Pressemitteilung

Keeper Security führt unternehmensweite Genehmigungs-Governance und Echtzeit-Transparenz für das Endpoint-Privilegienmanagement ein

Neue Erweiterungen stärken Genehmigungs-Workflows, Audit-Durchsetzung und operative Kontrolle für Windows, macOS und Linux

MÜNCHEN – 16. April 2026 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Cybersicherheitssoftware zum Schutz von Passwörtern und Passkeys, Infrastruktur-Secrets, Remote-Verbindungen und Endpoints, stellt neue Governance-Funktionen für den Endpoint Privilege Manager (EPM) vor. Die Weiterentwicklung ermöglicht es der Plattform, die operativen und Compliance-Anforderungen großer und verteilter Organisationen besser zu erfüllen. Mit wachsender Reife des Endpoint-Berechtigungsmanagements erwarten Unternehmen zunehmend strukturierte Genehmigungsworkflows, durchsetzbare Ablaufkontrollen und eine klare Nachvollziehbarkeit der Audits über alle Umgebungen hinweg. Die neuesten Erweiterungen von Keeper bringen dieses Maß an Governance in den Endpoint Privilege Manager ein. Sie stärken damit die zentrale Kontrolle und bewahren die patentierte Zero-Trust-Sicherheitsarchitektur der Plattform.

Keeper EPM hilft Unternehmen dabei, das Prinzip der minimalen Rechtevergabe („Least Privilege“) durch richtliniengesteuerte, temporäre Berechtigungserweiterungen durchzusetzen und gleichzeitig das Zero-Trust- und Zero-Knowledge-Sicherheitsmodell von Keeper beizubehalten. Alle Berechtigungen bleiben lokal verschlüsselt und sind nur für autorisierte Administratoren innerhalb der Keeper Admin Konsole zugänglich.

Im Mittelpunkt des Updates steht das zentrale Genehmigungs-Framework innerhalb der Keeper Admin Console. Anfragen für Berechtigungserhöhungen werden nun global mit rollenbasierten Genehmigern, Eskalationswegen und konfigurierbaren Genehmigungszeitfenstern gesteuert. Durch Ablaufprüfungen und die Workflow-Durchsetzung werden überflüssige Berechtigungen reduziert und die Trennung der Aufgaben verbessert, was ideal für Organisationen mit formalen Compliance- und regulatorischen Anforderungen ist.

Keeper EPM bietet außerdem eine verbesserte Echtzeit-Transparenz über Aktivitäten zur Berechtigungserweiterung. Administratoren können Anfragen in dem Moment überwachen, in dem sie auftreten – inklusive klarerer Statusdifferenzierungen und erweiterten Audit-Protokollen, die durch Korrelationskennungen unterstützt werden. Diese Verbesserungen erhöhen die operative Transparenz und die Nachvollziehbarkeit bei Untersuchungen, ohne die Benutzerfreundlichkeit zu beeinträchtigen.

Die neue Version stärkt zudem die Serviceintegrität durch automatisierte Überwachungsfunktionen, die eine kontinuierliche Durchsetzung über verwaltete Endpunkte hinweg sicherstellen. In Kombination mit einer granularen Richtliniensteuerung erhalten Unternehmen eine präzisere Kontrolle darüber, wie Privilegien über Windows-, macOS- und Linux-Systeme hinweg vergeben und überwacht werden. Indem sichergestellt wird, dass administrative Rechte bewusst vergeben, zeitlich begrenzt und vollständig für

Sicherheitsteams sichtbar sind, reduziert Keeper EPM das Risiko von Missbrauch. Zudem erleichtert es Administratoren die Nachverfolgung und Verwaltung erweiterter Zugriffsrechte über alle Endpoints hinweg.

„Privilegienmanagement ist am effektivsten, wenn Governance in jeder Berechtigungserweiterung integriert ist“, sagt Craig Lurey, CTO und Mitgründer von Keeper Security. „Sicherheitsteams benötigen strukturierte Genehmigungspfade, strikte Zeitkontrollen und sofortige Transparenz darüber, was auf ihren Endpunkten passiert. Die Verbesserungen des Keeper Endpoint Privilege Managers stärken diese Kontrollschicht. Berechtigungserweiterungen werden gezielt, begrenzt und vollständig auditierbar. So reduziert man dauerhafte Privilegien und kann auf Unternehmensebene sicher und effizient arbeiten.“

Keeper EPM ist eine governance-fähige Lösung für Unternehmen, die sowohl die Durchsetzung minimaler Rechtevergabe als auch operative Verantwortlichkeit innerhalb einer einheitlichen PAM-Plattform anstreben.

Weitere Informationen oder die Anfrage einer Demo finden Sie unter KeeperSecurity.com.

###

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-unterstützte, 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.

Erfahren Sie mehr unter KeeperSecurity.com
Folgen Keeper: 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