Datenblatt

Keeper Secrets Manager (KSM)

Schützen Sie sich vor Supply-Chain-Angriffen mit einer modernen, cloudbasierten Plattform zum Schutz von Infrastrukturgeheimnissen wie API-Schlüsseln, Datenbankpasswörtern, Zugriffsschlüsseln und Zertifikaten.

Herausforderungen

Gestohlene oder schwache DevOps-Geheimnisse sind eine der Hauptursachen für Supply-Chain-Angriffe. Geheimnisse sind im gesamten Quellcode, in Konfigurationsdateien und CI/CD-Systemen verstreut, was Unternehmen für Hacker angreifbar macht. Diese erweiterte Angriffsfläche stellt DevOps-, Sicherheits- und IT-Experten vor mehrere Herausforderungen:

1. Entwicklungsteams räumen der Produktivität oft Vorrang vor der Sicherheit ein. Deshalb kommt es vor, dass wohlmeinende Mitarbeitende hartcodierte Anmeldeinformationen in der gesamten Umgebung verteilen.
2. Verteilte und Remote-Mitarbeitende arbeiten über Regionen, Systeme und Umgebungen hinweg zusammen – was zu einer heterogenen Speicherung von Geheimnissen führt.
3. Ohne zentral verwaltete Zugriffskontrollen besteht die Gefahr, dass Mitarbeiter übermäßig privilegiert werden.
4. Viele Unternehmen müssen aufgrund von internen und Compliance-Richtlinien ihre Anmeldeinformationen regelmäßig rotieren, was nur mit einem umfassenden Tresor möglich ist.

Unternehmen benötigen eine sichere, benutzerfreundliche und kosteneffektive Möglichkeit, um die Verbreitung von Geheimnissen einzudämmen 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 DevOps-, IT- und Sicherheitsteams das Risiko einer verheerenden Datenschutzverletzung drastisch reduzieren.

Lösung

Der Keeper Secrets Manager bietet Ihren DevOps-, IT-, Sicherheits- und Software-Entwicklerteams eine cloudbasierte Sicherheitsplattform mit Zero-Trust und Zero-Knowledge zur Verwaltung von Infrastrukturgeheimnissen und zum Schutz der sensibelsten Daten Ihres Unternehmens.

Keeper Secrets Manager zentralisiert Ihre Geheimnisse, um die Ausbreitung zu verhindern, unbefugten Zugriff vorzubeugen und Prüfungen und Protokollierungen zu ermöglichen. Umfangreiche Software Development Kit (SDK) und API (Application Programming Interface) ermöglichen die Einschleusung von Anmeldeinformationen Just-in-Time in jede Programmiersprache, was neben dem menschlichen Zugriff auch den maschinellen Zugriff auf Geheimnisse abdeckt.

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.

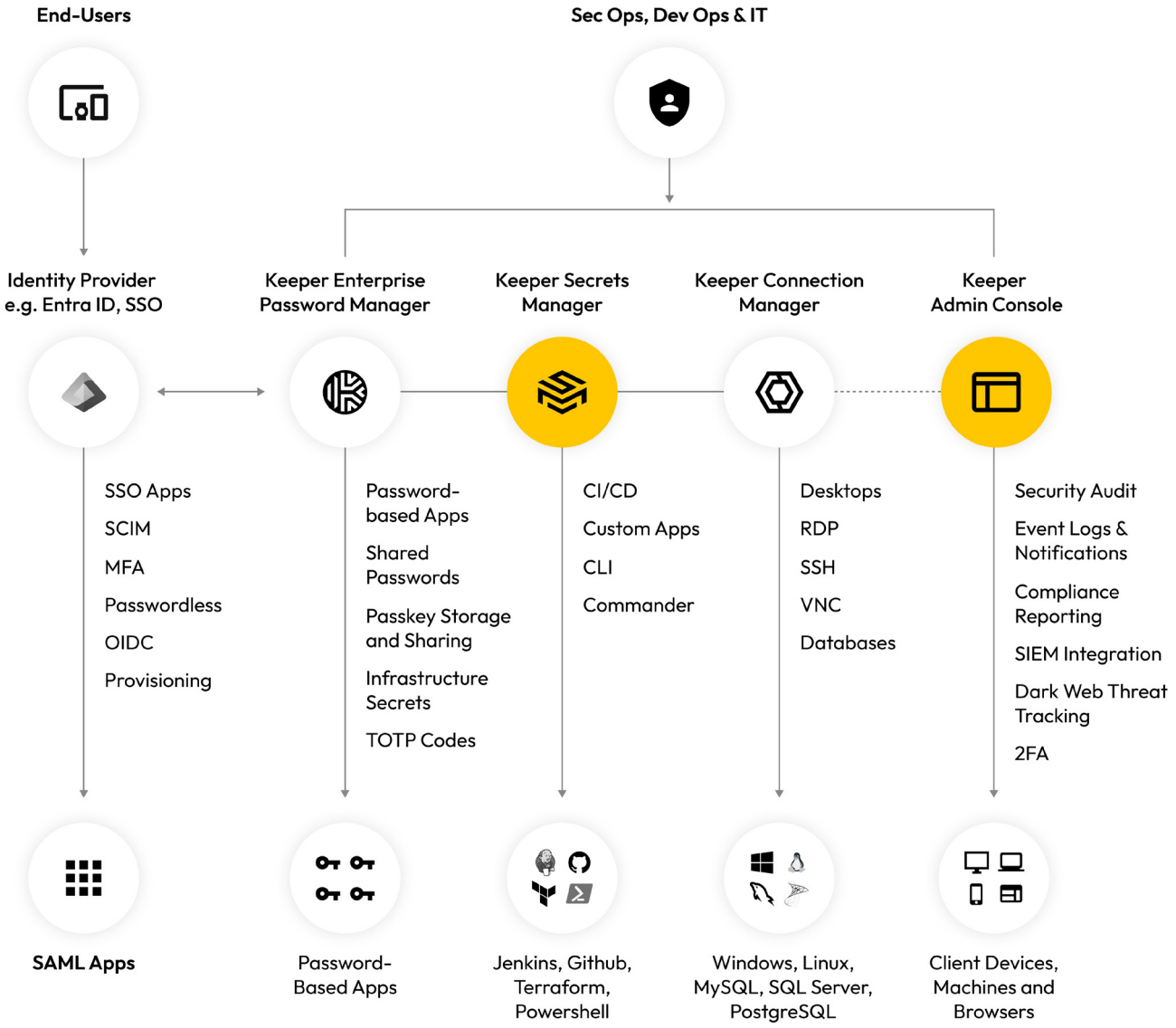
Keeper Security wird von den führenden Private-Equity-Firmen Insight Partner und Summit Partner unterstützt.

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

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.