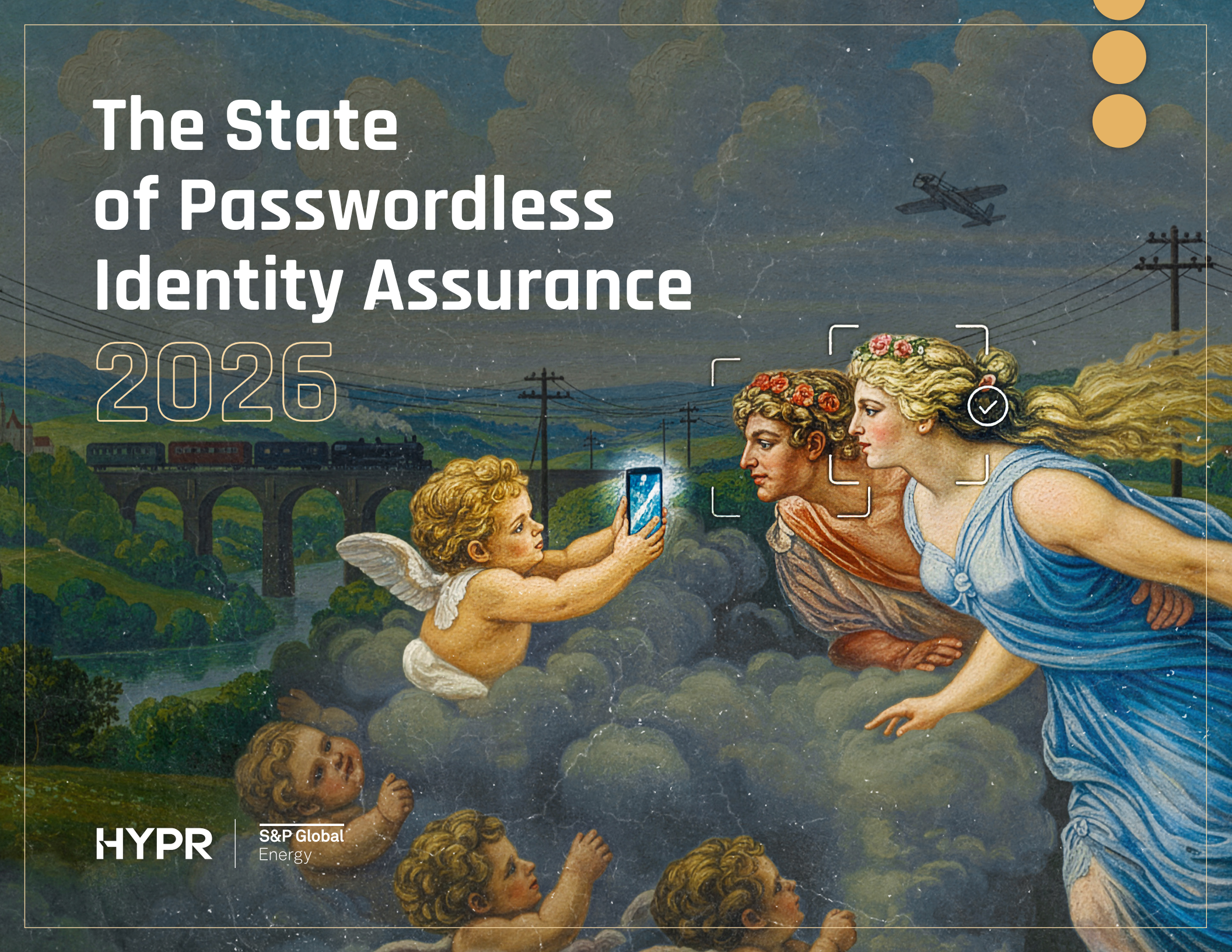
The State of Passwordless Identity Assurance 2026



HYPR | S&P Global Energy

Foreword

The Age of Industrialization

History rarely moves in straight lines. We tend to romanticize transformational eras by their singular breakthroughs: the lightning-bolt inventions that redefine the possible. But the more nuanced reality is, the slower, messier, and far more deliberate is the work of shaping innovation into systems that can scale.

The steam engine and the mechanized loom arrived in bursts of genius, but it took decades to architect the factory systems, safety standards, and global supply chains that made them world-altering. Innovation makes change imaginable; industrialization makes it real.
Identity is at that inflection point today.

Last year, we described an Identity Renaissance: a fundamental pivot away from the shared secrets and outdated authentication models of the past, and toward a more accurate understanding of identity as assurance of the person, not just the credential. The data provided the cutting criticism we needed: Identity vulnerabilities are driving the majority of breaches. Phishing-resistant authentication is more effective than traditional MFA. Attackers aren't breaking in; they're logging in.

Over the past year, our industry has moved from recognition to understanding. Security and identity leaders became more precise about what phishing resistance means. You evaluated passkeys, hardware-backed authentication, and identity verification with greater technical clarity. You mapped workflows and challenged legacy assumptions. And then, to the outside observer, progress appeared to slow.

That pause is not a retreat; it is a transition into the high-stakes work of industrial-grade execution. Identity is not a stand-alone control to be deployed once or optimized for a single use case. It is the connective tissue of the enterprise, spanning onboarding to account recovery, cloud infrastructure to help desk. It crosses the silos of HR, IT and Security.
As a security leader, you know that scaling identity without discipline risks replacing one kind of fragility with another.

We have entered the Age of Industrialization.
This is where innovation is tested by reality. Industrialization demands:

Intuitive User Experience: Moving beyond the pilot to a repeatable system that prioritizes the user across all workflow paths.

Governance: Integrating identity with HR, IT, Legal, and Security, allowing the system to react naturally and in real time.

Operational Efficiency: Surfacing the legacy dependencies and organizational seams that keep overhead and maintenance costs from exposing a brittle system.

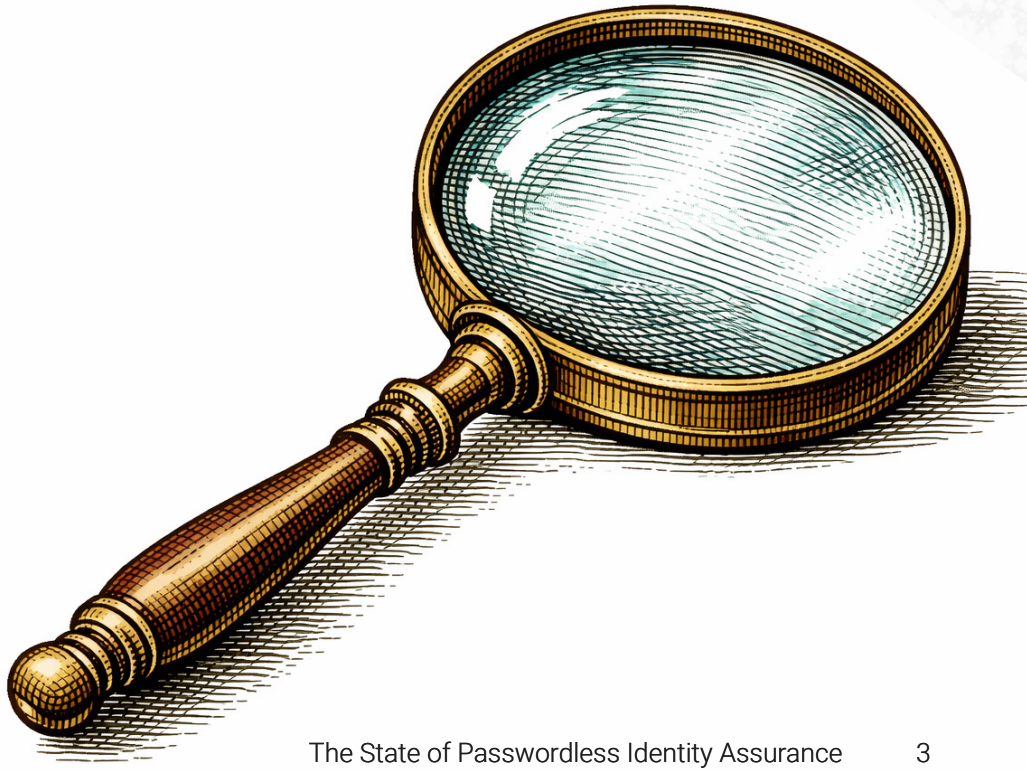
The lesson from history is clear: Breakthroughs ignite change, but systems are what sustain it. Today's most resilient enterprises are acting on that lesson. They are slowing down to understand their full set of use cases. They are aligning teams that have historically operated separately. They are designing identity programs meant to scale correctly, not just quickly. The urgency remains blazing. AI-driven phishing, vishing and deepfakes are accelerating identity abuse at an alarming speed. Partial solutions and rushed, fragmented rollouts no longer provide meaningful protection.

This year's ***State of Passwordless Identity Assurance*** report reflects this shift. It captures an industry that has had its breakthroughs and is now doing the harder work of turning insight into real change.
The Renaissance brought awareness. The Enlightenment brought understanding.

Industrialization is where we finally win at scale.

Bojan Simic
HYPR CEO

Contents



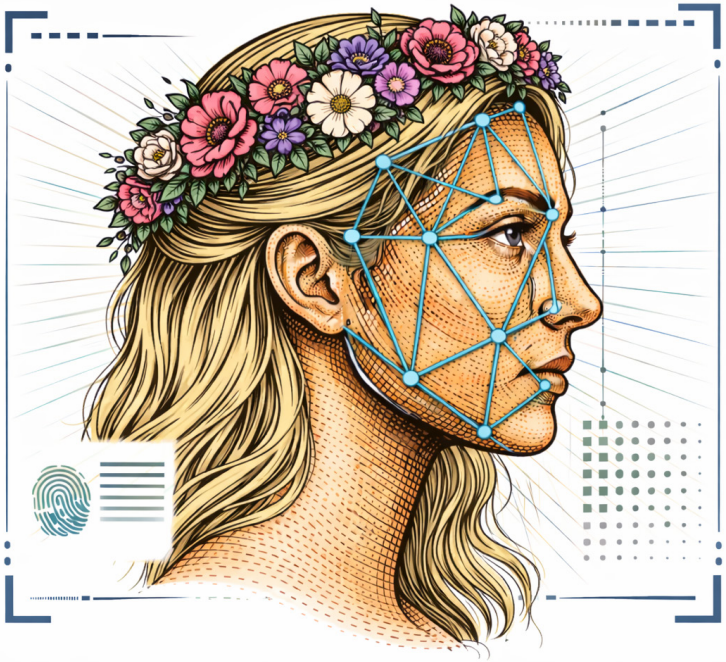
Introduction

The State of Passwordless Identity Assurance

The sixth annual State of Passwordless Identity Assurance report, commissioned by HYPR and produced by 451 Research from S&P Global Energy Horizons, demonstrates organizations are moving from identity awareness to understanding, but have not yet achieved broad, enterprise-wide execution.

Organizations have gained a clearer view of identity threats, phishing-resistant authentication and the importance of identity verification. However, the surge in adoption noted in our prior survey has stalled as early-adopter enthusiasm has waned. Deployments have also largely targeted specific use cases and user personas rather than being company-wide, and the same trend largely applies to identity verification (IDV). There are a host of potential reasons for this, including cost, compatibility, internal budget dynamics, deployment complexity, regulatory concerns and, most of all, a growing recognition of the requirements for enterprise-scale identity transformation.

Bridging this gap between awareness and execution marks the transition into the next chapter. We are entering the "Age of Industrialization," where the insights gained during identity's "Age of Enlightenment" are finally put into practice. The goal is to operationalize identity security at scale. This requires moving beyond the simple login to securing every touchpoint where identity is involved, from hiring and onboarding to sensitive application access, account recovery, device replacement and help desk interactions. The industry has moved past the "discovery" phase; enterprises no longer question what works but must now focus on universal execution and broader integration across the entire organizational structure.



Key Findings

AI-driven attacks are the top security concern

Generative AI and agentic AI have become the top identity security concerns. They are not only rearming existing threats such as phishing and ransomware but also creating new attacks, including deepfakes and employee impersonation fraud.

Passwordless adoption — more clarity but less action

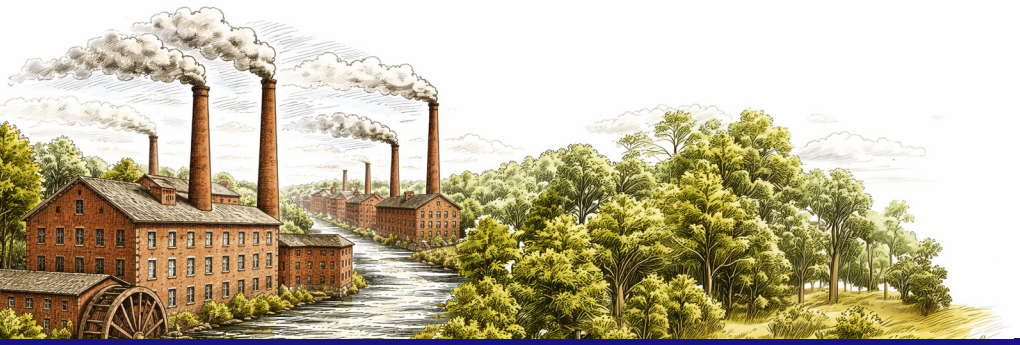
Respondents notably demonstrated increased clarity about the precise meaning of phishing-resistant and passwordless authentication methods compared to the 2025 study. Yet this understanding hasn't directly translated into action; the spike in passwordless adoption observed in last year's survey has plateaued.

Bridging the gap from pilot to production is critical

Though passwordless adoption has stalled, plans remain positive. Respondents have more pilot projects for passwordless authentication than for any other method, and a large percentage still plan to deploy passwordless tools within the next two years.

Identity verification is a "must-have," but usage is still fragmented

IDV is the second most-deployed identity management tool and a key response to breaches. However, IDV is still primarily used for a narrow range of internal use cases and user personas.



AI has generated a new industrial ecosystem of identity-based attacks

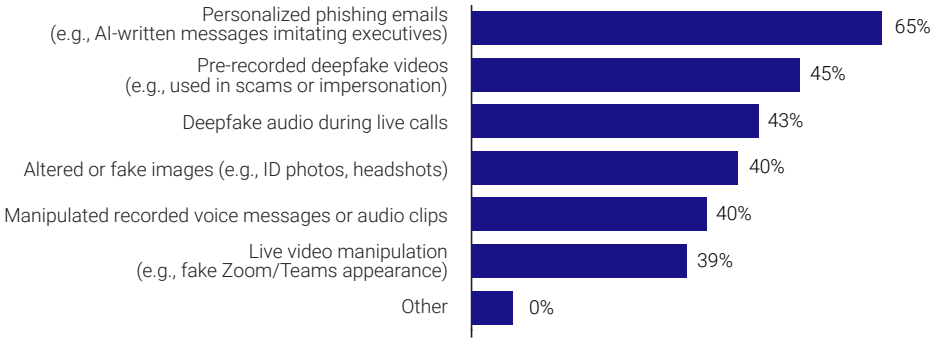
While cybersecurity investments have steadily increased, the breach trajectory continues to steepen — a paradox driven by the fact that identity remains the primary vector for modern attacks. Generative and agentic AI offer unprecedented efficiency in automating identity governance while simultaneously enabling adversaries to execute sophisticated, identity-based attacks at a velocity and scale that threatens to outpace manual defenses and reactive risk-detection measures.

It is no surprise that this year's survey results reflect a significant shift in the threat hierarchy. For the first time in report history, generative AI (53%) and agentic AI (45%) have emerged as the top identity-specific security concerns — displacing stolen or compromised credentials (38%) from its spot as the top identity security challenge.

For the first time in report history AI-driven attacks have emerged as the top identity security concern.

These concerns are well-founded: 43% of respondents identified AI-driven tactics as the most significant change in the attack landscape over the last year. Notably, nearly 40% of organizations report having experienced a GenAI-related security incident in the past 12 months. Among the 40% of respondents impacted by AI-based attacks, personalized phishing was the dominant identity risk, cited by nearly two-thirds of respondents (65%).

You indicated your organization experienced AI-generated or AI-enhanced attacks. What type(s) of AI-generated or AI-enhanced content has your organization encountered in the incident(s)?



Source: S&P Global Market Intelligence 451 Research custom survey commissioned by HYPR.

Synthetic media has emerged as a top-tier threat, with deepfakes registering concern across multiple formats including prerecorded videos (45%), live audio (43%) and the manipulation of live video such as Zoom calls (39%). Other AI-based identity attacks included altered or fake images or photos (40%) and manipulated voice messages or audio clips, such as voice cloning (voice phishing or "vishing") (40%). Voice cloning is a new and increasingly common AI-based technique that creates a synthetic version of a person's voice from audio samples that can be combined to form completely new sentences. This technique has been used to aggressively target help desks and call centers, as evidenced by the rise of Scattered Spider and Shiny Hunter threat groups.

Additional high-profile examples of voice cloning include a fraudulent Zoom meeting involving deepfake participants in Singapore and the cloning of the Italian Defense Minister's voice to make fake calls to several business executives. Overall, 87% of respondents experienced some form of deepfake as part of an AI-based attack, either audio (43%) or prerecorded video (45%).

AI, phishing and ransomware: A new force multiplier

Beyond stand-alone AI attacks, generative AI and agentic AI are industrializing traditional vectors such as phishing and ransomware. As a result, both the volume and efficiency of these attacks are increasing substantially. Phishing (43%) remains the most common type of cyberattack organizations have faced in the past 12 months, followed by malware and ransomware (37%). These are followed closely by AI-generated attacks (36%) and identity impersonation (35%, up from 30% last year). These findings highlight why AI has become the dominant identity security concern: It is not replacing existing attack vectors such as phishing and ransomware, but amplifying them — dramatically increasing their scale, speed and effectiveness.

Nearly

9 of 10

organizations that had an AI-based attack experienced an audio or video deepfake

Fears of fraudulent hires are real: Security responsibility is fragmented

Credential misuse, such as shared or stolen logins, continues to dominate the headlines and was the most prevalent type of identity-impersonation incident by a wide margin (54%). However, employee and candidate fraud has surged to become the second biggest concern (39%), while deepfake-generated audio and video (37%) tied with privileged account takeover (37%) to round out the top three.

The shift toward hybrid and remote work has created verification blind spots, resulting in a security vacuum that AI-armed attackers are aggressively exploiting. Nearly three-quarters of respondents reported at least moderate concern regarding fraudulent candidates, with nearly one-third identifying as "very concerned."

The hindsight tax: Why reactive spending and fragmented ownership hinders resilience

While cost remains a top adoption barrier for both passwordless MFA and IDV deployments, breaches paradoxically clarify the value of security. Our survey reveals a common, yet reactive, spending pattern: Increased budget and investment (59%) was the most common response to a breach, outpacing comprehensive audit (51%), security awareness training (49%) and a shift toward stronger authentication methods (48%).

The shift is a direct, albeit late, attempt to mitigate the quantifiable business impact of an attack — specifically business disruptions (39%), data loss (34%) and reputational damage (29%) — all of which carry costs far exceeding the initial price of defensive tools. However, this reliance on "panic buying" often indicates an immature identity security posture. When forced to react, organizations prioritize rapid deployment of IDV (61%), MFA (57%), and identity threat detection and response (52%) to address the failure points identified during a breach.

While these tools are effective — as evidenced by specialized software that can quickly discover most identity-related breaches — the efficiency of these investments is often undermined by a persistent ownership gap. Although identity security is rapidly becoming a board-level issue, its operational responsibility remains fragmented across HR, IT, cloud infrastructure, risk and security teams. This structural hurdle is a fundamental barrier to broader enterprise adoption, causing misalignment and challenges in resource and budgeting allocations. This is particularly evident in the lack of consensus on ownership of emerging threats. Respondents were divided on whether the responsibility for mitigating the risk of fraudulent hires lies with information security (31%), identity and access management (IAM) teams (24%) or IT (18%). Without a unified ownership model, organizations remain trapped in a cycle of reactive spending rather than proactive resilience.

Breach triggers budget:

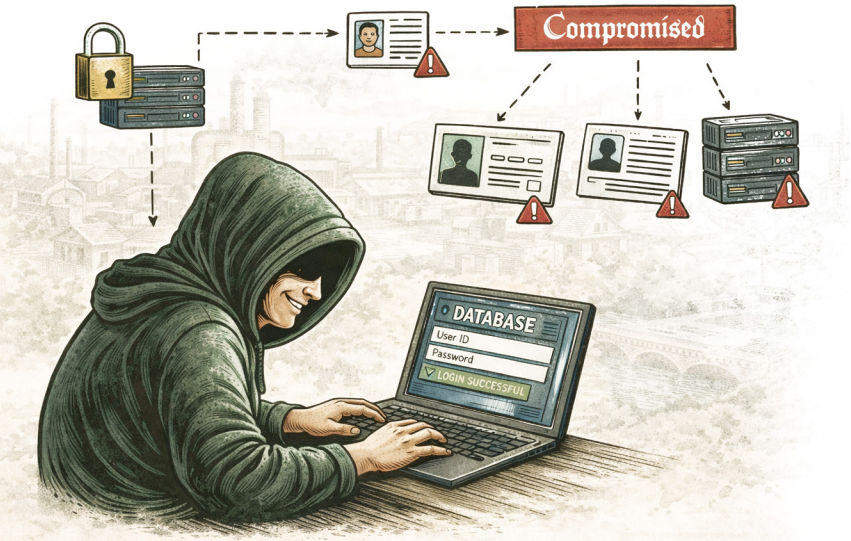
Almost 60%

spend on IDV and MFA only after impact.

Detection velocity: Debunking the dwell-time myth

Despite persistent myths about lengthy dwell times, modern defensive frameworks are proving highly effective at identifying threats in near-real time. The survey indicates that 65% of recent identity-based or AI attacks have been detected within a few hours, including 28% that were flagged immediately. Fewer than 10% took a week or more to detect. Most attacks (53%) were detected via third-party security tools such as IAM, security information and event management, or endpoint detection and response tools. Human-driven identification accounted for the remainder: Employees flagged 22% of incidents, while audits (15%) and external reports from customers or third parties (10%) rounded out the list.

However, as with any technological advancement, the benefits are available to both attackers and defenders. Thus, improved capabilities for detecting and responding to AI-based threats have been largely offset by a corresponding boost in attack efficiency. Detection times may be improving, but attackers can still steal credentials, establish persistence and begin data access faster than most response processes can meaningfully intervene, making reduced exfiltration windows largely ineffective.



The education barrier: Why conceptual ambiguity slows phishing-resistant adoption

The 2025 State of Passwordless Identity Assurance report highlighted widespread ambiguity regarding the technical definition of phishing resistance. At the time, organizations struggled to distinguish between compliant authentication methods and legacy MFA methods vulnerable to phishing and other methods of intercepting "secrets." Some of the confusion stems from multiple definitions of both passwordless authentication and phishing resistance proposed by vendors and industry bodies such as The FIDO Alliance and the SANS Institute.

This year's findings mark a significant breakthrough, with respondents demonstrating a clearer understanding of phishing resistance and passwordless authentication. For the first time, FIDO passkeys emerged as the most widely identified phishing-resistant authentication method, at 64%, a significant increase from 40% in 2025. Similarly, hardware keys (e.g., YubiKeys and other USB keys) rose sharply to 54% from 34%, while smartcards increased by roughly 15 percentage points, from 37% in 2025 to 52% in this year's survey. This clarity is imperative to operationalizing identity assurance because without technical assurance, broader adoption seems theoretical.

Nearly

One-Third

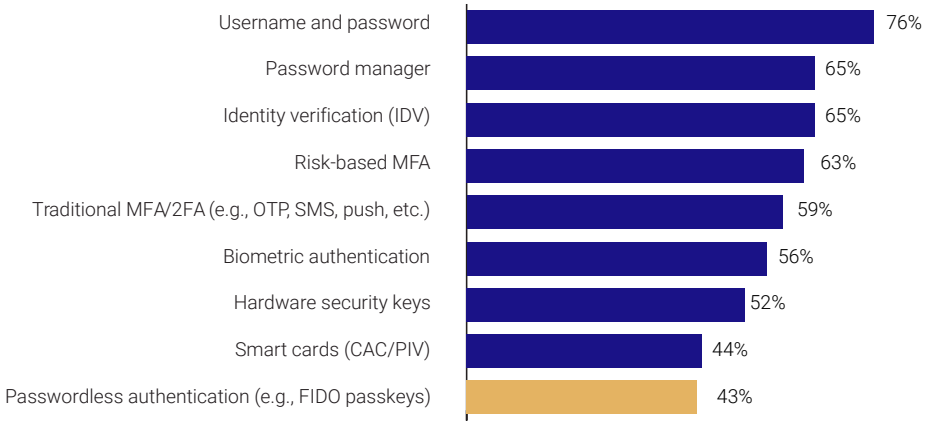
of respondents have passwordless pilot projects running, more than any other authentication method.

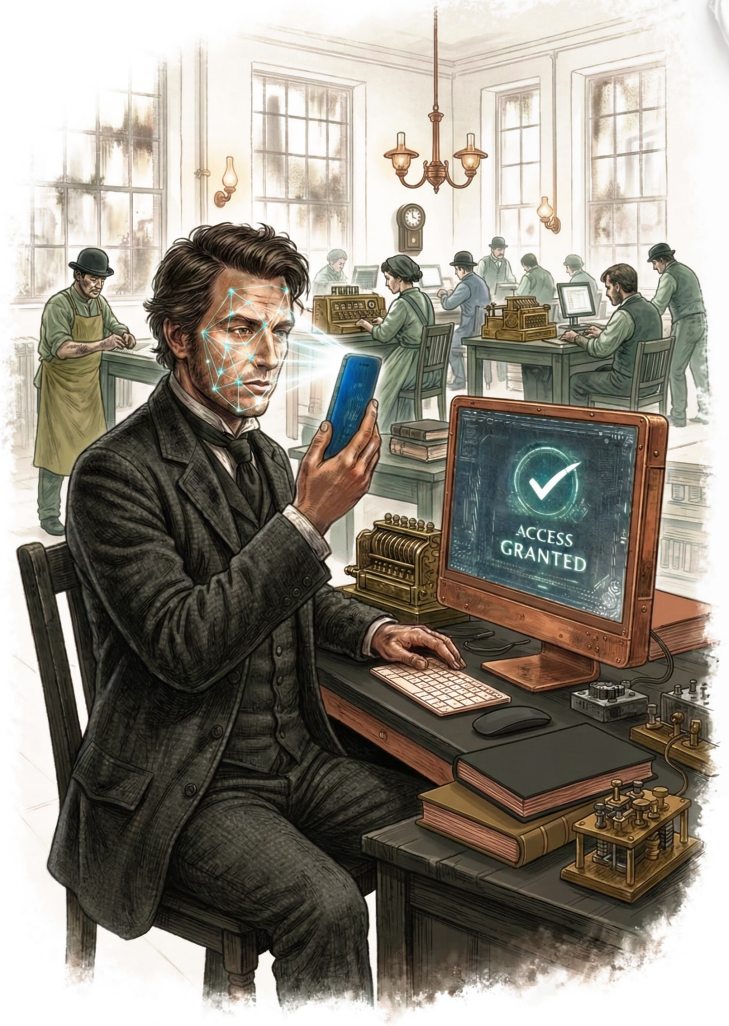
From pilot to adoption: Solving for infrastructure, legacy and scale

Despite increased market literacy, the momentum of passwordless adoption has encountered a strategic plateau, as usernames and passwords remain the dominant authentication method for 76% of respondents. By comparison, enterprise use of passwordless authentication remains low on the adoption curve, cited by just 43% of respondents. A similar slowdown in adoption was evident in 451 Research's Voice of the Enterprise survey data, which indicated that 30% of respondents have deployed passwordless authentication, essentially flat year over year from the prior survey.

The critical question is whether this is merely a temporary "blip" or a symptom of a more systemic issue. Technology adoption cycles are typically nonlinear, and authentication is no exception. As noted in Geoffrey Moore's book Crossing the Chasm, most IT innovations follow a familiar adoption pattern with five distinct segments. The "chasm" refers to the period of discontinuity between early adopters and early majority buyers. Viewed through this historical lens, the flat year-over-year growth observed in this year's results could simply be a temporary breather, representing a single data point on the path toward more mainstream adoption of passwordless authentication as the dominant method.

Please indicate the deployment status of the following technologies within your organization.





Interestingly,

65%

of enterprises indicate using IDV.

Yet implementation remains siloed, with most deploying to

less than 25%

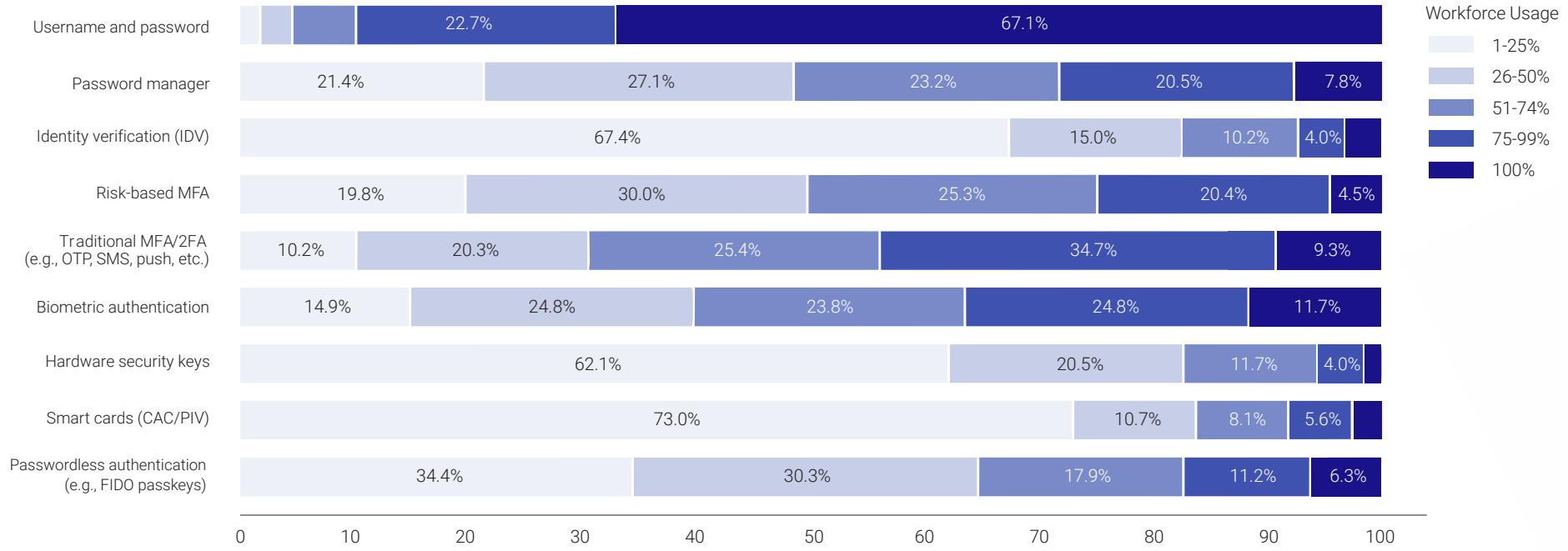
of their workforce...

Security tools like passwordless authentication and IDV are narrowly deployed, trapped in 'persona-based' and use case silos.

Many factors may contribute to this phenomenon. One is the initial excitement among early adopters who are willing to accept imperfections and friction as "bugs" are worked out in exchange for "first mover" competitive advantage. Conversely, many firms are more risk-averse and prefer to wait for products to mature before investing substantial time and money. Other constraints include the maturation of technology standards and the development of supporting infrastructure.

Regarding passwordless authentication specifically, this year's pause in adoption could also be a function of infrastructure lag — the need to wait for all systems to technically support passkeys and other forms of passwordless or phishing-resistant authentication. For example, many websites, apps and devices still do not support passwordless protocols such as FIDO2 and WebAuthN. The lack of support for legacy apps is a significant barrier to adoption, cited by nearly one-third (32%) of respondents.

Workforce Deployment Levels Aross Security Technologies

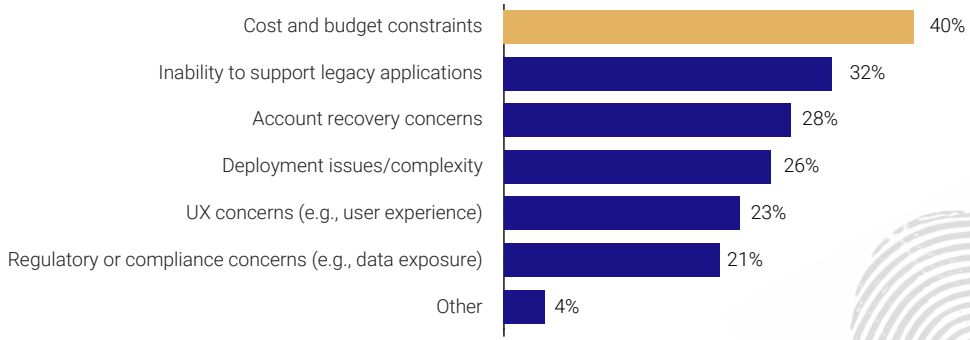


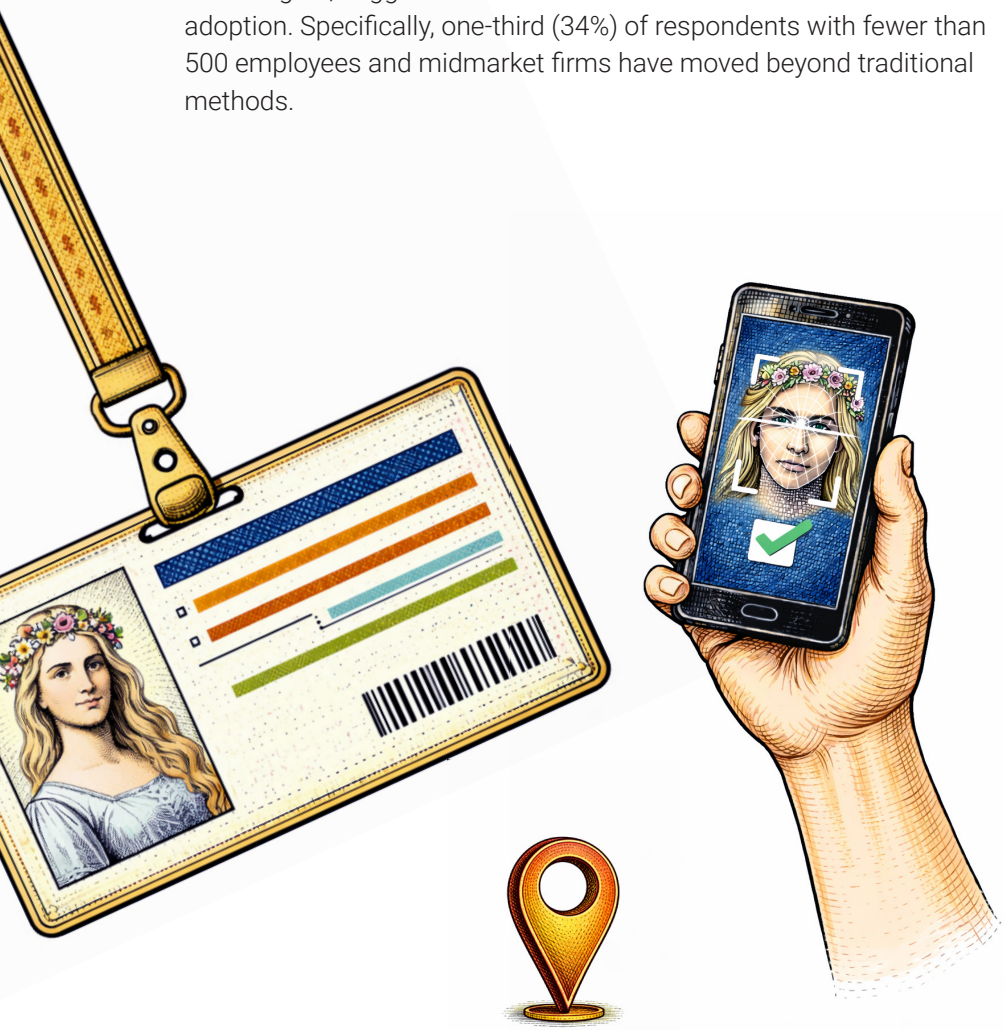
Ordered by workforce deployment status as seen on previous page

Consistent with broader cybersecurity trends, financial constraints (40%) emerged as the top deterrent to passwordless adoption. Notably, user experience is now less of a concern, identified by only 23%. This indicates that the usability gap is closing, and that the greater challenge is no longer convincing users but obtaining the necessary budget.

Another potential factor is the maturity of internal passwordless authentication programs, which can be linked to organizational scale. Our data shows a direct correlation between firm size and the transition to passwordless authentication. Low adoption rates among small and midsize businesses, which typically have smaller IT staff and budgets, suggest that internal resources are crucial for broader adoption. Specifically, one-third (34%) of respondents with fewer than 500 employees and midmarket firms have moved beyond traditional methods.

What has prevented your organization from deploying passwordless authentication for your workforce?





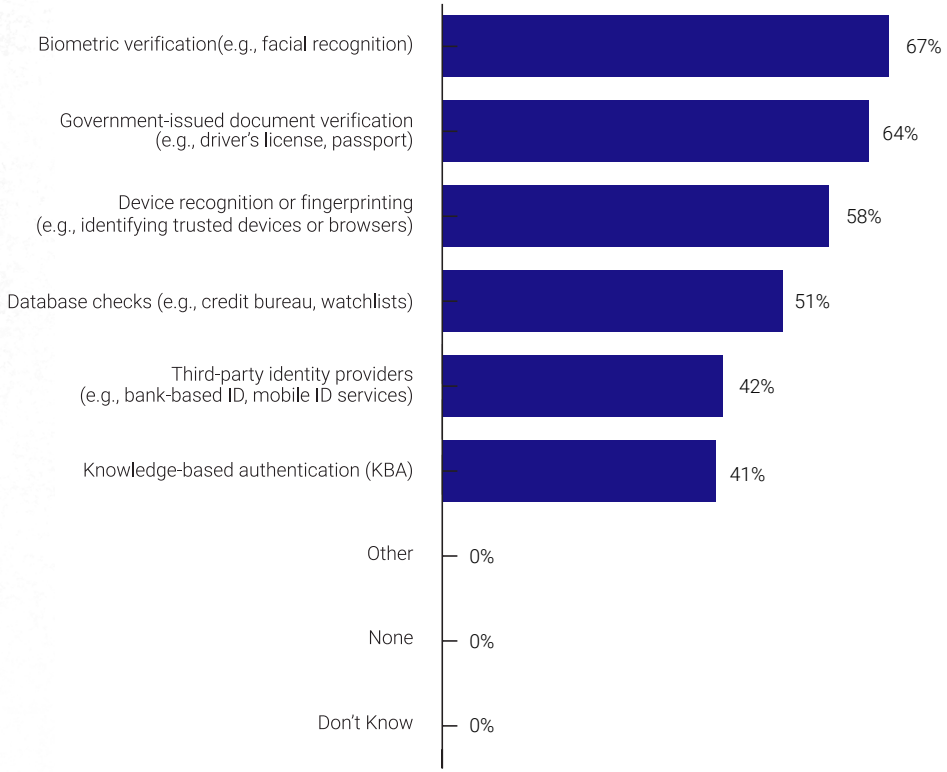
The pipeline for change: Pilots and future commitments

While current deployment figures show a temporary stall, plans and pipelines for passwordless implementation remain more encouraging. Nearly one-third of respondents have passwordless pilot projects underway, the highest among all authentication methods. With 43% already deploying passwordless authentication and another 28% committing to a rollout in the next two years, the data suggests that investment in passwordless technology is a strategic, multiyear project requiring lengthy planning across teams. The momentum is further validated, as nearly three-quarters are either “very likely” or “extremely likely” to invest in passwordless tools or passkeys in 2026. The top reasons include preventing password-based attacks (70%), enhancing device registration (60%), preventing fraud (54%) and simplifying the login experience (52%).

The rise of identity verification: Establishing a new authentication baseline

With nearly two-thirds of respondent organizations (65%) now utilizing IDV, the technology has moved well beyond adoption to become a rising enterprise standard. Not only are IDV adoption levels high relative to other forms of authentication, but it has emerged as a strong investment priority for preventing fraud and supporting workforce assurance. Current deployment methods show biometrics leading at 67%, closely followed by government-issued documents such as driver's licenses or passports (64%) and device recognition/fingerprinting (58%).

Which specific identity verification (IDV) methods does your organization currently use?



From persona-based protection to enterprise-wide assurance: Operationalizing trust across the enterprise

On average, 92% of enterprise employees still rely on usernames and passwords, with two-thirds of firms reporting 100% adoption of these legacy credentials across their workforce. Nearly two-thirds (65%) use "traditional" MFA such as OTP tokens, SMS messages or push notifications, while 60% use biometrics and 52% employ risk-based MFA.

The breadth of passwordless usage is more encouraging, with respondents reporting that 43% of their employees on average use passwordless technology. More than one-third of enterprises have successfully scaled passwordless to more than 50% of their workforce. Overall, these disparities suggest that phishing-resistant tools such as passwordless and IDV are currently confined to "persona-based" silos — prioritized for executives and privileged IT staff — while enterprise-wide protection remains a secondary roadmap objective.

IDV is among the least internally distributed authentication methods, typically used by a small percentage of employees or limited to a few specific user personas and use cases. On average, IDV is used by just 28% of employees. Organizations recognize they must verify users, but they need a unified approach to do so consistently and automatically. The lack of internal distribution may reflect ongoing uncertainty about ownership and budgeting for workforce IDV. While various stakeholders (HR, IT, IAM, security teams) have roles in procurement, none clearly own the entire process. Another factor is that IDV is still mainly reserved for specific use cases such as account creation (79%), high-risk transactions (76%), and credential reset and account recovery (59%).

Conclusion

As organizations emerge from the Age of Enlightenment, a better understanding of what is needed marks a major step forward for the passwordless movement.

The gap between password usage and true passwordless authentication is narrowing, but not quickly enough to keep pace with the accelerating velocity of AI-driven threats. This leaves enterprises burdened by a massive and growing "password debt" — legacy credentials, fragmented controls and persona-based deployments that attackers are exploiting.

This pause in adoption does not reflect a lack of readiness or conviction; rather, it reflects a collision with reality. Scaling identity is not a feature rollout; it involves complex systems work. It forces organizations to confront legacy infrastructure, fragmented ownership across HR, IT, IAM and security, and the operational complexity of consistently enforcing trust across every workflow where identity is granted.

Nowhere is this more evident than in workforce identity verification. Organizations overwhelmingly recognize the need to systematize the orchestration of workforce identity verification across the employee life cycle. However, responsibility remains diffuse, budgets misaligned, and deployment limited to narrow use cases. The tools exist. What is missing is a unified, automated, enterprise-wide approach.

Taken together, the findings in this report do not point to an industry falling behind but an industry entering its most difficult and consequential phase. Closing this deployment gap is the defining work of the Age of Industrialization — the effort that will determine whether the breakthroughs of the Renaissance and the clarity of the Enlightenment translate into durable resilience. Without enterprise-wide effort to operationalize identity across every workflow, organizations will continue to fund security reactively, absorbing preventable risks, disruptions and costs.

Methodology

The online survey collected data from 950 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 November 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 451 Research from S&P Global Energy Horizons, leading the identity and access management (IAM) vertical within the Information Security channel. Prior to his coverage of IAM, Garrett also covered cloud security data security and governance, risk and compliance. Within IAM, Garrett's current research specializations include passwordless authentication, cloud-native authorization, identity governance and administration (IGA), privileged access management (PAM), identity security and non-human identities (NHIs).

He arrived at S&P Global 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 Energy

See how HYPR helps secure your workforce and customers
Visit: hypr.com/get-a-demo