Keeper Security Highlights Urgent Need for Strong Credential Management on Change Your Password Day

Strong credential management is vital for organisations to protect critical systems and prevent unauthorised access to sensitive data

LONDON, UNITED KINGDOM, January 31, 2025 /EINPresswire.com/ -- In recognition of Change Your Password Day, Keeper Security, the leading cybersecurity provider of zero-trust and zero-knowledge Privileged Access Management (PAM) software protecting passwords, passkeys, privileged accounts, secrets and remote connections, is urging organisations to prioritise securing credentials to combat the escalating threat of cyber attacks. Without proper safeguards, compromised credentials can lead to devastating breaches, financial loss and reputational damage.

> This Change Your Password Day, we want to remind organisations of the critical importance of enforcing robust credential management policies."
>
> *Darren Guccione, CEO and Co-founder of Keeper Security*

Privileged accounts, often used by administrators or automated systems to access critical infrastructure, are prime targets for attackers because they provide extensive access to an organisation's most sensitive systems and data. Nearly 40% of data breaches involve these accounts, according to Verizon's 2024 Data Breach Investigations Report.

Breaches involving privileged accounts are also more costly, with the average breach costing $4.35 million, while those involving privileged accounts average $4.5 million, according to research from IBM and the Ponemon Institute. This highlights the critical need for strong credential security measures.

"Weak or stolen passwords are often the first and easiest entry point for cybercriminals. This Change Your Password Day, we want to remind organisations of the critical importance of

enforcing robust credential management policies," said Darren Guccione, CEO and Co-founder of Keeper Security. "Implementing tools like enterprise password management and privileged access management ensures credentials are stored and managed securely – with enforcement and visibility across the organisation – minimising the risk of unauthorised access that can lead to a damaging breach."

Understanding that human error often plays a significant role in breaches, Keeper emphasises the importance of educating employees about password security best practices. This includes training on identifying phishing attempts, avoiding password reuse, implementing MFA and recognising the risks of sharing credentials over unsecured channels. As businesses continue to navigate hybrid work environments, securing credentials is more critical than ever.

Keeper encourages organisations to:

- Implement Password Policies: Set and enforce a policy that requires passwords to be unique and at least 16 characters, with upper and lowercase letters, numbers and symbols.

- Adopt a Privileged Access Management (PAM) Solution: Implement PAM to secure privileged accounts, enforce strong password policies and limit access to critical systems.

- Enforce Multi-Factor Authentication (MFA): Add a critical additional layer of security to protect accounts, even if a password is compromised.

- Monitor for Breaches: Implement dark web monitoring to detect exposed credentials.

- Educate Employees: Conduct regular training on secure credential management and best practices.

The 2024 Verizon Data Breach Investigations Report highlights that 80% of organisations utilising PAM tools have seen a significant reduction in cyber attack success rates tied to credential theft and misuse. KeeperPAM, part of Keeper's comprehensive cybersecurity platform, delivers a powerful solution for securing privileged accounts. KeeperPAM secures and manages access to critical resources including servers, web apps, databases and workloads. As a cloud-native, zero-knowledge platform, KeeperPAM combines enterprise password management, secrets management, connection management, zero-trust network access and remote browser isolation in one easy-to-use interface.

Trusted by thousands of organisations and backed by over 10 years of SOC 2 compliance, ISO 27001, ISO 27017, ISO 27018 certifications and FedRAMP Authorization, KeeperPAM provides a secure foundation for protecting critical systems and data. It offers granular role-based enforcement policies, delegated administration and detailed visibility through advanced reporting tools, all of which help minimise the risk of credential compromise and prevent attackers from escalating access.

This Change Your Password Day, Keeper encourages all businesses to take proactive steps to secure their digital environments and protect their most valuable assets.

###

About Keeper Security
Keeper Security is transforming cybersecurity for millions of individuals and thousands of organisations globally. Built with end-to-end encryption, Keeper's intuitive cybersecurity platform is trusted by Fortune 100 companies to protect every user, on every device, in every location. Our patented zero-trust and zero-knowledge privileged access management solution unifies enterprise password, secrets and connections management with zero-trust network access and remote browser isolation. By combining these critical identity and access management components into a single cloud-based solution, Keeper delivers unparalleled visibility, security and control while ensuring compliance and audit requirements are met. Learn how Keeper can defend your organisation against today’s cyber threats at KeeperSecurity.com.

Charley Nash
Eskenzi PR
email us here
