Pressemitteilung

Keeper Security bringt native Google Cloud-Unterstützung für KeeperPAM für einheitliches, Multi-Cloud-Privileged-Access-Management

Die native Integration erweitert die Zero-Trust-Identitätssicherheit und das Privileged-Access-Management (PAM) über Google Cloud, AWS und Microsoft Azure hinweg.

MÜNCHEN, 18. Februar 2026 – Keeper Security, eine führende Plattform für Zero-Trust- und Zero-Knowledge-Identitätssicherheit sowie Privileged-Access-Management (PAM), gibt heute erweiterte PAM-Funktionen für Google Cloud Platform (GCP)-Umgebungen bekannt. Die neuesten Weiterentwicklungen von KeeperPAM ermöglichen es Unternehmen, privilegierten Zugriff zentral zu verwalten und zu überwachen sowie privilegierte Anmeldedaten für Google Cloud-Infrastrukturen und Google Workspace-Identitäten zu rotieren. Damit adressieren die Erweiterungen eine der hartnäckigsten Sicherheitslücken in modernen Cloud-Umgebungen.

Da Unternehmen die Nutzung der Cloud-Nutzung ausweiten, sind identitätsbasierte Angriffe zu einer der Hauptursachen für Datenschutzverletzungen geworden. Dieses Risiko wird durch KI-gestützte Automatisierung verstärkt, da sie die Anzahl und Privilegien von Nicht-Menschlichen Identitäten (NHIs) in Cloud-Umgebungen dramatisch erhöht. In Google Cloud-Umgebungen ist privilegierter Zugriff oft fragmentiert und umfasst sowohl nicht-menschliche Identitäten wie Service-Konten und Automatisierungen als auch menschliche Identitäten, die in IAM-Richtlinien eingebettet sind. Diese Konten sind häufig überprivilegiert und die Anmeldedaten werden nicht rotiert. Das erhöht die Angriffsfläche für Identitätsattacken und erweitert zudem den Schadensradius bei einer Kompromittierung.

KeeperPAM schließt diese Lücke, indem es identitätsbasiertes, cloud-natives PAM für Google Cloud bereitstellt sowie Infrastruktur-, SaaS- und NHI-Sicherheit in einer einzigen Zero-Trust-Plattform vereint.

„Sicherheitsvorfälle in der Cloud entstehen selten durch eine einzelne Fehlkonfiguration. Sie entstehen durch unkontrollierte Identitätsvermehrung“, sagt Darren Guccione, CEO und Mitgründer von Keeper Security. „Mit KeeperPAM können Unternehmen Zero-Trust-Prinzipien konsistent auf Google Cloud-Infrastrukturen und Google Workspace-Identitäten anwenden, das Prinzip der geringsten Privilegien durchsetzen und dauerhaften Zugriff ohne zusätzliche Komplexität eliminieren.“

Vereinheitlichung von Infrastruktur- und Identitätssicherheit in Google Cloud

KeeperPAM integriert sich in Google Cloud über ein dediziertes Service-Konto und ein schlankes Keeper Gateway, das ausgehende, agentenlose Zugriffe ermöglicht – im Einklang mit der Zero-Trust-Architektur. Die Plattform erkennt automatisch GCP-Ressourcen und identifiziert privilegierte Identitäten, die in IAM-Richtlinien referenziert sind, einschließlich Google Workspace-Nutzern.

Kernfunktionen umfassen:

- **Einheitliches Privileged-Access-Management für GCP und Google Workspace:** Sichere und zentrale Verwaltung von Infrastruktur-Anmeldedaten und menschlichen Identitäten auf einer einzigen Plattform.
- **Automatisierte Rotation von Anmeldedaten:** Rotation von Passwörtern für Google Workspace-Nutzer und Cloud-Service-Konten, um dauerhafte Privilegien zu eliminieren.
- **Durchsetzung des Prinzips der geringsten Privilegien:** Unterstützung von benutzerdefinierten IAM-Rollen mit minimalen Berechtigungen reduziert übermäßige Privilegien und begrenzt den Schadensradius bei einem Sicherheitsvorfall.
- **Zero-Knowledge-Schutz für Cloud-Anmeldedaten:** Service-Konto-Schlüssel und privilegierte Anmeldedaten werden verschlüsselt im Keeper Vault gespeichert und sind für Nutzer oder Endpunkte nie sichtbar.
- **Audit-fähige Transparenz und Compliance:** Zentralisierte Protokollierung und Berichterstattung vereinfachen Audits und unterstützen regulatorische Anforderungen in Cloud-Umgebungen.

Entwickelt für moderne Cloud-, Multi-Cloud- und Hybrid-Umgebungen
Im Gegensatz zu veralteten PAM-Lösungen, die für lokale Infrastrukturen entwickelt wurden, ist KeeperPAM cloud-nativ und speziell für Cloud-, Multi-Cloud- und Hybrid-Umgebungen konzipiert. Die Plattform erfordert keine Änderungen an inbound Firewall-Regeln, keine Bastions-Hosts und keine Agenten. Damit können Unternehmen Google Cloud-Umgebungen absichern, ohne in bestehende Architekturen oder Workflows eingreifen zu müssen. Die Funktionen erweitern die einheitlichen privilegierten Zugriffskontrollen von KeeperPAM konsistent über Google Cloud, AWS und Microsoft Azure hinweg.

„Die meisten PAM-Tools wurden nie dafür entwickelt, Cloud-Identitäten im großen Stil zu verwalten – insbesondere menschliche Identitäten, die in SaaS-Plattformen wie Google Workspace eingebettet sind“, sagt Craig Lurey, CTO und Mitgründer von Keeper Security. „KeeperPAM spiegelt die Funktionsweise heutiger Cloud-Umgebungen wider und bietet praktische Kontrollen für das Prinzip der geringsten Privilegien, automatisierte Rotation und Transparenz über Identitäten, die zunehmend von Angreifern ins Visier genommen werden.“

Reduzierung der Auswirkungen von Sicherheitsverletzungen durch Zero Trust
Durch die Beseitigung von dauerhaftem Zugriff mit Hilfe der Durchsetzung einer kontinuierlichen Überprüfung hilft KeeperPAM Unternehmen dabei, die Auswirkungen von kompromittierten Anmeldedaten zu reduzieren. Die Plattform unterstützt ein Zero-Trust-Sicherheitsmodell, das laterale Bewegungen einschränkt und das Risikofenster bei Missbrauch von Anmeldedaten verkürzt.

Die neuen Google Cloud-Funktionen sind ab sofort Teil der KeeperPAM-Plattform. Die vollständige technische Dokumentation ist unter docs.keeper.io verfügbar.

###

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.

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