Keeper® Security Adds Support for Hardware Security Keys as Sole 2FA Method

Business and consumer users now have even more control over the use of security keys for convenient and highly secure authentication.

LONDON, UNITED KINGDOM, January 17, 2024 /EINPresswire.com/ -- Keeper Security, the leading provider of zero-trust and zero-knowledge cybersecurity software protecting passwords, passkeys, privileged access, secrets and remote connections, today introduces support for hardware security keys as a single Two-Factor Authentication (2FA) method. Implementing user authentication with only a hardware security key enhances overall security by providing a robust physical second factor, mitigating remote attacks and reducing dependency on mobile devices. Administrators can enforce the use of a hardware key as the sole 2FA method and mandate even more robust restrictions by requiring the use of a PIN.

> With Keeper, administrators can now enforce the use of a hardware security key as the sole 2FA option, empowering users with a simple and user-friendly, but highly secure authentication method."
>
> *Craig Lurey, CTO and Co-founder of Keeper Security*

Stronger authentication factors are becoming increasingly important as cybercriminals become more sophisticated, breaking down what were previously considered ironclad defences. Traditional 2FA methods such as SMS and Time-Based One-Time Password (TOTP) can be vulnerable to social engineering and SIM swapping. In fact, the National Institute of Standards and Technology (NIST) removed the use of SMS authentication from its recommended authentication methods list due to its vulnerabilities. This has led organisations and individuals alike to seek out more secure 2FA alternatives.

“Cybercriminals are creative and relentless in their mission to break historically secure solutions,” said Craig Lurey, CTO and Co-founder of Keeper Security. “In response, many organisations are transitioning to hardware-based 2FA devices like YubiKey. With Keeper, administrators can now enforce the use of a hardware security key as the sole 2FA option, empowering users with a simple and user-friendly, but highly secure authentication method."

While support for hardware security keys is not new to Keeper®, users were previously required to have a backup 2FA option in addition to their security key. Now, enterprise and consumer users alike can have a security key as their only 2FA method. Keeper enables users to have multiple security keys, allowing users to have backup keys, keys in multiple locations or keys for multiple devices.

Existing users can log in to the Keeper Web Vault or Keeper Desktop App version 16.10.12+ to remove other methods of 2FA if they prefer to only use a security key on its own. Administrators can also require their users to enable a PIN (FIDO2 user verification) with their security key, further protecting their organisations. Keeper supports login on iOS and Android devices with a security key. However, setup of a security key as the sole 2FA method must be performed on the Web Vault or Keeper Desktop App.

This is the latest enhancement to Keeper's solutions, on the heels of announcing Granular Sharing Enforcements for its platform. Enterprises select Keeper because of its strong security architecture; ability to support federated and passwordless authentication with any identity provider; seamless integration into on-premises, cloud or hybrid environments; and ease of use across desktop and mobile devices. Keeper Security Government Cloud Password Manager and Privileged Access Manager is FedRAMP Authorised and StateRAMP Authorised, and maintains the Keeper Security zero-trust security framework alongside a zero-knowledge security architecture, so users have complete knowledge, management and control over their credentials and encryption keys.

###

About Keeper Security
Keeper Security is transforming cybersecurity for people and organisations around the world. Keeper's affordable and easy-to-use solutions are built on a foundation of zero-trust and zero-knowledge security to protect every user on every device. Our next-generation privileged access management solution 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 best-in-class password and passkey management, secrets management, privileged access, secure remote access and encrypted messaging.

Charley Nash
Eskenzi PR
charley@eskenzipr.com