Pressemitteilung

VaynerX standardisiert die Sicherheit von Zugangsdaten weltweit mit Keeper Security

Führendes modernes Mediaunternehmen stärkt Zugriffskontrollen und verbessert Transparenz mit dem Keeper Enterprise Password Manager

MÜNCHEN, 28. Januar 2026 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Cybersicherheitssoftware zum Schutz von Passwörtern und Passkeys, Infrastrukturgeheimnissen, Remote-Verbindungen und Endpunkten, stellt heute eine neue Case Study vor. Diese zeigt, wie VaynerX die Sicherheit von Zugangsdaten unternehmensweit deutlich verbessert hat. Das global agierende Media- und Kommunikationsunternehmen setzt dafür den Keeper Enterprise Password Manager, einen Bestandteil der KeeperPAM®-Plattform, ein, um das Risiko von Cybersecurity-Vorfällen zu reduzieren und die organisatorische Sicherheit zu stärken.

VaynerX unterstützt einige der weltweit bekanntesten Marken in den Bereichen Werbung, Medien, Commerce und digitale Transformation. Mit Teams in mehreren Regionen, die auf eine Vielzahl interner Systeme sowie externer Kundenplattformen zugreifen, erkannte das Unternehmen die Notwendigkeit eines konsistenten und zentralisierten Ansatzes für das Zugangsdaten-Management. Ziel war es, Risiken zu minimieren und gleichzeitig die Geschwindigkeit und Flexibilität zu erhalten, die ein kundengetriebenes Business erfordert.

„Vor Keeper hatten wir keinen einheitlichen Ansatz im Unternehmen, der alles in einer zentralen Übersicht abbilden konnte“, sagt John Georgatos, Global Chief Information Officer bei VaynerX. „Nach der Einführung von Keeper waren die Mitarbeitenden sofort begeistert. Sie schätzten die Funktionen und konnten viele der Probleme lösen, die sie mit früheren Plattformen hatten.“

Unternehmen jeder Größe sind weiterhin mit anhaltenden, zugangsdatenbasierten Risiken in zunehmend komplexen Authentifizierungsumgebungen konfrontiert. Die globale Studie von Keeper zeigt, dass 40 Prozent der Mitarbeitenden Passwörter für mehrere Konten wiederverwenden. Zudem berichten 67 Prozent der Unternehmen, dass Phishing trotz fortschrittlicherer Authentifizierungsmethoden eine dauerhafte Bedrohung bleibt. Für global agierende, kundenorientierte Organisationen, die auf gemeinsam genutzte Zugänge zu Drittanbieter-Plattformen angewiesen sind, machen diese Risiken eine starke Absicherung von Zugangsdaten und ein sicheres Credential Sharing zu kritischen operativen Anforderungen.

Der Keeper Enterprise Password Manager basiert auf der Zero-Trust- und Zero-Knowledge-Sicherheitsarchitektur von Keeper. Das bedeutet, dass alle Zugangsdaten Ende-zu-Ende verschlüsselt und weder Keeper noch unbefugten Dritten zugänglich sind. Die Plattform bietet starke Verschlüsselung, zentrale Verwaltung (Governance), sichere Optionen für das Teilen von Zugangsdaten sowie detaillierte Transparenz über deren Nutzung. So können Unternehmen ihre Angriffsfläche gegenüber zugangsdaten-basierten Attacken reduzieren und gleichzeitig die Produktivität aufrechterhalten. Mit der fortschreitenden Modernisierung der Authentifizierung unterstützt Keeper zudem Passkeys neben den klassischen

Zugangsdaten, sodass Teams die Zugriffssicherheit erhöhen können, ohne bestehende Workflows zu beeinträchtigen.

Für VaynerX war die Auswahl einer Passwortmanagement-Lösung nicht allein eine Frage der Sicherheit. Benutzerfreundlichkeit, zentrale Administration sowie eine nahtlose Integration in bestehende Tools und Prozesse waren entscheidend, um eine hohe Akzeptanz in der globalen Belegschaft zu erreichen.

„Die Entscheidung für Keeper fiel aufgrund der Funktionalität, der einfachen Bedienung und der Möglichkeit, das System zentral zu verwalten und so Sicherheitszugriffe auf Enterprise-Niveau umzusetzen“, sagt John Maalouf, SVP, Global Head of Procurement bei VaynerX. „Der Einstieg mit Keeper war unkompliziert. Wir erhielten direkt nach der Testphase Zugriff, und die Integration in die von uns genutzten Plattformen und Tools verlief sehr reibungslos.“

Branchenerhebungen unterstreichen, warum die Absicherung von Zugangsdaten inzwischen höchste Priorität hat. Studien zufolge sind mehr als 80 Prozent aller Datenschutzverletzungen auf schwache, wiederverwendete oder kompromittierte Passwörter zurückzuführen. Dies verdeutlicht die Bedeutung eines zentralisierten Credential Managements für Organisationen, die in großem Umfang auf gemeinsam genutzte Zugänge und Zusammenarbeit angewiesen sind.

„Zugangsdatenbezogene Bedrohungen zählen weiterhin zu den hartnäckigsten Risiken für Unternehmen“, erklärt Darren Guccione, CEO und Mitgründer von Keeper Security. „Die Erfahrungen von VaynerX mit Keeper dienen als praxisnaher Leitfaden und zeigen, wie Unternehmen ihr Passwortmanagement auf solider Grundlage stärken können – zum Schutz vor Zugriffen, zur Wahrung des Kundenvertrauens und zur Vorbereitung auf die Zukunft der Authentifizierung, ohne unnötige Komplexität zu schaffen.“

Die vollständige Case Study mit dem Titel „VaynerX führt Keeper unternehmensweit für seine globale Belegschaft ein“ bietet einen detaillierten Einblick, wie eine global tätige, kundenorientierte Organisation das Thema Zugangsdaten-Sicherheit erfolgreich und skalierbar umgesetzt hat.

###

Über Keeper Security:
Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware, das Tausende von Organisationen und Millionen von Menschen in über 150 Ländern schützt. Keeper ist ein Pionier der Zero-Knowledge- und Zero-Trust-Sicherheit für jede IT-Umgebung. Das Herzstück, KeeperPAM®, ist eine KI-fähige, Cloud-native Plattform, die alle Benutzer, Geräte und Infrastrukturen vor Cyberangriffen schützt. Keeper wurde für seine Innovationen im Gartner Magic Quadrant für Privileged Access Management (PAM) ausgezeichnet und sichert Passwörter und Passkeys, Infrastrukturgeheimnisse, Remote-Verbindungen und Endpunkte mit rollenbasierten Durchsetzungsrichtlinien, Least-Privilege und Just-in-Time-Zugriff. Erfahren Sie auf KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de