Pressemitteilung

Keeper Security erweitert Zero-Trust-Kontrolle für privilegierten Zugriff auf Slack

Neue Integration unterstreicht Keepers Strategie, Sicherheitskontrollen nahtlos in bestehende Systeme einzubetten – ohne Abstriche bei Zero-Knowledge- oder Least-Privilege-Prinzipien

MÜNCHEN, 26. 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, kündigt seine Slack-Integration an. Damit erweitert Keeper die sichere, richtlinienbasierte Zugriffskontrolle auf eine der weltweit meistgenutzten Kollaborationsplattformen.

Slack wird in Unternehmen aller Größen als zentrales Kollaborationswerkzeug eingesetzt. Da Teams die Messaging-Kanäle zunehmend auch für Genehmigungen, Incident Response und die tägliche Abstimmung nutzen, ist Slack zu einem zentralen Ort geworden, an dem operative Entscheidungen getroffen und umgesetzt werden. Da Tausende Integrationen von Drittanbietern die Slack-basierten Arbeitsabläufe unterstützen, hat sich die Plattform zu einem primären Arbeitsbereich für die operative Koordination entwickelt und damit zu einem natürlichen Ort für die Einführung von Zugriffskontrollen mit zentralisierter Durchsetzung.

Die Integration ermöglicht es Unternehmen, Zugriffe auf Ressourcen im Keeper Vault – etwa auf gemeinsam genutzte Ordner, Service Accounts, Zugangsdaten und geschützte Anwendungen – direkt in Slack zu beantragen und zu genehmigen. Keeper bleibt dabei das führende System für die Durchsetzung, Verschlüsselung, Auditierung und Compliance. Sowohl die Slack-App als auch die Container der Keeper-Commander-Anwendung werden beim Kunden selbst betrieben. Dadurch bleibt die Zero-Knowledge-Architektur von Keeper gewahrt und der Kunde behält die vollständige Kontrolle über die Ver- und Entschlüsselung seiner Daten.

„Sicherheit gerät immer dann ins Wanken, wenn Anwender gezwungen sind, kontrollierte Umgebungen zu verlassen“, erklärt Craig Lurey, CTO und Mitgründer von Keeper Security. „Wir haben diese Integration so konzipiert, dass Slack als Workflow-Oberfläche fungiert und nicht als Sicherheitsgrenze. Slack ist der Ort, an dem gearbeitet wird. Keeper ist der Ort, an dem Zugriffe durchgesetzt werden. Diese klare Trennung ermöglicht es Unternehmen, schneller zu agieren, ohne neue Risiken zu schaffen.“

Viele Workflow-Integrationen verwischen aus Gründen der Bequemlichkeit sicherheitsrelevante Grenzen. Keeper verfolgt einen anderen Ansatz und hat die Integration mit klarer Aufgabenverteilung aufgebaut: Workflow-Plattformen stoßen Anfragen und Genehmigungen an, während ausschließlich Keeper die Zugriffsregeln und kryptografischen Kontrollen durchsetzt. Dieses Modell bewahrt die nötige Sicherheit für Unternehmen, ohne dass Teams gezwungen sind, außerhalb ihrer bestehenden Arbeitsabläufe zu arbeiten.

Durch die Integration von Zugriffsgenehmigungen in eine etablierte Kollaborationsumgebung können Unternehmen unsichere Nebenkanäle wie E-Mail-Threads, Direktnachrichten oder Screenshots eliminieren und gleichzeitig strenge Zugriffsrichtlinien mit minimalen

Berechtigungen sowie eine zentralisierte Governance in Cloud-, Hybrid- und lokalen Umgebungen aufrechterhalten.

Mit dieser Funktionalität lassen sich Prozesse der Zugriffsregelungen deutlich verschlanken, ohne die Kontrolle zu verlieren. Anfragen werden in Slack initiiert und automatisch auf Basis von Keeper-Richtlinien an die zuständigen Genehmiger weitergeleitet. Zugriffe werden Just-in-Time (JIT) und ohne dauerhafte Berechtigungen gewährt. Jede Anfrage, Genehmigung und jeder Zugriff wird zentral protokolliert, um Audit- und Compliance-Anforderungen zu erfüllen.

Die Slack-Integration ist Teil von Keepers übergreifender Plattformstrategie, um Zero-Trust-Zugriffskontrolle in genau jene Arbeitssysteme auszuweiten, in denen Entscheidungen ohnehin getroffen werden – ohne Sicherheitskontrollen zu fragmentieren oder neue Angriffsflächen zu schaffen. Dieser Ansatz ermöglicht es Unternehmen, Zugriffs-Workflows zu modernisieren und gleichzeitig eine zentrale, konsistente und revisionssichere Durchsetzung beizubehalten.

„Mit der zunehmenden Verbreitung kollaborativer und verteilter Arbeitsmodelle muss sich Sicherheit weiterentwickeln, ohne an Autorität einzubüßen“, ergänzt Lurey. „Diese neue Integration spiegelt Keepers langfristige Sichtweise wider, Zugriffskontrolle als umfassende Plattformfähigkeit zu verstehen und nicht als isolierte Einzelintegration.“

Die Keeper-Slack-Integration ist ab sofort für Kunden von Keeper verfügbar. Weitere Informationen 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-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