Keeper Connection Manager: Neue Funktionen für den Next-Gen Zero-Trust-Netzwerkzugriff

München, 17. Januar 2023 – Keeper Security, führender Anbieter von Zero-Trust- und Zero-Knowledge-Cyber-Security-Lösungen zum Schutz von Passwörtern, Daten und Verbindungen, kündigte heute das neueste Update seines Keeper Connection Manager (KCM) an. Dieses ermöglicht DevOps- und IT-Teams jetzt den unmittelbaren Zugriff auf RDP-, SSH-, Datenbank- und Kubernetes-Endpunkte über einen Webbrowser, so dass keine VPN-Verbindung mehr erforderlich ist. Der Keeper Connection Manager 2.11.0 ist in der Lage, direkt mit Microsoft SQL Server- und PostgreSQL-Datenbanken zu interagieren.

Dank dieser neuen Funktionalität können Unternehmen ihren Administratoren genau den Zugriff auf Datenbanken und Tabellen gewähren, den sie zum Ausführen ihrer Aufgaben benötigen. Für einen temporären Zugriff bietet der Keeper Connection Manager eine schnelle und einfache Lösung - anders als das bei der Installation clientseitiger Software der Fall ist. Die Administratoren müssen nur einen Browser öffnen und sich anmelden, um Zugriff auf das zu erhalten, was sie benötigen. Gleichzeitig wird alles, was sie nicht brauchen, vor einem Zugriff geschützt. Interaktive Datenbanksitzungen können aufgezeichnet und überwacht werden. Das schützt einerseits vor Insider-Bedrohungen und ermöglicht den Administratoren dennoch eine umfassende Überwachung.

Keeper Connection Manager ist ein Agenten- und Client-loses Remote Desktop Gateway, das in jeder lokalen oder Cloud-Umgebung installiert werden kann. Neben PostgreSQL-, Microsoft SQL Server- und MySQL-Datenbanken unterstützt Keeper Connection Manager auch die Verbindung zu RDP-, SSH-, VNC-Servern und Kubernetes-Pods. Zu den weiteren Kernfunktionen der Lösung gehören Sitzungsaufzeichnungen und detaillierte Audit-Trails, die gemeinsame Nutzung von Sitzungen mit mehreren Benutzern, rollenbasierte Zugriffskontrollen, Zwei-Faktor-Authentifizierung, Active Directory, SSO- und LDAP-Integration sowie ein benutzerdefiniertes Branding. Der Keeper Connection Manager baut auf Apache Guacamole auf.

IT- und DevOps-Teams entscheiden sich für den Keeper Connection Manager wegen der erweiterten Funktionen, des sofortigen Zugriffs, die reduzierten Supportkosten und um durch sicheren, temporären und überwachten Zugriff auf autorisierte Geräte und Maschinen das Sicherheitsrisiko für Drittanbieter und Auftragnehmer zu minimieren. Keeper-Kunden können den Keeper Connection Manager sofort in Keeper Secrets Manager (KSM) integrieren, um Anmeldeinformationen für Verbindungen zu privilegierten Systemen im Keeper Vault zu verwalten. Keeper Connection Manager kann IT- und DevOps-Teams zudem bei der Einhaltung von SOC2, SOX, HIPAA, DSGVO, FINRA, FedRAMP, StateRAMP unterstützen und helfen andere branchenspezifische Vorschriften einzuhalten.

Über Keeper Security Inc.
Keeper Security verändert die Art und Weise, wie Menschen und Organisationen auf der ganzen Welt ihre Passwörter, Geheimnisse und vertraulichen Informationen schützen. Die benutzerfreundliche Cybersecurity-Plattform von Keeper basiert auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer und jedes Gerät zu schützen. Die Lösung ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in die Systemumgebung integrieren, um Datenschutzverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Einhaltung von Vorschriften zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelpersonen und Tausenden von Unternehmen auf der ganzen Welt und ist der führende Anbieter von erstklassigem Passwortmanagement, Geheimnismanagement, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Schützen Sie was wichtig ist, auf KeeperSecurity.com.

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
a.schmidt@tc-communications.de
Thilo Christ, +49 171 622 06 10
thilo.christ@tc-communications.de
oder
keeper@eskenzipr.com