Datenblatt

Enterprise Password Manager

Verhindern Sie Sicherheitsverletzungen, reduzieren Sie die Helpdesk-Kosten und stellen Sie die Compliance sicher.

Herausforderungen

Schwache und gestohlene Passwörter, Anmeldeinformationen und DevOps-Geheimnisse sind eine der Hauptursachen für Datenschutzverletzungen. Den meisten Unternehmen fehlt der Überblick über diese Bedrohungen. Sie haben keine Möglichkeit, Best Practices für die Sicherheit bei allen Mitarbeitenden, an allen Standorten, auf allen Geräten, Anwendungen und Systemen durchzusetzen. Dadurch entstehen eine Reihe von Herausforderungen für IT-Admins:

01

Unternehmen werden immer komplexer und bestehen aus menschlichen und maschinellen Anmeldeinformationen, die geschützt werden müssen.

02

Moderne Arbeitsweisen mit verteilter Remote-Arbeit und Multi-Cloud-Computing haben die traditionellen IT-Perimeter obsolet gemacht, was das Risiko für alle erhöht.

03

Die Angriffsflächen nehmen exponentiell zu, da Milliarden zusätzlicher Geräte, Anmeldeinformationen und Geheimnisse mit verteilten Netzwerken verbunden sind – sowohl innerhalb des Unternehmens als auch an anderen Geschäftsstandorten.

04

Herkömmliche Cybersicherheitslösungen sind von Natur aus voneinander abgeschottet, wodurch was zu kritischen Lücken in Bezug auf Transparenz, Sicherheit, Kontrolle, Compliance und Berichterstattung führt.

Unternehmen, die sich diesen zentralen Herausforderungen nicht stellen, sehen sich einem erhöhten Risiko von Datenschutzverletzungen, Compliance-Verstößen und betrieblichen Reibungen gegenüber.

Lösung

Keeper Enterprise Password Manager überwacht und schützt jeden Benutzer auf jedem Gerät im gesamten Unternehmen mit vollständigen Cloud- und nativen Anwendungsfunktionen. Keeper lässt sich nahtlos in bestehende IT-Technologie integrieren, einschließlich Security Information and Event Management (SIEM), Multifaktor-Authentifizierung (MFA), passwortlose und Identitätsanbieter (IdP)-Lösungen.

Keeper bietet umfassende Authentifizierung und Verschlüsselung für jede Website, jede Anwendung und jedes System, mit dem Mitarbeitende interagieren. Die Plattform ist einfach zu implementieren, auch für technisch nicht versierte Benutzer leicht zu übernehmen und das sicherste Produkt seiner Art. Keeper verfügt über die branchenweit längste SOC 2 Typ I- und II-Compliance und ist nach ISO 27001, 27017 und 27018 zertifiziert sowie FedRAMP- und StateRAMP-autorisiert.

Halten Sie sich Hacker vom Leib!

Mehr erfahren
keepersecurity.com

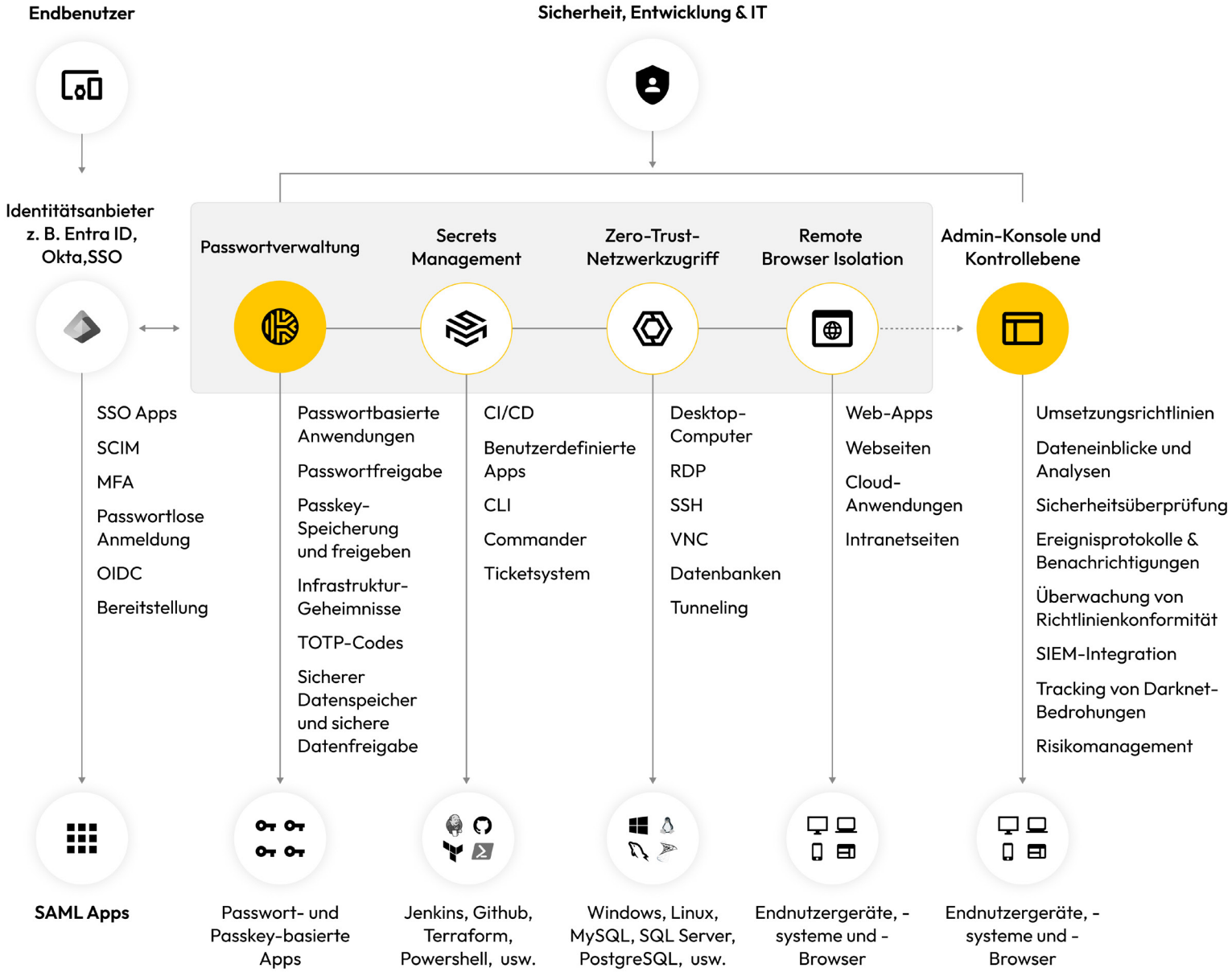
Starten Sie eine kostenlose Testversion
keeper.io/try

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 PASSWORD MANAGER

Keeper Privileged Access Management-Plattform



Geschäftswert

- Verhindern Sie Ransomware und Cyberangriffe im Zusammenhang mit Anmeldeinformationen
- Verschaffen Sie sich umfassende Transparenz, setzen Sie Best Practices und Kontrollen für die Sicherheit durch und rationalisieren Sie Compliance-Audits
- Verbessern und erweitern Sie Ihre bestehende Single Sign-On (SSO)-Bereitstellung
- Verbessern Sie die Produktivität Ihrer Mitarbeitenden und reduzieren Sie die Belastung durch passwortbezogene Tickets für Ihr Helpdesk- und IT-Team

Wichtige Funktionen

- Verschlüsselte Endbenutzer-Tresore
- Speicherung, Verwaltung und Freigabe von Passwörtern und Passkeys
- KeeperFill®-Browser-Erweiterung powered by KeeperAI™
- Web-, Desktop- und mobile Apps
- Darknet-Überwachung mit BreachWatch
- Nahtlose Bereitstellung und Integrationen
- Rollenbasierte Zugriffskontrollen (RBAC)