KEEPER | PRESS RELEASE

Keeper Security Reimagines and Secures the Passwordless Future with Keeper SSO Connect™ Cloud

Expanded Solution Eliminates IAM Security Gaps with Zero-Knowledge Encryption Model; Seamlessly Integrates With Any Identity Provider or Data Environment

CHICAGO, IL, March 9, 2021 – Keeper Security, provider of the top-rated and industry-leading cybersecurity platform for preventing password-related data breaches and cyberattacks, today announced the release of **Keeper SSO Connect™ Cloud**, a fully-managed SAML 2.0 SaaS solution that can be seamlessly integrated with any identity provider, enabling organizations to significantly enhance and extend their Single Sign-on (SSO) deployments with an integrated zero-knowledge password encryption system. The new cloud deployment option is available as an alternative to Keeper's existing SSO Connect on-premise solution.

The COVID-19 pandemic severely **weakened organizations' security posture** as they scrambled to deploy remote workforces. Many organizations have turned to SSO solutions to reduce password fatigue, minimize help desk tickets for lost passwords, and enhance security and efficiency. However, these solutions have security gaps, which *Keeper SSO Connect* addresses.

"SSO provides great convenience for enterprise employees to access a handful of cloud applications with a single login. However, this leaves large security gaps for protecting the thousands of websites and services that employees use, in addition to other confidential information that needs to be protected in an encrypted vault." said Craig Lurey, Keeper Co-Founder and CTO. "Keeper is the only enterprise password management solution that uses zero-knowledge encryption while at the same time providing a seamless login experience with any SAML 2.0 compatible identity provider. Unlike other solutions, Keeper's integration does not require the user to type in a master password to access their vault. Keeper's security model ensures that the enterprise is in complete control of their encryption keys."

Under Keeper's proprietary zero-knowledge security and encryption model, all data is encrypted and decrypted locally on the user's device using Elliptic Curve and AES-256 cryptography. Customer data cannot be viewed by Keeper Security employees nor by any outside party. Keeper protects organizations against brute force, man-in-the-middle (MITM), and password-stuffing attacks that seek to compromise employee passwords.

With *Keeper SSO Connect*, users log into their Keeper vault through a third-party SSO identity provider such as Microsoft Azure, Okta, Jumpcloud, Ping, Duo or OneLogin. This prompts an authentication request from recognized devices, secured by two-factor authentication. If a user is attempting to access the system from a new device, InfoSec administrators can easily grant access or give permission from an existing device, without compromising security.

"Our primary research indicates that as organizations reduce access friction, they proportionally decrease the frequency of access policy violations and breach events, improving overall security effectiveness," noted Steve Brasen, Research Director at Enterprise Management Associates (EMA). "*Keeper SSO Connect* enables a client-side encryption model that enhances security effectiveness while simultaneously simplifying user access and reducing management efforts."

InfoSec administrators also gain complete visibility and control into employee password practices, enabling them to enforce so they can't enforce security policies such as using a strong, unique password for every account and enabling multi-factor authentication on all accounts that support it. With no installation cost or upfront equipment needed, *Keeper SSO Connect Cloud* can be deployed rapidly across all devices.

To learn more about how Keeper can become a critical part of your identity access management tech stack, check out our **infographic** and **whitepaper.**

© 2021 Keeper Security

KEEPER | PRESS RELEASE

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the highly-rated and patented cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. In 2020, Keeper was named PCMag's Best Password Manager of the Year & Editors' Choice for the third time. Keeper has also been named PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM).

© 2021 Keeper Security