Keeper Security Insight Report: Navigating a Hybrid Authentication Landscape

Keeper's report reveals that while 80% of organisations are adopting passkeys, 57% of IT leaders report challenges in managing dual authentication systems

LONDON, HERTFORDSHIRE, UNITED KINGDOM, January 24, 2025 /EINPresswire.com/ -- Keeper Security, the leading cybersecurity provider of zero-trust and zero-knowledge Privileged Access Management (PAM) software protecting passwords, passkeys, privileged accounts, secrets and remote connections, announces the release of its latest Insight Report, "Navigating a Hybrid Authentication Landscape." This report explores the evolving strategies organisations are using to secure sensitive data and identities in an increasingly complex digital environment. As traditional password-based authentication faces rising threats, including phishing and credential stuffing, organisations are increasingly adopting innovative solutions like passkeys to strengthen their security. However, passwords remain integral to many legacy systems, resulting in the need for a hybrid approach that combines both passkeys and passwords.

> “Organisations are navigating a pivotal shift in authentication, balancing the need for modern passkeys with the continued reliance on passwords for many legacy systems.” ”
> *Darren Guccione, CEO and co-founder at Keeper Security*

The findings of Keeper’s report, based on insights from IT and security leaders worldwide, highlight the relationship between emerging authentication technologies and the persistence of passwords in securing online systems. The report provides an in-depth look at how organisations are navigating these challenges while maintaining robust security.

Key findings from the report include:

Majority of Organisations are Adopting Passkeys: Passkeys, which use public key cryptography to authenticate users without the need for passwords, are gaining traction. 80% of organisations are using or planning to adopt passkeys, as they offer a significant reduction in risks like phishing and credential stuffing, compared to traditional passwords.

Hybrid Authentication is Common: 40% of businesses continue to rely on hybrid authentication systems that blend both passwords and passkeys. These hybrid setups are often necessary due to the prevalence of legacy systems and specialised applications that have yet to support passkeys.

Phishing Remains a Persistent Threat: Despite the adoption of passkeys, phishing continues to be a major threat. In fact, 67% of businesses report phishing as a persistent issue in hybrid authentication environments, underscoring the need for comprehensive security measures beyond passkeys alone.

IT Leaders Face Challenges with Dual Systems: Managing both passwords and passkeys presents a significant challenge for 57% of IT leaders, such as concerns over user confusion, integration difficulties and training demands in managing hybrid systems.

Phased Adoption of Passkeys: 70% of organisations, adopting passkeys are implementing them in phases, prioritising critical systems first and ensuring operational compatibility with existing password-based systems.

The report highlights the need for organisations to adopt a layered approach to authentication, balancing modern solutions like passkeys with strong password practices. It also stresses the importance of employee training, infrastructure upgrades and streamlined integration to ensure the security and usability of authentication systems as organisations continue their digital transformation.

“Organisations are navigating a pivotal shift in authentication, balancing the need for modern passkeys with the continued reliance on passwords for many legacy systems,” said Darren Guccione, CEO and Co-founder, Keeper Security. “Our mission is to provide comprehensive solutions that can manage and secure every type of credential – from traditional passwords to passkeys and secrets – all within a zero-trust and zero-knowledge framework. This approach ensures organisations can confidently adapt to the hybrid authentication landscape while maintaining the highest standards of security and usability.”

As we recognise Data Privacy Week next week, Keeper Security’s report serves as a timely reminder of the critical role authentication plays in safeguarding sensitive information. With cyber threats continuing to evolve, organisations must stay proactive in adopting flexible, secure authentication methods to stay ahead of emerging risks.

For more insights, please click here to access the full Keeper Security Insight Report.

###

About Keeper Security

Keeper Security is transforming cybersecurity for people and organisations globally. Keeper's intuitive solutions are built with end-to-end encryption to protect every user, on every device, in every location. Our zero-trust privileged access management platform deploys in minutes and seamlessly integrates with any tech stack to prevent breaches, reduce help desk costs and ensure compliance. Trusted by millions of individuals and thousands of organisations, Keeper is the leader for password, passkey and secrets management, privileged access, secure remote access and encrypted messaging. Learn how our zero-trust and zero-knowledge solutions defend against cyber threats at KeeperSecurity.com.

Bethany Smith
Eskenzi PR
email us here
Visit us on social media:
Facebook
X
LinkedIn
Instagram
