

Keeper Connection Manager (KCM)

Bietet agentenlosen, clientlosen und sicheren Fernzugriff auf RDP-, SSH-, Datenbank- und Kubernetes-Endgeräte über einen Webbrowser.

Herausforderungen

Unternehmen jeder Größe müssen einen sicheren und zuverlässigen Zugriff auf ihre IT-Infrastruktur, Datenbanken und Backend-Websites gewährleisten. Veraltete Remote-Zugriffslösungen führen jedoch häufig zu eingeschränkter Skalierbarkeit, hohem Verwaltungsaufwand, Frustration bei den Endbenutzern und gravierenden Sicherheitslücken.

1. Virtuelle private Netzwerke (VPNs) bieten in der Regel zu viel Zugriff, insbesondere für Vertragspartner, Lieferanten und gelegentlich eingesetzte Mitarbeitende.
2. VPNs schützen nicht vor Cookie-Tracking, Viren oder anderer Malware.
3. VPNs sind teuer und für das IT-Personal bekanntermaßen schwierig zu konfigurieren und zu warten, und auch für die Endbenutzer ist die Nutzung schwierig.
4. Einige Lösungen beruhen auf Kombinationen von Agenten, Clients und verteilten Bastion-Servern, was die Systemkomplexität erhöht und die Benutzerakzeptanz beeinträchtigt.

Mitarbeitende müssen von überall aus sichere, zuverlässige und benutzerfreundliche Remote-Verbindungen aufbauen können, um das Risiko eines unbefugten Zugriffs auf sensible Daten zu minimieren.

Lösung

Keeper Connection Manager löst das Komplexitäts- und Sicherheitsdilemma mit einer modernen, agentenlosen Lösung, die die Sicherheit, Benutzerfreundlichkeit und Geschwindigkeit bietet, die in den heutigen verteilten Remote-Arbeitsumgebungen erforderlich sind.

Der Keeper Connection Manager ist nach dem Prinzip der geringsten Privilegien konzipiert. Die Zugriffsrechte werden über Benutzer und Gruppen delegiert, die automatisch von den Paketen des Keeper Connection Managers und durch strenge Dateiberechtigungen erstellt werden.

Der gesamte Datenverkehr läuft über ein sicheres, authentifiziertes Gateway. Die Desktops sind nie dem öffentlichen Internet ausgesetzt. Gemäß den Zero-Trust-Prinzipien werden nur autorisierte und authentifizierte Verbindungen zugelassen.

Über Keeper Security

Keeper Security verändert die Cybersicherheit für Menschen und Unternehmen auf der ganzen Welt.

Die erschwinglichen und benutzerfreundlichen Cybersicherheitslösungen von Keeper basieren auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer auf jedem Gerät zu schützen. Millionen von Einzelpersonen und Tausende von Unternehmen verlassen sich auf Keeper, wenn es um die erstklassige Verwaltung von Passwörtern, Passkeys und Geheimnissen, Privileged Access Management (PAM), sicheren Fernzugriff und verschlüsselte Nachrichten geht. Unsere Cybersicherheitsplattform der nächsten Generation ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in jeden Technologie-Stack integrieren, um Datenschutzverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Compliance zu gewährleisten.

Keeper Security wird von den führenden Private-Equity-Firmen Insight Partner und Summit Partner unterstützt.

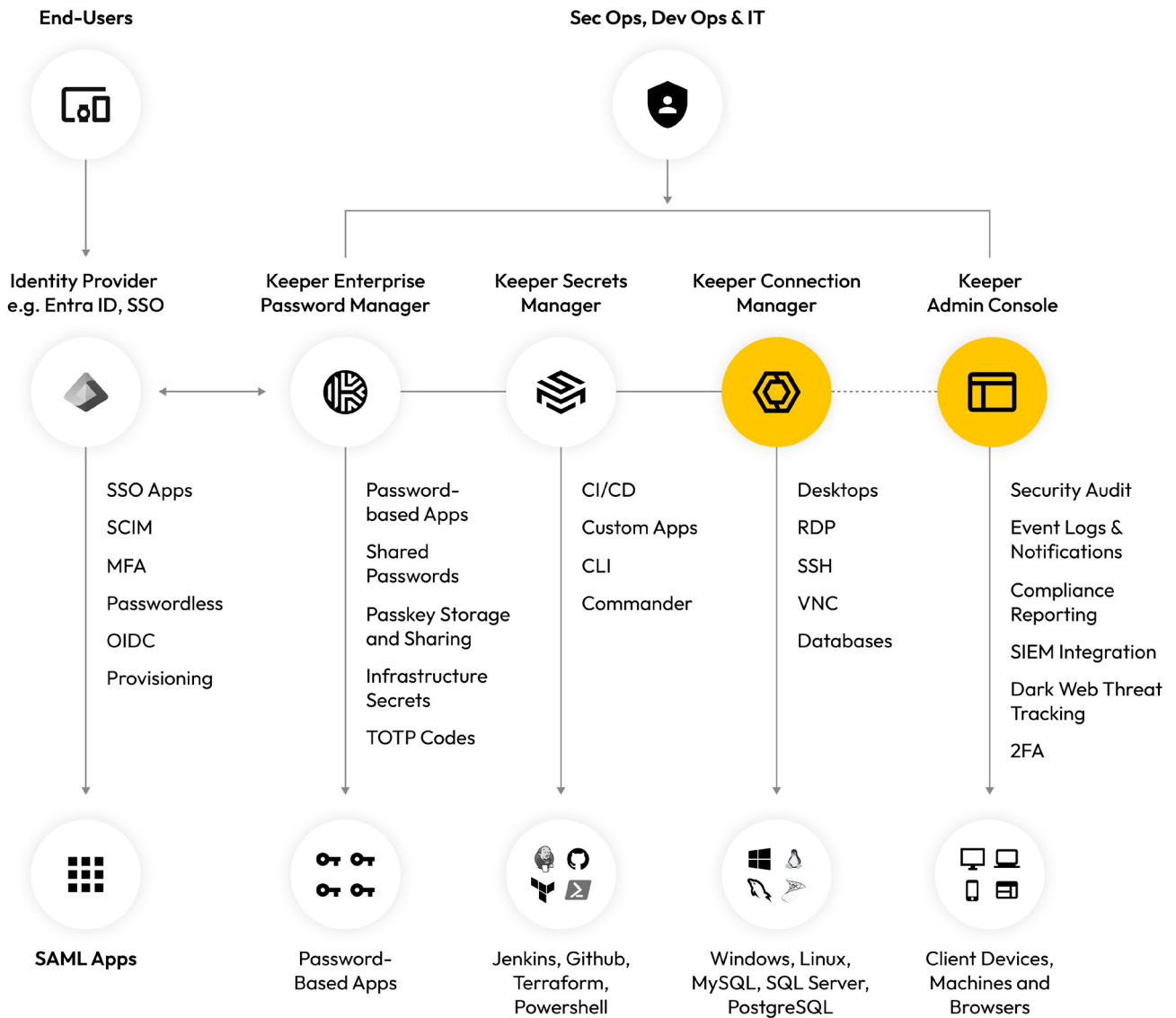
Keeper Security
Vermeiden Sie Hackerangriffe.

Mehr erfahren
keepersecurity.com

Starten Sie noch heute eine kostenlose Testversion
keepersecurity.com/start-business-trial.html



Keeper Privileged Access Management Platform



Geschäftswert

Remote-Browser-Isolierung

Begrenzen Sie Cybersicherheitsbedrohungen, indem Sie Browsing-Sitzungen in einer kontrollierten Remote-Umgebung hosten.

Fernzugriff auf Datenbanken

Schützen Sie proprietäre Daten und PII mit sicherem Fernzugriff auf Datenbanken.

Sicherer Fernzugriff auf die Infrastruktur

Stellen Sie von überall aus sichere Remote-Verbindungen her, ohne Anmeldeinformationen preiszugeben

Privileged Account Session Management

Erfüllen Sie Compliance-Anforderungen mit geprüften und aufgezeichneten Sitzungen.

Key Capabilities

- Webbasierter Zugriff mit End-to-End-Verschlüsselung
- Multifaktor-Authentifizierung
- Agentenloser Zugriff (kein VPN erforderlich)
- Mehrere Datenspeicher
- Zero-Knowledge-Sicherheit
- Zero-Trust-Framework
- Richtlinien-Engine für Rollenbasierte Zugriffskontrolle (RBAC)
- Ereignisüberwachung und Sitzungsaufzeichnung
- Passwortlose Authentifizierung
- Multiprotokoll-Unterstützung
- Integration mit Keeper Secrets Manager