KEEPER®

Keeper Security Insight Report

Navigating a Hybrid Authentication Landscape

Introduction

As the threat landscape evolves, advanced strategies are essential to protect sensitive data and identities. Traditional password-based authentication, though still prevalent, has increasingly demonstrated its vulnerability to sophisticated threats like phishing and credential stuffing. Passkeys offer a promising alternative, leveraging public key cryptography, consisting of a private key stored locally on a user's device and a public key stored with the service provider. This ensures that even if a breach occurs, cybercriminals can only access the public key, which is useless without the private key.

Passkeys are gaining significant traction, with 80% of organizations either already using or planning to adopt this technology. Beyond their security benefits, passkeys offer unparalleled ease of use, eliminating the need to remember complex passwords and enabling seamless authentication. Businesses are recognizing the advantages of passkeys—particularly their resilience to common attack vectors like phishing. However, widespread adoption remains hindered by limited support from websites and applications, as well as challenges posed by legacy systems and the need for physical access to the device storing the passkey.

While adoption progresses, passwords remain deeply ingrained in millions of systems worldwide, making a hybrid approach—where passkeys and passwords coexist—the current reality for both individuals and organizations.

This report explores the evolution of modern authentication solutions, drawing on insights from over 800 IT and security leaders globally. By examining the benefits, challenges and interplay between passkeys and passwords, organizations can develop a more secure and user-friendly approach to online authentication.

Hybrid Authentication: A Pragmatic Approach

Passkeys are no longer experimental; they are an integral part of modern authentication strategies. While adoption is growing rapidly, Keeper's survey reveals that 40% of businesses still manage hybrid systems that blend passwords and passkeys. This highlights the continued reliance on passwords, particularly for legacy systems and niche applications.

40%

of businesses still manage hybrid systems that blend passwords and passkeys.

Benefits of Hybrid Systems

- **Layered Security:** Passkeys reduce risks like phishing, while passwords provide a solution for systems without passkey support.
- **Enhanced Flexibility:** Businesses can transition at their own pace, adopting passkeys where feasible while maintaining operations in environments that still rely on passwords.
- **Simplified User Experience:** Passkeys streamline login processes by removing the need for users to remember passwords, providing fast and intuitive authentication.

However, maintaining a hybrid authentication approach introduces complexity. Employees must navigate dual methods and IT teams face challenges integrating modern solutions with older systems. To streamline operations and maintain security, organizations need clear policies, robust training and secure password management.

The Enduring Role of Passwords

While passkeys represent a significant leap forward in authentication, passwords aren't going away anytime soon. Many organizations still rely on passwords, particularly due to the prevalence of legacy systems and the resource demands of transitioning to passkey-only environments. Keeper's research highlights the continued security risks, with 67% of businesses reporting phishing as a persistent threat, even in hybrid setups where both passwords and passkeys are used.

This reality is further compounded by poor password practices—40% of employees reuse passwords across multiple accounts, leaving organizations vulnerable to credential stuffing attacks. A comprehensive Privileged Access Management (PAM) platform, which includes integrated password management, helps mitigate these risks by enforcing strong, unique credentials while securing access to critical systems. As organizations prepare for a shift toward passkey-centric solutions, PAM provides the tools to manage today's hybrid authentication environment effectively.

Why Passwords Persist

Passwords are deeply ingrained due to:

- **Legacy Systems:** Many enterprise systems are still reliant on password-based authentication and do not yet support passkeys.
- **Cost Considerations:** Fully transitioning to passkeys can be resource-intensive, particularly for smaller organizations.
- **Behavioral Challenges:** Users are accustomed to passwords, and shifting away from them requires a cultural shift supported by ongoing education and training.

67%

of businesses reporting phishing as a persistent threat, even in hybrid setups.

Balancing Security with Usability

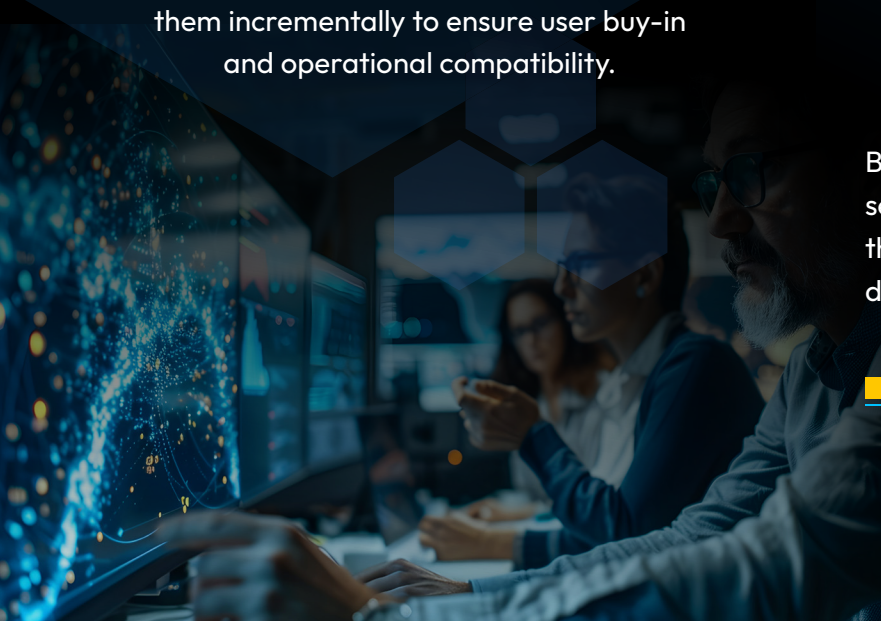
IT Leadership Perspectives

57%

of IT leaders express concerns about managing dual systems, highlighting user confusion, integration challenges and training demands.

70%

of businesses adopting passkeys are taking a phased approach, introducing them incrementally to ensure user buy-in and operational compatibility.



One of the greatest challenges in authentication is maintaining robust security without compromising the user experience. Hybrid authentication systems require careful planning to achieve this balance.

Navigating Complexity

When it comes to implementing passkeys, organizations must:

- **Educate Users:** Providing clear, consistent guidance on when and how to use passkeys versus passwords helps minimize user confusion and disruption to workflows.
- **Update Systems:** Investing in IT infrastructure is essential to integrate passkeys with existing applications.
- **Streamline Processes:** Tools like Single Sign-On (SSO) and centralized authentication management can help reduce friction in hybrid environments.

By addressing usability concerns alongside security objectives, businesses can foster trust in their systems, improve productivity and minimize disruption to operations.

Strategic Deployment of Passkeys

Passkeys are particularly effective in high-security industries like banking, healthcare and critical infrastructure, where the risks of unauthorized access are highest. Meanwhile, passwords remain a viable option for lower-risk applications, offering cost-effective solutions for legacy systems and less critical assets. To ensure adequate security, passwords should be at least 16-characters long with upper and lowercase letters, numbers and symbols, and protected by Multi-Factor Authentication whenever available.

This strategic layering of authentication methods ensures a balance between security and efficiency, allowing businesses to allocate resources where they will have the greatest impact.

Tailoring Authentication to Risk

Organizations optimizing their authentication strategies should consider:

- **High-Security Environments:** When available, use passkeys to protect sensitive data, privileged accounts and customer records.
- **Lower-Risk Applications:** Retain passwords for non-critical systems where the risk of compromise is lower.
- **Legacy Applications:** When passkeys are not available, enforce password best practices and implement MFA to provide additional security.

Preparing for the Future

80%

of organizations plan to integrate both passkeys and passwords moving forward.

70%

of businesses currently without passkey support are considering phased adoption, prioritizing critical systems first.

As the digital threat landscape evolves, authentication strategies must evolve as well. The transition to passkeys represents a significant advancement, but businesses must approach it with a long-term perspective. Key findings from Keeper's survey include:

Recommendations for Businesses

Businesses should prioritize investing in employee training to ensure teams are equipped with the knowledge to use passkeys effectively and recognize potential security threats. Modernizing infrastructure is crucial, as upgrading systems to support passkeys will help ensure seamless interoperability. A layered approach to authentication is also recommended, as it allows businesses to leverage the strengths of both passkeys and traditional methods, mitigating risks across diverse systems. Ultimately, the future of authentication depends on adaptability; by staying informed and proactive, businesses can not only address current challenges but also embrace emerging technologies for enhanced security.

Methodology

This research was conducted by Keeper Security in collaboration with the independent research agency TrendCandy. The study surveyed a total of 801 IT and security leaders from key regions across the globe, including the US or Canada, the UK, France, Japan, Australia or New Zealand and Germany.