Datenblatt

KEEPER CONNECTION MANAGER

Einrichtung von privilegierten Sitzungen in der Cloud und vor Ort, Erstellen von Tunneln, Zugriff auf eine Zero-Trust-Infrastruktur und sicherer Remote-Datenbankzugriff ohne VPN.

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.

01

Virtuelle private Netzwerke (VPNs) bieten in der Regel zu viel Zugriff, insbesondere für Vertragspartner, Lieferanten und gelegentlich eingesetzte Mitarbeitende.

02

VPNs schützen nicht vor Cookie-Tracking, Viren oder anderer Malware, sodass Unternehmen einem steigenden Risiko ausgesetzt sind.

03

VPNs sind teuer und bekanntermaßen schwierig zu konfigurieren, zu warten und zu nutzen, was sowohl Administratoren als auch Benutzer frustriert.

04

Einige Lösungen beruhen auf Kombinationen von Agenten, Clients und verteilten Bastion-Servern, was die Systemkomplexität erhöht und die Benutzerakzeptanz verlangsamt.

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 agentenlosen Lösung, die die Sicherheit, Einfachheit und Geschwindigkeit bietet, die in den heutigen 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.

Halten Sie sich Hacker vom Leib!

Mehr erfahren
keepersecurity.com

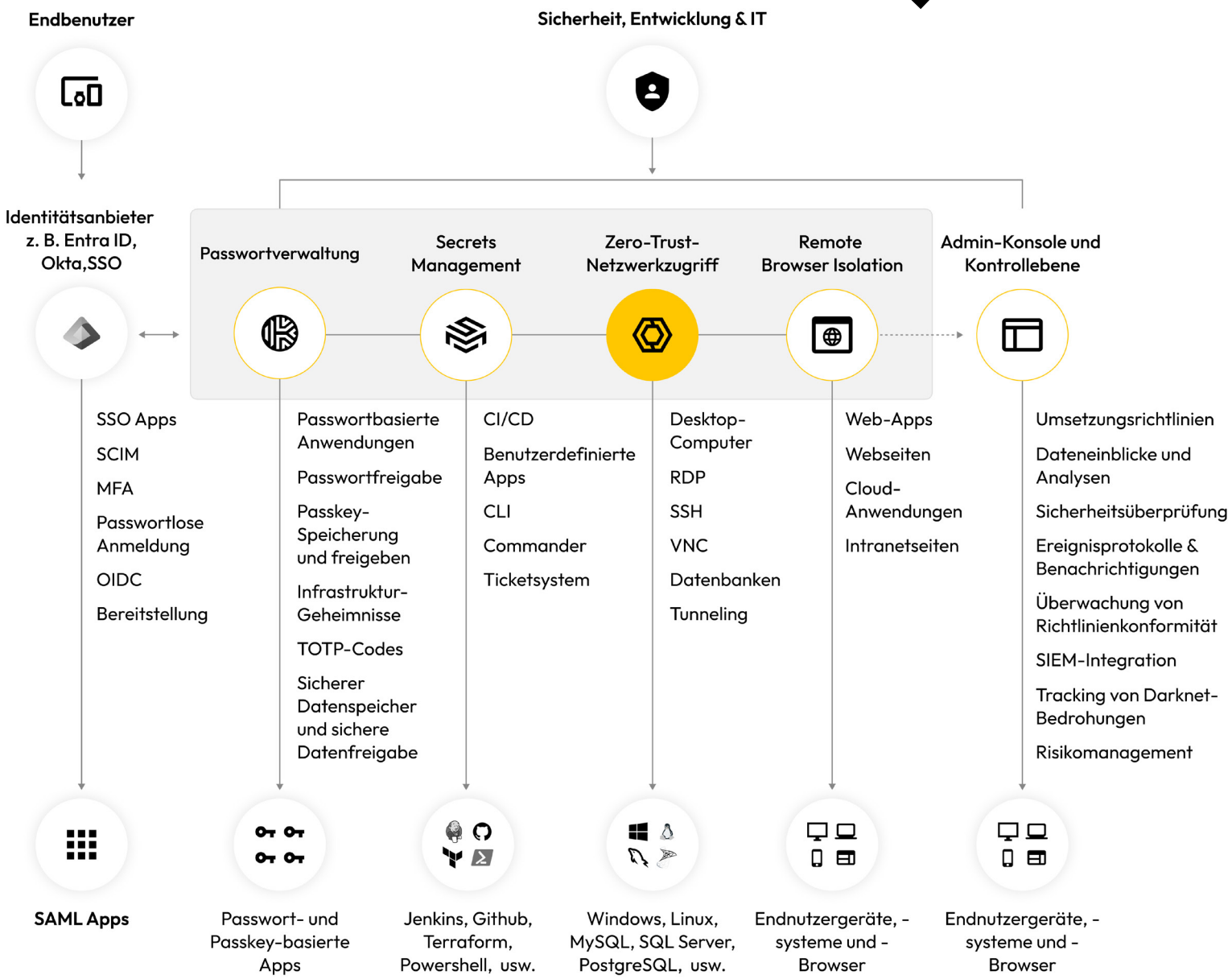
Starten Sie eine kostenlose Testversion
keeper.io/kcm

Über uns

Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die intuitiven Lösungen von Keeper basieren auf einer End-to-End-Verschlüsselung, um jeden Anwender auf jedem Gerät und an jedem Standort zu schützen. Keeper genießt das Vertrauen von Millionen von Einzelnutzern und Tausenden von Unternehmen und ist führend bei der Verwaltung von Passwörtern, Passkeys und Geheimnissen, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging.

KEEPER CONNECTION MANAGER

Keeper Privileged Access Management-Plattform



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 sichere Remote-Verbindungen für alle Benutzer her, egal ob intern oder extern, und zwar von jedem beliebigen Ort aus, ohne Anmeldeinformationen preiszugeben.

Privileged Account Session Management
Erfüllen Sie Compliance-Anforderungen mit geprüften und aufgezeichneten Sitzungen.

Wichtige Funktionen

- Webbasierter Zugriff mit End-to-End-Verschlüsselung
- Multifaktor-Authentifizierung
- Agentenloses Zugriff (kein VPN erforderlich)
- Zero-Knowledge-Sicherheit
- Zero-Trust-Framework
- Rollenbasierte Zugriffskontrolle (RBAC) – Richtlinien-Engine
- Ereignisüberwachung und Sitzungsaufzeichnung
- Multiprotokoll-Support
- Remote-Browser-Isolierung
- Integration mit Keeper Secrets Manager