provide the best of both worlds — strong security and a seamless user experience. However, a range of authenticators meet the requirements for phishing-resistance, and this is reflected in our results.

> ...reducing fraud (63%) is the top reason to adopt passwordless or FIDO-based authenticators...

Top 3 Reasons to Adopt Passwordless for CIAM

63% reduce fraud

58% improve UX

55% reduce phishing

Toward Identity-First Security

3

Identity verification is widely deployed, particularly after a breach, but still misunderstood

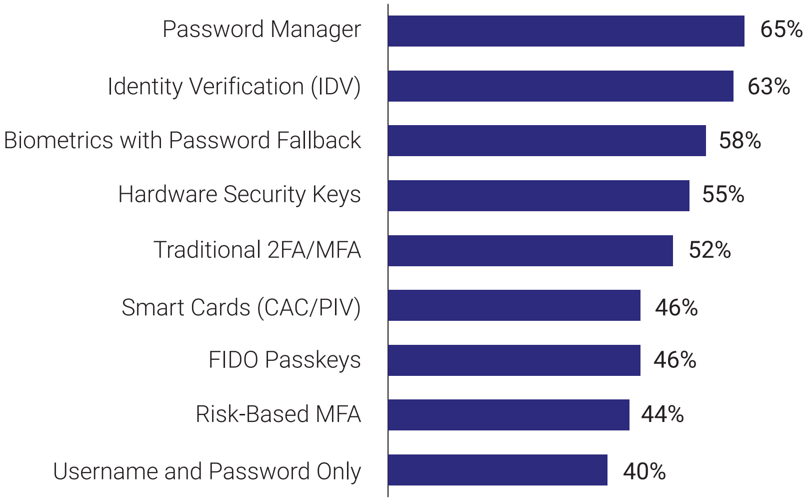
Identity verification methods complement authentication systems by verifying that a person is who they say they are, and not a fraudster or bot. There are various IDV tools and techniques, but the most common by far are traditional, manual methods such as in-person office visits. Other IDV techniques include document verification (driver's license, passport), device verification (phone number via SMS, synced passkey), background checks and location checks (geolocation, IP location, address on file). Newer techniques include selfie checks, text and video chat, biometric facial recognition, and manager attestation. IDV can also include "liveness" checks to guard against deepfakes during the registration or onboarding process.

Identity verification (63%) is one of the most widely deployed IAM tools in our survey, trailing only password managers (65%), and ahead of biometrics (58%). However, this is likely due to a high number of respondents relying on "traditional" IDV techniques such as in-person office visits that are particularly ill-suited for remote and hybrid work strategies. IDV is also identified as a common response to cyberattacks: It is the top tool organizations have implemented after experiencing a breach (68%).

68%

of organizations implement an IDV tool after a breach

Workforce Identity Security Technologies Currently Deployed



Some of the top reasons for deploying IDV include more secure account recovery and password reset (57%), preventing deepfakes and impersonation (53%) and secure device registration (51%). Efficiency is also a key driver of IDV deployments: Half of respondents note the need for faster account recovery and credential resets, in addition to more security. It follows that most organizations plan to increase their budget for IDV in the coming year.

While these are positive indicators, our data suggests the industry remains too reliant on traditional IDV methods such as office visits and document-based authentication, which are inefficient and insecure. Physical office visit (72%) is the top cited IDV method for workers joining an organization, followed distantly by document authentication (48%) and biometrics (43%). The top IDV method for credential reset is knowledge-based authentication/security questions (45%), though biometrics (42%) and passkeys (40%) are close behind. Physical office visits are also the most common method for device replacement (37%). This presents significant security issues because outdated, stand-alone methods remain a key vector for attackers to establish seemingly legitimate accounts or credentials — a tactic that would be more difficult with modern IDV methods that combine multiple signals or data points, such as documentation plus location, or SMS backed up by audio or video.

Additionally, each of these processes receives relatively low marks for efficiency. When asked which processes are "highly efficient," just 33% cite credential resets, 30% cite device replacement and 29% cite joining the organization.

Most organizations may be aware that current, manual methods of IDV are insufficient, but compatibility concerns and budget constraints are hindering implementation of modern methods. Indeed, our survey data shows that compatibility concerns with existing IT (39%) and cost/budget (35%) are the top reasons given by respondents for not deploying IDV, while lack of clear benefit/business case (28%) is third. It is worth noting that this is more than double the percentage citing lack of clear benefit as a barrier to deploying passwordless authentication (12%), suggesting the IDV industry has work to do to convince potential buyers of its benefits.

Figure 10. To better understand the identity security landscape within your organization, please indicate which identity security technologies are currently deployed across your various applications for your workforce. Select all that apply.
Base: All respondents (n=756).
Source: S&P Global Market Intelligence 451 Research custom survey commissioned by HYPR.

Conclusion

Identity-based breaches remain a large and growing part of the modern IT experience.

Part of the explanation is that older methods of authentication and identity verification remain a big part of the identity management picture in many firms. The good news is that most organizations have an eye to the future and are looking to adopt new, phishing-resistant approaches such as passkeys and modern IDV solutions that promise the "holy grail" of identity — a combination of vastly improved security and better user experience. A potential catalyst is that half of organizations view breaches as an opportunity to update their authentication methods.

The challenge for many organizations, therefore, is to make the most of existing investments while moving toward new approaches to avoid falling behind and remaining vulnerable to attacks. As the findings in this report illustrate, organizations that embrace new methods of authentication and identity verification are less likely to experience identity breach than those that lag.

Methodology

The online survey collected data from 750 global IT security decision-makers, specifically targeting those in managerial positions or higher, who are engaged in the identity life cycle and security measures. Conducted in January 2025, the global survey included respondents from the US, UK, France, Germany, Australia/New Zealand, Japan and Singapore, ensuring diverse geographic representation. The sample comprised a mix of private and public sector companies across multiple industries, including financial services, manufacturing and healthcare, focusing on organizations with 250 or more employees. Respondents were screened based on their responsibilities related to identity verification and security to ensure relevant insights into passwordless authentication practices.

About the Author

Garrett Bekker is a principal research analyst at S&P Global Market Intelligence 451 Research, leading the identity and access management (IAM) vertical within the Information Security channel. Prior to his coverage of IAM and cloud security, Garrett also covered data security and governance, risk and compliance. Within IAM, Garrett's current research specializations include passwordless authentication, cloud-native authorization, privileged access management and identity threat detection and response.

He arrived at S&P Global Market Intelligence through its 2019 acquisition of 451 Research, which he joined in 2014. Garrett has viewed security from a variety of perspectives over the past 25 years. He started his career in security as an equity research analyst at several investment banking firms, most recently Merrill Lynch, where he covered information security, infrastructure software and networking companies. Garrett has also worked with early-stage enterprise security vendors, including Bat Blue (acquired by OPAQ Networks), in sales and marketing roles.

Garrett holds a bachelor's degree in international studies from the University of Buffalo. He has completed all coursework for a doctorate in economics from The New School in New York. He also completed undergraduate studies at McGill University in Montreal, and graduate work at Cambridge University in the UK.

About HYPR

HYPR, the leader in passwordless identity assurance, delivers the industry's most comprehensive end-to-end identity security for your workforce and customers.

By unifying phishing-resistant passwordless authentication, adaptive risk mitigation, and automated identity verification, HYPR ensures secure and seamless user experiences for everyone.

Trusted by organizations worldwide, including two of the four largest US banks, leading manufacturers, and critical infrastructure companies, HYPR secures some of the most complex and demanding environments globally, showcasing our commitment to innovation and security excellence. Visit: **hypr.com/get-a-demo**

HYPR

S&P Global
Market Intelligence