2026

Global State of Authentication Survey

Perceptions Vs. Reality: Gaps In Authentication Security

yubico | okta

Table of Contents

Executive Summary 1

The Adoption Gap 3

- High Familiarity with Modern Authentication 4
- Trapped by the Onboarding Default 5
- The Home-to-Work Spillover 6
- Optimism Bias and the Non-Human Threat 7

Dollars and Sense: The AI Phishing Surge 8

- The Death of the "Obvious" Phish 9
- Deepfakes and High Success Rates 10
- Can You Spot the Bot? (Spoiler: The Experts Couldn’t) 11

The Agentic Future: Securing Non-Human Identities 12

- The Verification Mandate 13
- Delegation Outpaces Security Controls 14
- The Requirement for Human-in-the-Loop 15

Regional Analysis 16

Creating a New Security Architecture 18

Conclusion 20

Corporate Statements & Methodology 22

Executive Summary

For years, enterprise security strategies have operated under a foundational assumption: if we educate people, security will follow. Cybersecurity leaders are clear about what it takes to protect both organizations and individuals: adopt multi-factor authentication (MFA) and prepare for AI-driven threats that could widen existing security gaps.

Still, all too often, security knowledge doesn't translate into practice, and organizations remain vulnerable. There is a persistent gap between knowing and doing.

The findings of this report suggest that the gap isn't educational but rather structural: both inside and outside of work, login friction and authentication fatigue consistently pulls even the most knowledgeable professionals toward the path of least resistance. This may be underscored by possible concerns of being locked out of personal accounts, individuals could revert to simple passwords and familiar SMS MFA. Overcoming insecure defaults – such as usernames and passwords – requires recognizing that even highly skilled experts fall prey to human behavioral biases and operational blind spots. The opportunity is not to change the person, but to change the underlying infrastructure: organizations must eliminate legacy defaults and replace them with friction-free, phishing-resistant authentication across all systems.

In recent years, we've surveyed working adults around the globe to find out how much they're building smart cybersecurity practices into their lives. This year, Yubico took a new approach, partnering with Okta to survey nearly 2,000 cybersecurity and IT professionals across nine countries. These are people who live in the security world full-time. They design policies, manage access, and know better than anyone how easily standard passwords crumble under attack.

Nearly

2,000

Technology And Security Professionals

9

Countries

Moving Beyond Passwords and Awareness

Our findings reveal a major opportunity for organizations to modernize their cybersecurity practices by creating a new security architecture. While expertise and awareness of secure authentication methods are at an all-time high, even security professionals still rely on legacy password-based workflows initiated during workforce onboarding. And as long as enterprises issue passwords during onboarding, employees will continue to use them.

When it comes to phishing, rather than relying on workforce visual inspection to catch subtle anomalies indicating an illegitimate webpage, forward-looking security teams recognize that phishing-resistant authentication is the ultimate safeguard, removing humans entirely from security decision-making. Instead, modern authentication methods secure at the exact moment of access through a cryptographic exchange of signed nonces and domain verification, ensuring that even if an employee falls victim to a phishing lure, authentication fails automatically and the attack is completely halted.

The bottom line: Security awareness is not the bottleneck to the secure enterprise. The bottleneck is operational friction and outdated default practices that don't account for addressing identity before, during, and after authentication. Closing this gap requires moving beyond education and enforcing the use of hardware-backed, phishing-resistant authentication across every identity, both human and machine.

yubico | okta

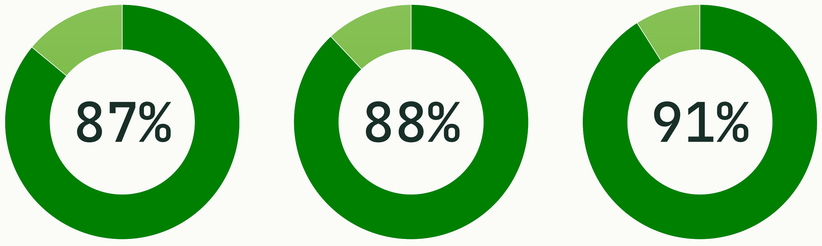
The Adoption Gap



High Familiarity with Modern Authentication

Enterprise security teams possess deep domain knowledge. When asked to evaluate access controls, they identify **device-bound, hardware-backed passkeys** as the most secure (**31%**), outranking mobile authenticator apps (**29%**) and synced passkeys (**27%**).

Their familiarity is undeniable: **87%** are familiar with passkeys, **82%** have received security training from their employer, and only **3%** have never used a passkey. On paper, these professionals are experts at identifying which tools are the gold standard for protecting enterprises, employees, and customers against cyber threats.



High Awareness:

87% of security professionals are familiar with passkeys, and **31%** explicitly recognize device-bound, hardware-backed passkeys as the most secure credential available.

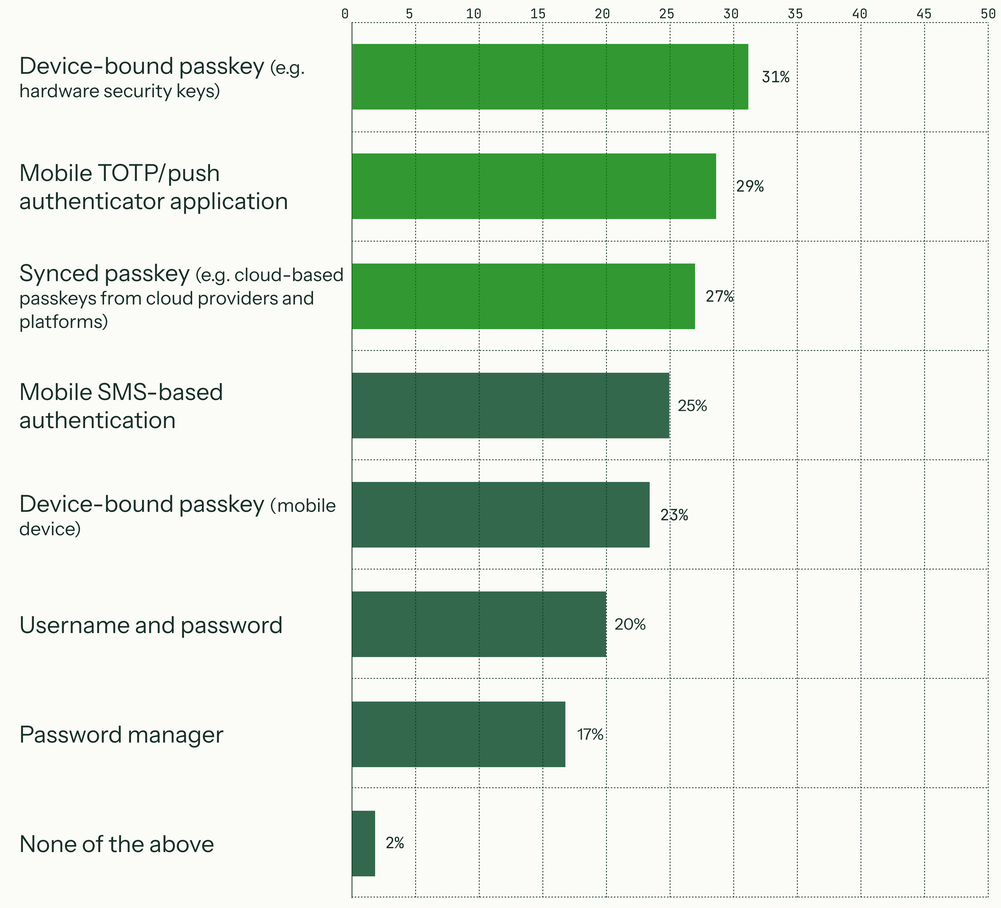
Proactive Security Culture:

88% of security leaders express confidence in their organization's current safety posture, reflecting significant investments in tools, infrastructure, and team training.

Ready for the AI Era:

91% of leaders recognize the importance of authenticating AI agents, demonstrating forward-thinking readiness for non-human identities.

In your opinion, what are the most secure methods of authentication?



Trapped by the Onboarding Default

Despite their expertise, daily habits mirror those of non-technical workers. Usernames and passwords remain the single most common way security pros log in to work accounts (**43%**), while hardware-backed passkeys rank as one of the last methods in actual daily adoption, at **25%**.

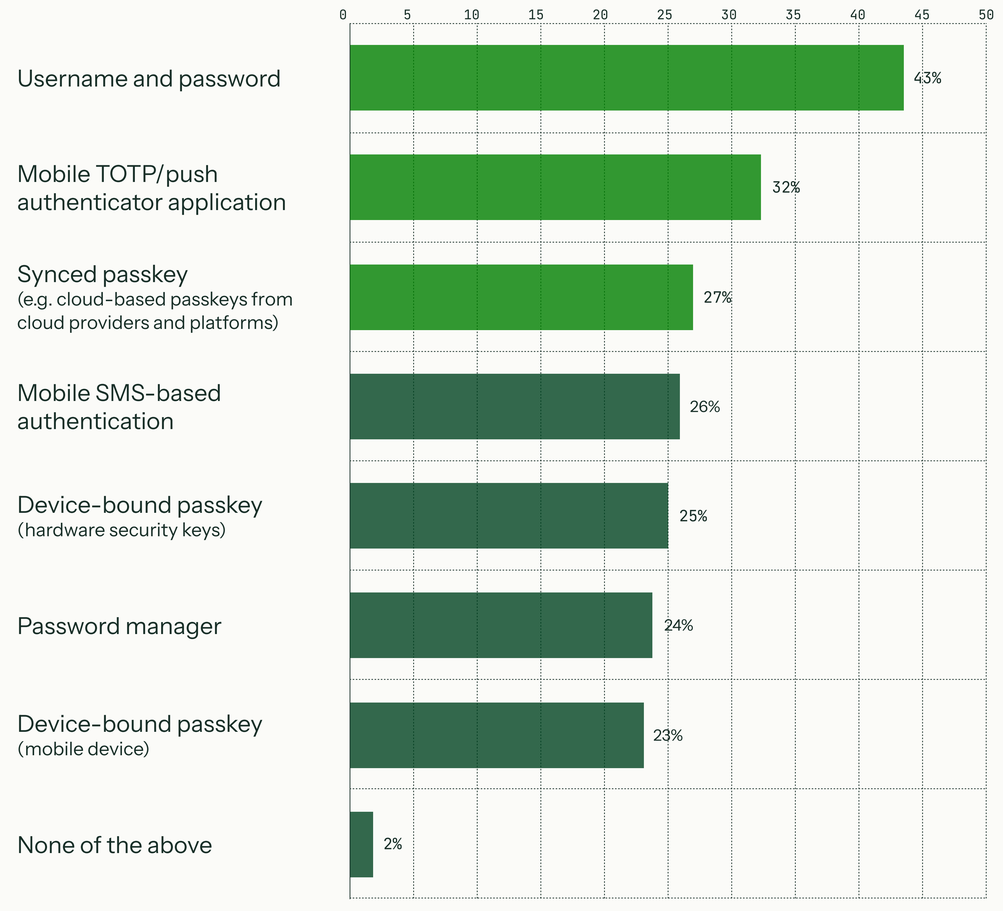
The survey reveals that long-standing workplace habits often trace back to day-one defaults. Over half of respondents (**52%**) were issued traditional username-and-password credentials when starting their roles, establishing legacy login habits that persist over time.

Operational disconnects deepen the risk:

- **76%** of organizations use fragmented authentication methods across different internal applications.
- **45%** rely on usernames and passwords as the primary credential across systems.
- **23%** do not mandate MFA across all enterprise applications and services.

The context in which these defaults exist changes between work and home. In the work setting, onboarding defaults and potential lockouts are backed by an IT helpdesk ready to restore access. At home, individuals are left to manage their security on their own.

How do you authenticate/login to your work accounts?

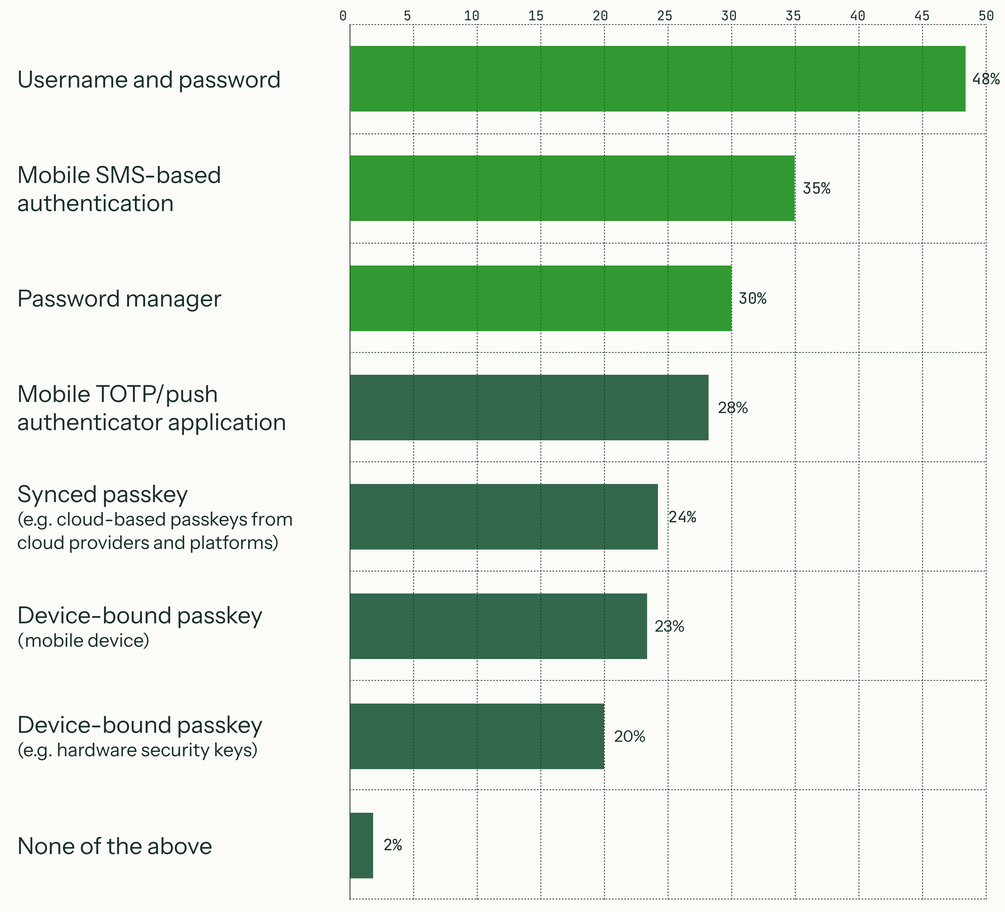


The Home-to-Work Spillover

Given our human tendency to choose the easiest path, overcoming authentication defaults takes concerted effort both inside and outside of work. Perhaps it's not surprising, then, that even in their personal lives, **48%** of cybersecurity pros rely primarily on usernames and passwords, followed by SMS-based verification (**35%**). Only **20%** use hardware-backed passkeys for personal accounts.

With **28%** leaving their personal email unprotected by MFA, attackers gain an easy entry point. An unprotected inbox linked to a mobile carrier (**38%**) serves as the catalyst for SIM-swap attacks, putting both personal identity and corporate credentials at risk.

How do you authenticate/login to your personal accounts?



Optimism Bias and the Non-Human Threat

Despite these vulnerabilities, **88%** of respondents describe their enterprise as "secure" (with **34%** claiming "very secure").

In behavioral psychology, this is known as **optimism bias**, the belief that expertise insulates an individual or institution from negative outcomes. Security leaders rate their own posture generously while assuming competitors face greater exposure.

As enterprises integrate autonomous AI software agents into daily workflows, accounts guarded by passwords will soon be accessed by non-human helpers. An organization that fails to enforce strong authentication for human employees cannot safely govern autonomous agents.

> Enterprise cybersecurity has a critical execution gap. Security leaders know hardware-backed passkeys - specifically hardware security keys - offer the highest level of protection, yet nearly half still rely on basic usernames and passwords daily. The gap isn't expertise; it's overcoming the friction to user adoption.

Poupak Enbom,
Chief Market and Growth Officer at Yubico

Operational disconnects deepens the risk



88% of respondents describe their enterprise as "secure".

34% claiming "very secure"

Dollars and Sense: The AI Phishing Surge



The Death of the "Obvious" Phish

As generative AI accelerates digital communication and makes it more tailored, AI-driven phishing attempts across the industry have naturally increased. **70%** of respondents noted an increase in organizational phishing over the past year, with **55%** being targeted by personalized attacks directly. **22%** have even received targeted messages within the last week.

Rather than relying on legacy indicators of a phishing webpage, such as typos or awkward phrasing, forward-looking security teams are recognizing that phishing-resistant authentication, not human visual inspection, is the ultimate safeguard. In other words, humans should not be responsible for identifying and stopping AI-based threats. Instead, the most innovative methods secure at the moment of authentication through domain verification and cryptographic-based security. This ensures that even if a user falls victim to a phishing attempt, the authentication technology can detect and block the login, even if the user is completely unaware of the attack.



Deepfakes and High Success Rates

Because modern attacks bypass traditional cognitive filters, initial breach rates have surged. 44% of respondents report that their organization suffered at least one successful AI-driven attack in the past 12 months.

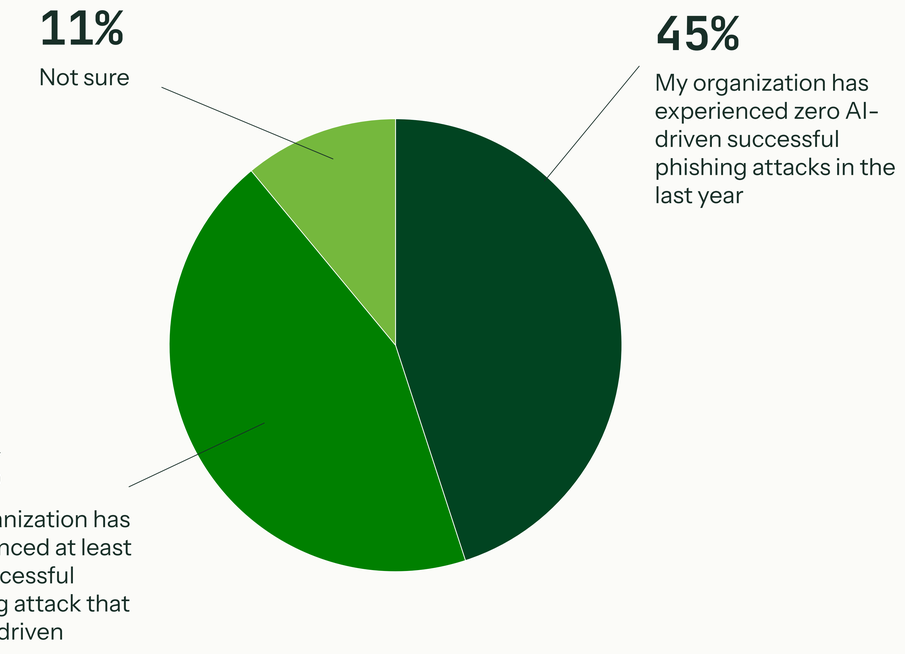
Voice cloning and synthetic media now allow bad actors to impersonate trusted colleagues with minimal source material:

- **43%** reported suspicious video, voice memo, or phone impersonations targeting executives or clients.
- **29%** were directly targeted by deepfake communications.

Okta's 2026 AI Agents at Work report describes a second route into the same organizations. More than half of the knowledge workers surveyed (**52%**) reported using unsanctioned AI tools at work, with nearly a quarter doing so regularly. Among those using unapproved tools, the most commonly shared materials were internal messages and emails (**54%**), HR-related information (**45%**), and confidential company documents, including financials and contracts (**39%**).

okta

Which of the following statements is true about the success of artificial intelligence (AI) driven phishing attacks at your organization in the last year?



Can You Spot the Bot? (Spoiler: The Experts Couldn’t)

Organizations have long relied on employees as a "human firewall" to spot anomalies. To test this defense, we presented security leaders with two messages: one human-written, one AI-generated - and asked them to identify the source.

The results reveal that **human detection is no longer a viable security control:**

- Only 36% of security professionals correctly identified a question that a human wrote, 54% thought AI wrote the message, and 10% weren’t sure.
- 39% of respondents also failed to recognize the AI-generated question.

Human email

Hi [NAME],

Our Employee Handbook has been updated to incorporate changes for 2027. Several areas have been added. Please review the updated document in its entirety and acknowledge receipt by November 1, 2026.

Required Action - Due November 1, 2026
Please log in to our company’s intranet and look for the prompt under Things to Do. This and all of our policies are accessible on our home page.

Thank you in advance for your cooperation in helping our company remain compliant.

Warm regards,
Your HR Team

AI email

Hi [NAME],

As we look ahead and plan for the future, we’ve given our Employee Handbook a fresh update for 2027. We've added a few important new sections to make sure our policies keep supporting you and our growing team in the best way possible.

Because of these new additions, we need everyone to review the updated document and quickly sign off on it.

What we need from you by November 1, 2026:
1. Log in to the company intranet.
2. Check your "Things to Do" list on the home page.
3. Take a look through the updated handbook and click to acknowledge you've received it.

(Keep in mind: You can always find the handbook, along with all of our other company policies, pinned to the intranet home page whenever you need to reference them.)

Thank you so much for taking a few minutes out of your day to help us keep everything running smoothly and compliantly!

Warmly,
Your HR Team

The Agentic Future: Securing Non-Human Identities



The Verification Mandate

As autonomous AI agents shift from passive assistants to active operational tools, verifying machine identity has become a top priority. **91% of respondents state it is essential to verify the identity and authenticity of AI agents**, with **57%** rating it as critical.

Okta's 2026 Businesses at Work report finds that 74% of organizations report widespread or moderate use of nonhuman identities, that 90% lack a comprehensive strategy for governing them, and that only 32% govern AI agents with the same rigor they apply to human identities.

okta



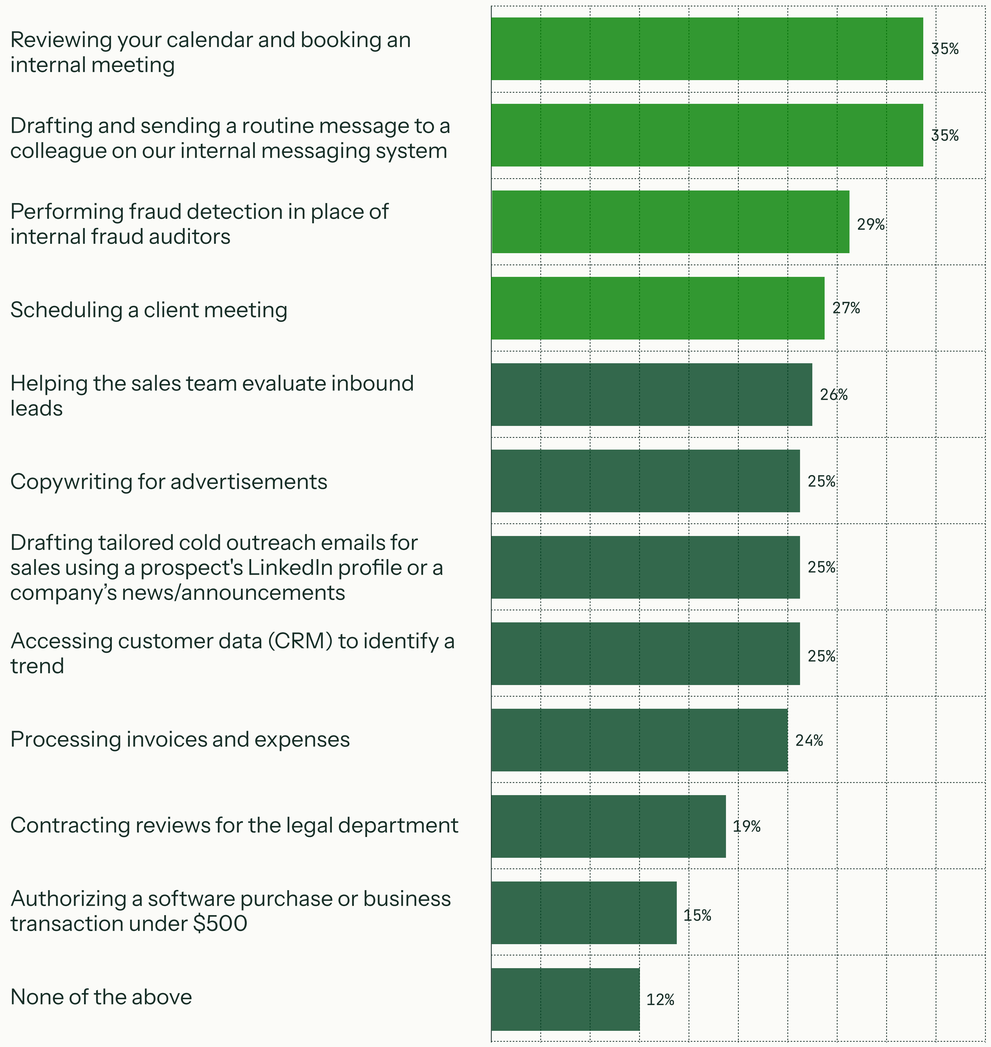
Delegation Outpaces Security Controls

Workforce delegation to AI agents is moving rapidly. Security leaders report high comfort levels delegating operational tasks to AI:

1. Scheduling & Calendar Management (35%)
2. Drafting Internal Communications (35%)
3. Automated Fraud Detection (29%)
4. Client-Facing Meetings (27%)

Generational divides are stark when it comes to AI-delegated communications: **68% of Gen Z professionals** feel comfortable permitting an AI agent to communicate with clients or colleagues on their behalf, compared to just **27% of Baby Boomers**.

Which tasks, if any, are you comfortable outsourcing to an AI agent to automate on your behalf?



The Requirement for Human-in-the-Loop

While comfort levels with AI delegation vary, one thing remains clear: human-in-the-loop is still critical, with **91% insisting on maintaining a "human-in-the-loop" approval step** before an agent executes actions on their behalf.

While agent-to-agent workflows require autonomous execution to scale, human verification can serve as a safety check for critical workflows, for instance, before an agent escalates privileges or executes financial transactions.



> While security leaders and younger generations are eagerly handing operational tasks over to AI - from routine scheduling (35%) to client interactions (up to 68% for Gen Z) - an overwhelming 91% still draw a firm line at execution, insisting on keeping a human in the loop for final approval.

Poupak Enbom,
Chief Market and Growth Officer at Yubico

Regional Analysis

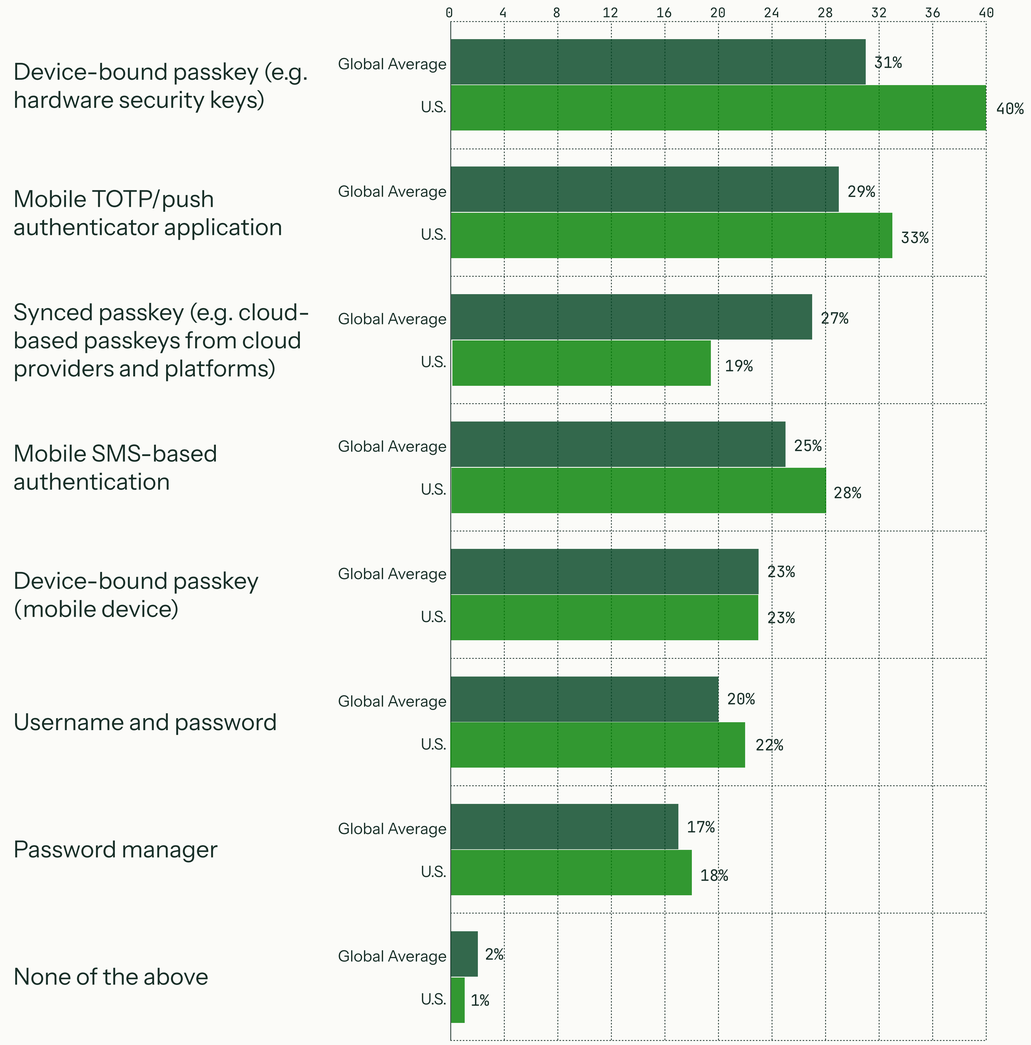


The United States Adoption Gap

No market illustrates the gap between awareness and practice more clearly than the United States: **it possesses the highest technical awareness, the lowest systemic trust, and the slowest rate of operational change.**

- **High awareness: 40%** of U.S. security leaders identify hardware-backed passkeys as the most secure credential (vs. **23%** in the UK), and **48%** of passkey users have personal experience using hardware-backed keys them (vs. **28%** in Singapore).
- **High reliance on legacy credentials:** Simultaneously, the U.S. leads all markets in password dependency - **50%** use usernames and passwords at work, and **56%** use them at home.
- **Low trust:** Only **58%** of U.S. respondents believe the enterprises handling their personal data are doing enough to protect it (vs. **82%** in India).

What are the most secure methods of authentication?



Creating a New Security Architecture



Eliminating Credential Risk: A Three-Phase Hardware Defense Plan

Building a more secure enterprise requires recognizing that awareness training cannot fix an architectural problem. Despite high security literacy, organizations remain hindered by operational friction, perceived deployment costs, and legacy onboarding defaults that treat high-assurance MFA as an optional luxury rather than a foundational requirement.

To eliminate credential risk in the AI era, security architectures must enforce phishing-resistant, hardware-backed passkeys and other device-bound cryptographic authenticators across three distinct phases.

- **Before Authentication:** Mandate device health and posture checks to verify endpoint compliance before establishing an access session. Issue phishing-resistant authenticators to new employees as part of the workforce onboarding process to support high-assurance MFA from the first login attempt.
- **During Authentication:** Enforce the use of phishing-resistant authentication in application sign-on policies to consistently and automatically mitigate AI phishing attempts at sign-in.
- **After Authentication:** Maintain continuous context and risk evaluation to detect session compromise. Requiring proof of human presence, either through a physical hardware interaction such as a key touch or biometric authentication, for human-in-the-loop authorization of autonomous AI workflows.



Conclusion



From Awareness to Enforcement

The results of the 2026 Global State of Authentication demonstrate that security awareness alone is insufficient to safeguard the enterprise. The opportunity is to break a systemic pattern: inside and outside the workplace, operational defaults and built-in friction push even smart, highly knowledgeable experts toward the path of least resistance. True security cannot depend on human vigilance against increasingly sophisticated AI threats; it requires shifting corporate architecture to make the smart choice the automatic default.

Security leaders already know what works. It is time for corporate policy and infrastructure to reflect that knowledge.



Corporate Statements & Methodology

About Yubico

Yubico (Nasdaq Stockholm: YUBICO) is a global cybersecurity pioneer and creator of the YubiKey, the gold standard for phishing-resistant, hardware-backed authentication. Since co-creating global passkey standards in 2007, Yubico has eliminated account takeovers for enterprises, governments, and individuals across 160+ countries. Our global footprint includes headquarters in Stockholm, Sweden, Silicon Valley, California; and Singapore. Learn more at www.yubico.com.

About Okta

Okta, Inc. is The World's Identity Company™. We secure AI, machine, and human identity so everyone is free to safely use any technology. Our workforce and customer solutions empower businesses and developers to protect their AI agents, users, employees, and partners while driving security, efficiencies, and innovation. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.

Methodology

Talker Research conducted a quantitative online survey of **1,890 technology and security professionals** across nine markets: the United States, the United Kingdom, Australia, India, Japan, Singapore, France, Germany, and Sweden.

Respondents held roles in Cybersecurity, IT, Product Management, Software Engineering, and Hardware Engineering within enterprise organizations (sized 500+ employees).

Results May Vary: Case studies, customer testimonials, and performance metrics represent the specific operational outcomes of the featured organizations under their unique configurations, network environments, and implementation parameters. These materials are intended for general informational purposes only and are not intended to be legal, privacy, security, compliance, or business advice. ©2026 Okta, Inc. and/or its affiliates.

The survey was commissioned by Yubico and Okta and administered between July 2, 2026, and July 16, 2026.