

High Awareness, Low Adoption: New Survey Reveals Nearly Half of Security Professionals Still Rely on Passwords

Global study from Yubico and Okta highlights a critical execution gap in enterprise security, shows how modern identity controls can eliminate password dependency.

STOCKHOLM & SANTA CLARA, Calif. & SINGAPORE--([BUSINESS WIRE](#))-- Regulatory News:

A new survey from [Yubico](#) (NASDAQ STOCKHOLM: YUBICO), the pioneer of phishing-resistant authentication and creator of the original passkey, the YubiKey, and [Okta, Inc.](#), reveals a significant gap between security knowledge and everyday practice. While security leaders overwhelmingly recognize phishing-resistant passkeys as more secure than passwords, nearly half still rely on vulnerable login methods in their daily work.

Conducted by [Talker Research](#), the annual [2026 Global State of Authentication* report](#) surveyed nearly 2,000 cybersecurity and IT professionals across nine countries. The report highlights that cybersecurity's primary vulnerability is no longer a lack of education or awareness, but a structural problem driven by operational friction and outdated onboarding defaults. Organizations cannot rely solely on additional security awareness training to resolve this gap. Rather, real progress starts with what employees are handed on their first day.

Key Findings Include:

- 43% rely on passwords at work - despite many knowing passkeys are more secure. 31% cited hardware passkeys as the gold standard, 27% voted synced passkeys as most secure and 23% said device-bound passkeys through a mobile device are best.
- 52% inherited passwords on day one, proving that legacy onboarding defaults dictate long-term security habits.
- 44% suffered an AI-driven attack in the last 12 months with Singapore experiencing the highest rate globally (58%), contrasting sharply with Japan (30%) and Germany (38%).
- 39% of security pros failed to distinguish AI-generated text from human writing.
- India (68%), Australia (60%), and the U.S. (56%) show the highest proportion of workers who are "very familiar" with passkeys.
- 91% would like a "human-in-the-loop" approval step before autonomous AI agents execute critical actions.
- Indian professionals lead global markets in willingness to delegate client/colleague communications to AI agents (41% "very comfortable"), compared to just 4% in Japan and 12% in France.
- 50% of U.S. security pros use passwords at work, leading all surveyed global markets in legacy password dependency despite having the highest technical awareness.

"Enterprise cybersecurity has a critical execution gap," said Poupak Enbom, Chief Market and Growth Officer at Yubico. "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."

This operational disconnect begins early: over 50% of security professionals inherit legacy credentials on day one, establishing password dependency by default and perpetuating unsafe habits. Generative AI worsens this risk, as seasoned cybersecurity experts struggle to spot synthetic messaging, making user vigilance unreliable.

Furthermore, deploying autonomous AI agents compounds these issues, as the 91% who want a human approval step will need a reliable way to confirm a real person is behind it.

"Bridging this gap requires organizations to build security directly into the onboarding experience," said Charlotte Wylie, SVP Deputy CSO at Okta. "When legacy login habits persist, enterprises remain vulnerable to modern attack vectors. Together with Yubico, we are providing a unified approach that ensures every employee is protected by zero-trust, phishing-resistant authentication from their first day on the job."

To overcome these structural hurdles, Yubico and Okta are partnering to streamline how enterprise identity systems issue, manage, and enforce hardware-backed credentials. By embedding phishing resistance directly into modern access management platforms, the companies aim to help IT teams eliminate password dependencies without creating operational friction for employees.

About Yubico

Yubico (Nasdaq Stockholm: YUBICO) is a global cybersecurity pioneer dedicated to making the digital world safer for everyone. As the creator of the YubiKey, Yubico set the gold standard for phishing-resistant, hardware-backed authentication—virtually eliminating account takeovers while keeping secure login effortless.

A leader in authentication since 2007, Yubico co-created global standards like FIDO2, WebAuthn, and FIDO U2F, and introduced the foundational technology behind the modern passkey. Today, the company’s passkey solutions secure businesses, governments, and individuals in more than 160 countries, safeguarding the entire digital identity lifecycle from onboarding to recovery.

Trusted by the world’s most security-conscious brands, AI frontiers, and institutions, YubiKeys deliver fast, friction-free, passwordless access across hundreds of enterprise applications out of the box. True to its mission, Yubico also drives the Secure it Forward philanthropic initiative, donating YubiKeys to vulnerable communities and nonprofits globally.

Our global footprint includes headquarters in Stockholm, Sweden, Silicon Valley, California; and Singapore. Yubico is proud to be recognized as one of TIME’s 100 Most Influential Companies and Fast Company’s Most Innovative Companies. Learn more at www.yubico.com.

*The 2026 Global State of Authentication report was conducted by Talker Research between July 2, 2026, and July 16, 2026. The quantitative survey polled 1,890 technology and security professionals in enterprise organizations (500+ employees) across nine markets: the United States, the United Kingdom, Australia, India, Japan, Singapore, France, Germany, and Sweden. Respondents held roles across Cybersecurity, IT, Product Management, Software Engineering, and Hardware Engineering.

Contacts

Media Contact:
Yubico Communications Team
press@yubico.com

Source: Yubico