

Keeper® Streamlines Compliance Processes With Granular Sharing Enforcements

Organisations can adhere to strict security compliance policies with full visibility and control over employee usage and sharing of credentials and records.

LONDON, UNITED KINGDOM, January 10, 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,

announces Granular Sharing Enforcements for all products in the Keeper® platform. Granular Sharing enables administrators to enforce detailed creating and sharing permissions at the user level. By implementing these permissions, organisations can ensure employees only have access to the resources necessary for their roles, minimising the risk of unauthorised access, data breaches and lateral movement within a network.

“

It's critical for organisations to have security solutions that help them adhere to increasing regulations and compliance requirements.”

Craig Lurey, CTO and Co-founder of Keeper Security

“It's critical for organisations to have security solutions that help them adhere to increasing regulations and compliance requirements,” said Craig Lurey, CTO and Co-founder of Keeper Security. “Granular permission control helps organisations enhance their security posture by restricting access to sensitive information and systems. With Granular Sharing Enforcements, it's easier than ever for IT administrators to better control the principle of least

privilege and streamline operations within their organisations.”

Keeper's added Granular Sharing Enforcement policies provide more detailed restrictions that administrators can apply to users for both creating and sharing records. Most employees do not need access to all of the data or functionalities within an organisation, and many industries and geographical regions have specific regulations and compliance requirements regarding data protection and privacy, including HIPAA, GDPR, PCI DSS and SOX. Granular permission controls enable organisations to align with local and industry regulations by allowing them to define and enforce access policies. This helps in ensuring the organisation is compliant with industry standards and legal requirements.



Key features of Keeper's Granular Sharing Enforcements include:

Auditing: Keeper provides clear alerting and reporting on over 100 different event types.

Version control: Only a small subset of users have permissions to update or share records, helping teams ensure information is consistent and accurate.

Seamless access on any device: Keeper provides the same user experience across platforms, ensuring cross functionality and ease of use, whether on web, desktop or mobile.

Encryption: Keeper provides secure sharing with elliptic curve encryption, ensuring cybercriminals cannot intercept passwords or other shared records in transit.

Keeper Administrators can easily customise permissions to best suit the compliance needs of their organisation. Administrators modify permissions in the Enforcement Policies section of the Admin Console for the chosen role by selecting Creating and Sharing. Most permissions are activated by default for maximum security. Enforcements have been designed to be simple and powerful, allowing admins to choose the appropriate settings for their unique needs.

Granular Sharing Enforcements are available for all sharing needs within Keeper's Enterprise Password Manager, Keeper Secrets Manager and KeeperPAM. With Keeper's zero-knowledge password management and security platform, IT administrators have complete visibility into employee password practices, enabling them to monitor password use and enforce password security policies, including strong, unique passwords, Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and other security policies. Keeper Secrets Manager® is a fully managed cloud-based, zero-knowledge platform for securing infrastructure secrets such as API keys, database passwords, access keys, certificates and any type of confidential data.

Its latest offering, KeeperPAM™, provides next-generation Privileged Access Management (PAM) that is disrupting the traditional PAM market. KeeperPAM delivers enterprise-grade password, secrets and privileged connection management within a unified SaaS platform that is cost-effective, easy to use and simple to deploy. KeeperPAM enables least-privilege access with zero-trust and zero-knowledge security. 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.

###

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

This press release can be viewed online at: <https://www.einpresswire.com/article/678879514>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.