VaynerX Standardises Credential Security at Global Scale With Keeper Security

The leading modern media company strengthened access control and improved visibility using Keeper Enterprise Password Manager

LONDON, UNITED KINGDOM, January 28, 2026 /EINPresswire.com/ -- Keeper Security, the leading provider of zero-trust and zero-knowledge privileged access management software protecting passwords and passkeys, infrastructure secrets, remote connections and endpoints, today announces the release of a new case study highlighting how VaynerX strengthened credential security across its organisation. The global modern media and communications company leveraged Keeper Enterprise Password Manager, part of the KeeperPAM® platform to mitigate the risk of cybersecurity breaches and strengthen its organisational security.

VaynerX supports some of the world's most recognisable brands across advertising, media, commerce and digital transformation. With teams working across multiple regions and accessing a wide range of internal systems and external client platforms, the organisation identified the need for a more consistent and centralised approach to credential management in order to reduce risk while maintaining the speed and flexibility required in a client-driven business.

"Prior to Keeper, we weren't using a unified approach across the organisation that could capture everything in a single pane of glass," said John Georgatos, Global Chief Information Officer at VaynerX. "Once we introduced Keeper, people immediately loved it. They loved the features and were able to solve a lot of the problems they had with previous platforms."

Organisations of all sizes continue to face persistent credential-based risk in increasingly complex authentication environments. Keeper's global research (https://www.keeper.io/hubfs/Reports/Navigating-Hybrid-Authentication-Landscape-Insight-Report-EN.pdf) shows that 40% of employees reuse passwords across multiple accounts, while 67% of businesses report phishing remains a persistent threat, even as organisations adopt more advanced authentication methods. For global, client-facing organisations that rely on shared access to third-party platforms, these risks make strong credential security and secure credential sharing critical operational requirements.

Keeper Enterprise Password Manager (https://www.keepersecurity.com/enterprise.html?&utm_medium=press_release&utm_campaign=Communications) is built on Keeper's zero-trust and zero-knowledge security architecture,

meaning all credentials are encrypted end-to-end and never accessible to Keeper or any unauthorised third party. The platform enables strong encryption, centralised governance, secure credential sharing options and detailed visibility into credential usage, helping organisations reduce exposure to credential-based attacks while maintaining productivity. As organisations modernise authentication, Keeper also supports passkeys alongside traditional credentials, enabling teams to strengthen access security without disrupting existing workflows.

For VaynerX, selecting a password management solution required more than strong security alone. Ease of use, centralised administration and seamless integration with existing tools and workflows were essential to driving adoption across its global workforce.

"Choosing Keeper came down to its functionality, ease of use and the ability to centrally manage the system, giving us enterprise-level security access," said John Maalouf, SVP, Global Head of Procurement at VaynerX. "Keeper was a simple process to get started. We got access right away after our initial trial, and it was very seamless to integrate Keeper into the various platforms and tools that we already use."

Industry research reinforces why strengthening credential security has become a critical priority. Studies show that more than 80% (https://scoop.market.us/identity-and-access-management-statistics/) of data breaches are linked to weak, reused or compromised passwords, underscoring the importance of centralised credential management for organisations that rely on shared access and collaboration at scale.

"Credential-related threats remain among the most persistent risks facing organisations today," said Darren Guccione, CEO and Co-founder of Keeper Security. "VaynerX's experience with Keeper serves as a roadmap demonstrating how organisations can strengthen password management as a practical foundation for protecting access, maintaining client trust and preparing for the future of authentication without adding unnecessary complexity."

The full case study, "VaynerX Deploys Keeper Enterprise-Wide Across a Global Workforce," (https://www.keepersecurity.com/en_GB/resources/vaynerx-case-study/) is now available and provides a closer look at how a global, client-facing organisation approached credential security at scale.

###

About Keeper Security

Keeper Security is one of the fastest-growing cybersecurity software companies that protects thousands of organisations and millions of people in over 150 countries. Keeper is a pioneer of zero-knowledge and zero-trust security built for any IT environment. Its core offering, KeeperPAM®, is an AI-enabled, cloud-native platform that protects all users, devices and infrastructure from cyber attacks. Recognised for its innovation in the Gartner Magic Quadrant

for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, remote connections and endpoints with role-based enforcement policies, least privilege and just-in-time access. Learn why Keeper is trusted by leading organisations to defend against modern adversaries at KeeperSecurity.com (http://keepersecurity.com/).

Learn more: KeeperSecurity.com (https://www.keepersecurity.com/?&utm_medium=press_release&utm_campaign=Communications)

Charley Nash
Account Manager Eskenzi PR
charley@eskenzipr.com
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
TikTok
X

This press release can be viewed online at: https://www.einpresswire.com/article/887221616