KEEPER®
CONNECTION MANAGER

Datenblatt: Fernzugriff für DevOps und IT-Teams

Sofortzugriff mit Zero-Trust-Sicherheit auf Ihre Remote-Infrastruktur

Der Keeper Connection Manager bietet DevOps- und IT-Teams die Möglichkeit, über den Browser den sicheren und unkomplizierten Zugriff auf RDP, SSH- und Kubernetes-Endpunkte zu erlauben.

Der sichere und einfache Zugriff auf die gesamte interne Infrastruktur war schon immer eine Herausforderung. Der Zugriff wird normalerweise nur einmal auf ein System gewährt und ist dann nie wieder ein Thema. Im Laufe der Zeit kommen jedoch immer mehr Zugriffsberechtigte hinzu, bis schließlich nicht mehr ganz so leicht nachvollziehbar ist, wie viele Personen eigentlich Zugriff auf diese kritischen Systeme haben.

Sobald Änderungen am Zugriff vorgenommen werden müssen oder der Zugriff überprüft werden muss, ist das immer ein gehöriger Kraftakt. Wenn etwas schiefgeht, lässt sich im Nachhinein oft nicht mehr nachvollziehen, was genau an einem System verändert wurde.

Einige Anbieter versuchen dieses Problem mit Agents, Clients, verteilten Bastion-Servern oder einer Kombination dergleichen zu lösen. Diese Ansätze haben jedoch den Nachteil, dass die Systemkomplexität zunimmt, die Sicherheit Schaden nimmt und die breite Akzeptanz darunter leidet.

Keeper Connection Manager löst das Komplexitäts- und Sicherheitsdilemma mit einer modernen Lösung ohne Agents. Sie bietet das Maß an Sicherheit, Benutzerfreundlichkeit und Geschwindigkeit, das in den heutigen Homeoffice-Umgebungen vonnöten ist.

Welche Vorteile bietet Ihnen Keeper Connection Manager für Ihre IT- und DevOps-Teams?

- Schnelle Integration mit Keeper Secrets Manager. Verwaltung von Zugangsdaten für Verbindungen zu privilegierten Systemen im Keeper Tresor.
- Passwortlose Authentifizierung bei Remote-Servern über alle gängigen Authentifizierungslösungen mit oder ohne IdP-Lösung.
- Sofortiger Zugriff auf die Konsolensitzung Ihrer privilegierten Systeme. Geräte müssen nicht vor Ort integriert werden, wodurch Supportkosten gesenkt werden.
- Um SOX, HIPAA, GDPR, FINRA und andere branchenspezifische Vorschriften einzuhalten, können Administratoren privilegierte Sitzungen aufzeichnen und detaillierte Protokolle führen.
- Hochmoderne, erweiterte Funktionen unterstützen Multi-User-Zugriff, Multi-Sitzungsfreigabe, mehrere offene Sitzungen und schnelles Wechseln zwischen Sitzungen.
- Der Zugriff auf vertrauliche Systeme kann vollständig gesperrt werden, um sicherzustellen, dass keine unbekannten oder unbefugten Zugangspunkte vorhanden sind.
- Mindern und reduzieren Sie das Risiko für Drittanbieter und Auftragnehmer durch sicheren, temporären und überwachten Zugriff auf autorisierte Geräte und Rechner.

KEEPER
CONNECTION MANAGER

Datenblatt
Remote-Zugriff für DevOps und IT-Teams

Eine schnelle, einfache und sichere Verbindung zu Ihrer Remote-Infrastruktur. Unterstützt durch Zero-Trust-, Zero-Knowledge-Sicherheit und erstklassigen Support.

Was macht den Keeper Connection Manager so viel sicherer als herkömmliche Remote-Desktop-Lösungen?

- Der gesamte Datenverkehr wird über ein sicheres, authentifiziertes Gateway geleitet. Die Remote-Sitzung wird niemals dem öffentlichen Internet ausgesetzt.
- Gemäß den Zero-Trust-Prinzipien sind nur autorisierte, authentifizierte Verbindungen zulässig.
- Alle Remote-Funktionen werden hinter der Unternehmens-Firewall ausgeführt. Homeoffice-Benutzer genießen den gleichen Schutz, als würden sie in einem Büro im Unternehmensnetzwerk arbeiten.
- Client-Zertifikate und mehrstufige Authentifizierungen können für noch mehr Sicherheit erzwungen werden.
- Keeper Connection Manager wurde entwickelt, um nach dem Prinzip der geringsten Berechtigung zu arbeiten. Zugriffsrechte werden sorgfältig durch Benutzer und Gruppen delegiert, die automatisch von den Keeper Connection Manager-Paketen und durch strenge Dateiberechtigungen erstellt werden.
- Endbenutzer kommunizieren mit Remote-Desktops über eine sichere Sitzung von ihrem Browser aus. Dies ist eine einfache und effektive Möglichkeit, um den Datenverkehr zwischen Endbenutzern und dem Gateway zu verschlüsseln, ohne dabei Abstriche bei der Leistung in Kauf nehmen zu müssen.
- Der Zugriff auf privilegierte Systeme kann gewährt werden, ohne dass dem Endbenutzer die Zugangsdaten offengelegt werden.
- Funktioniert mit RDP-, SSH-, VNC-, K8s- und MySQL-Endpunkten.

Anwendungsszenarien	Keeper Connection Manager
Webbasierter Zugriff	✓
Mehr-Stufen-Authentifizierung	✓
Agentunabhängiger Zugriff	✓
Mehrere Datenspeicher	✓
Zero-Knowledge-Sicherheit	✓
Zero-Trust-Framework	✓
Sitzungsaufzeichnung	✓
Passwortlose Authentifizierung	✓
Unterstützung mehrerer Protokolle	✓
Integration mit Keeper Secrets Manager	✓

Über Keeper Security, Inc.

Keeper Security, Inc. (Keeper) ist die führende Lösung zum Schutz vor passwortbezogenen Datenpannen und Cyberbedrohungen. Auf die Zero-Trust-, Zero-Knowledge-Sicherheit und Verschlüsselungssoftware von Keeper vertrauen Millionen von Menschen und Tausende von Unternehmen aus aller Welt. Keeper wurde vom PC Magazine zum besten Passwort-Manager des Jahres und Editors' Choice ernannt. Von PCWorld wurde es ebenfalls zum Editors' Choice gewählt. Außerdem hat Keeper mehrere G2 Best Software Awards erhalten. Keeper ist nach SOC-2 und ISO 27001 zertifiziert und wird über das System for Award Management (SAM) auch von der US-Regierung verwendet. Nähere Informationen unter **https://keepersecurity.com**.