Datenblatt

KEEPER SECRETS MANAGER

Verteidigen Sie sich gegen Cyberangriffe, indem Sie Infrastrukturgeheimnisse wie API-Schlüssel, Datenbankpasswörter, Zugriffsschlüssel und Zertifikate sichern.

Herausforderungen

Gestohlene oder schwache DevOps-Geheimnisse sind eine der Hauptursachen für Supply-Chain-Angriffe. Geheimnisse sind in den Quellcode, die Konfigurationsdateien und CI/CD-Systeme verteilt und machen Unternehmen für Hacker angreifbar. Diese erweiterte Angriffsfläche stellt DevOps-, Sicherheits- und IT-Experten vor mehrere Herausforderungen:

01

Der Produktivität wird Vorrang vor der Sicherheit eingeräumt, und wohlmeinende Mitarbeitende verwenden die Anmeldeinformationen in der gesamten Umgebung als Hardcoding.

02

Moderne, verteilte Belegschaften arbeiten über Regionen, Systeme und Umgebungen zusammen, was ohne angemessene Kontrollen zu einem höheren Risikopotenzial führt.

03

Ohne zentral verwaltete Zugriffskontrollen besteht die Gefahr, dass Mitarbeitende übermäßig privilegiert werden, Bedrohungsvektoren öffnen und die Compliance reduzieren.

04

Interne und Compliance-Richtlinien schreiben häufig eine regelmäßige Rotation der Anmeldeinformationen vor, was nur mit einem umfassenden Tresormanagement möglich ist.

Unternehmen benötigen eine sichere, benutzerfreundliche und kosteneffektive Möglichkeit, um Geheimnisse zu speichern und den Zugriff mit den geringsten Privilegien durchzusetzen. Durch die Koordinierung des Zugriffs, die automatische Rotation von Anmeldeinformationen und die Gewährleistung einer durchgängigen Verschlüsselung können Teams das Risiko einer verheerenden Datenschutzverletzung drastisch reduzieren.

Lösung

Keeper Secrets Manager ermöglicht es Ihren Teams, CI/CD-Pipelines, DevOps-Tools, benutzerdefinierte Software und Multi-Cloud-Umgebungen in eine vollständig verwaltete Zero-Knowledge- und Zero-Trust-Plattform zu integrieren, um Infrastrukturgeheimnisse zu schützen und die Verbreitung von Geheimnissen zu reduzieren.

Keeper Secrets Manager zentralisiert Geheimnisse, um die Ausbreitung zu verhindern, unbefugten Zugriff vorzubeugen und Prüfungen und Protokollierungen zu ermöglichen. Ein umfangreiches Software Development Kit (SDK) und eine Anwendungsprogrammierschnittstelle (API) ermöglichen die bedarfsorientierte Einbindung von Anmeldeinformationen in jede beliebige Programmiersprache und so den maschinellen und menschlichen Zugriff auf Geheimnisse abzudecken.

Halten Sie sich Hacker vom Leib!

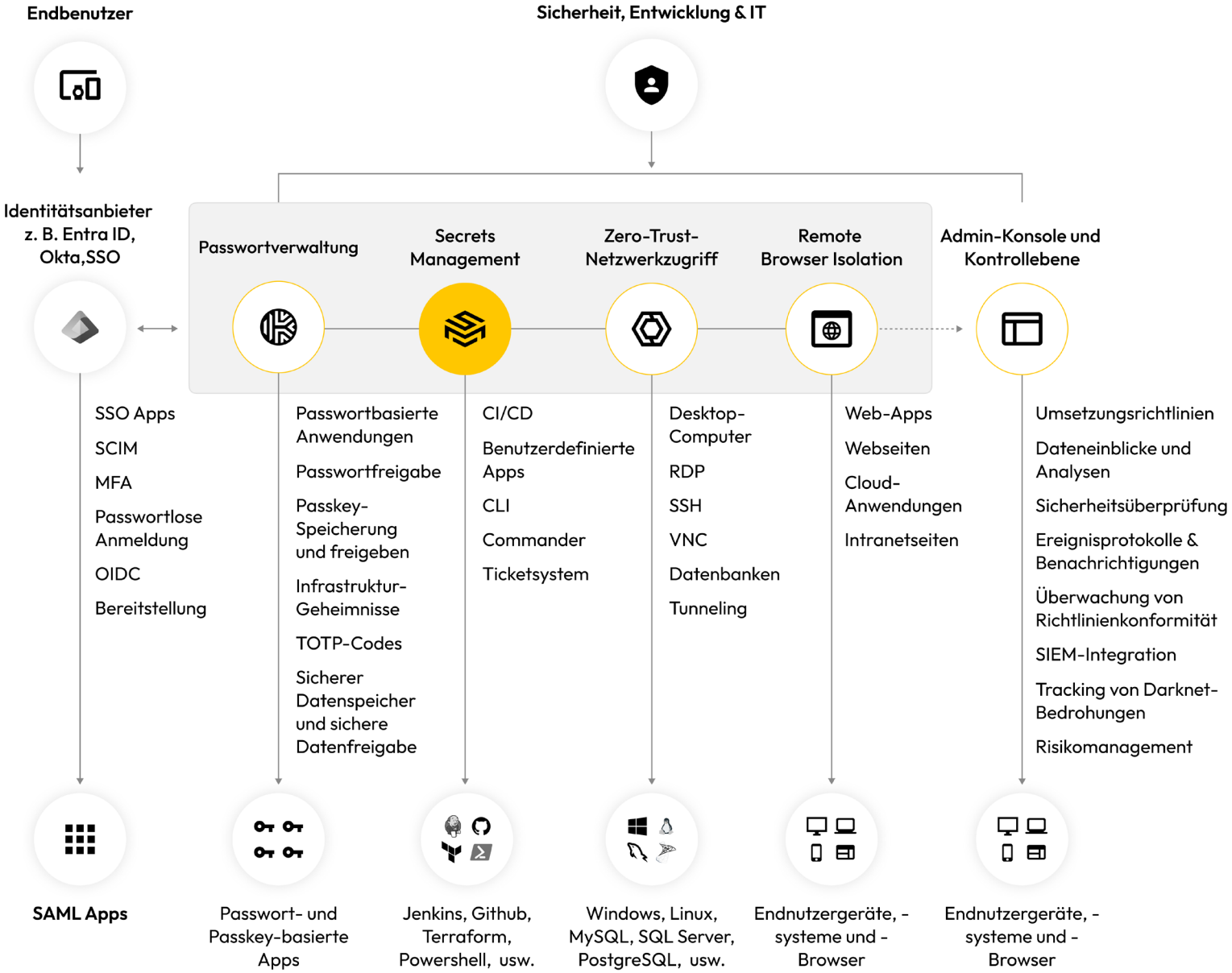
Mehr erfahren
keepersecurity.com

Demo anfordern
keeper.io/ksm

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 Privileged Access Management-Plattform



Geschäftswert

Sichert Ihre hoch privilegierten Systeme und Daten
Konsolidieren Sie Ihre Geheimnisse in einer einheitlichen Plattform und beseitigen Sie die Verbreitung von Geheimnissen, indem Sie hartcodierte Anmeldeinformationen aus Quellcode, Konfigurationsdateien und CI/CD-Systemen entfernen.

Flexible und schnelle Integration
Sofortige Integration mit allen gängigen CI/CD-Plattformen wie Github Actions, Jenkins und Ansible.

Einfach zu implementieren und benutzerfreundliche Anwendung
Vollständig cloudbasierte Zero-Trust- und Zero-Knowledge-Plattform, die keine komplexen Netzwerk-, Speicher- oder Konfigurationen mit hoher Verfügbarkeit erfordert.

Wichtige Funktionen

- Automatische Rotation der Anmeldeinformationen für Dienst- und Admin-Konten, Benutzeridentitäten, REST-basierte API-Konten, Maschinen und Benutzerkonten in Ihrer Infrastruktur und in Multi-Cloud-Umgebungen.
- Verwalten Sie Zugriffsrechte und Berechtigungen mit rollenbasierten Zugriffskontrollen.
- Client-Geräte entschlüsseln die Tresorgeheimnisse lokal nach dem Abruf. Keeper hat keine Möglichkeit, gespeicherte Tresordaten zu entschlüsseln.
- Keeper Secrets Manager ist ein vollständig verwalteter Dienst mit unbegrenzter Skalierungskapazität.