Datenblatt

Enterprise Password Manager (EPM)

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-Administratoren:

1. Ein Unternehmen besteht aus menschlichen und maschinellen Anmeldeinformationen, die geschützt werden müssen.
2. Verteilte Remote-Arbeit und Multi-Cloud-Computing haben traditionelle IT-Perimeter obsolet gemacht.
3. 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.
4. Herkömmliche Cybersicherheitslösungen sind uneinheitlich und voneinander abgeschottet, wodurch kritische Lücken in Bezug auf Transparenz, Sicherheit, Kontrolle, Compliance und Berichterstattung entstehen.

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 EPM lässt sich nahtlos in bestehende IT-Technologie integrieren, einschließlich Security Information and Event Management (SIEM), Multifaktor-Authentifizierung (MFA), passwortlose und Identitätsanbieter (IdP)-Lösungen.

Keeper EPM bietet umfassende Authentifizierung und Verschlüsselung für jede Website, jede Anwendung und jedes System, mit dem Mitarbeitende interagieren. Keeper EPM 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, eine ISO 27001-Zertifizierung und ist FedRAMP- und StateRAMP-autorisiert.

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.

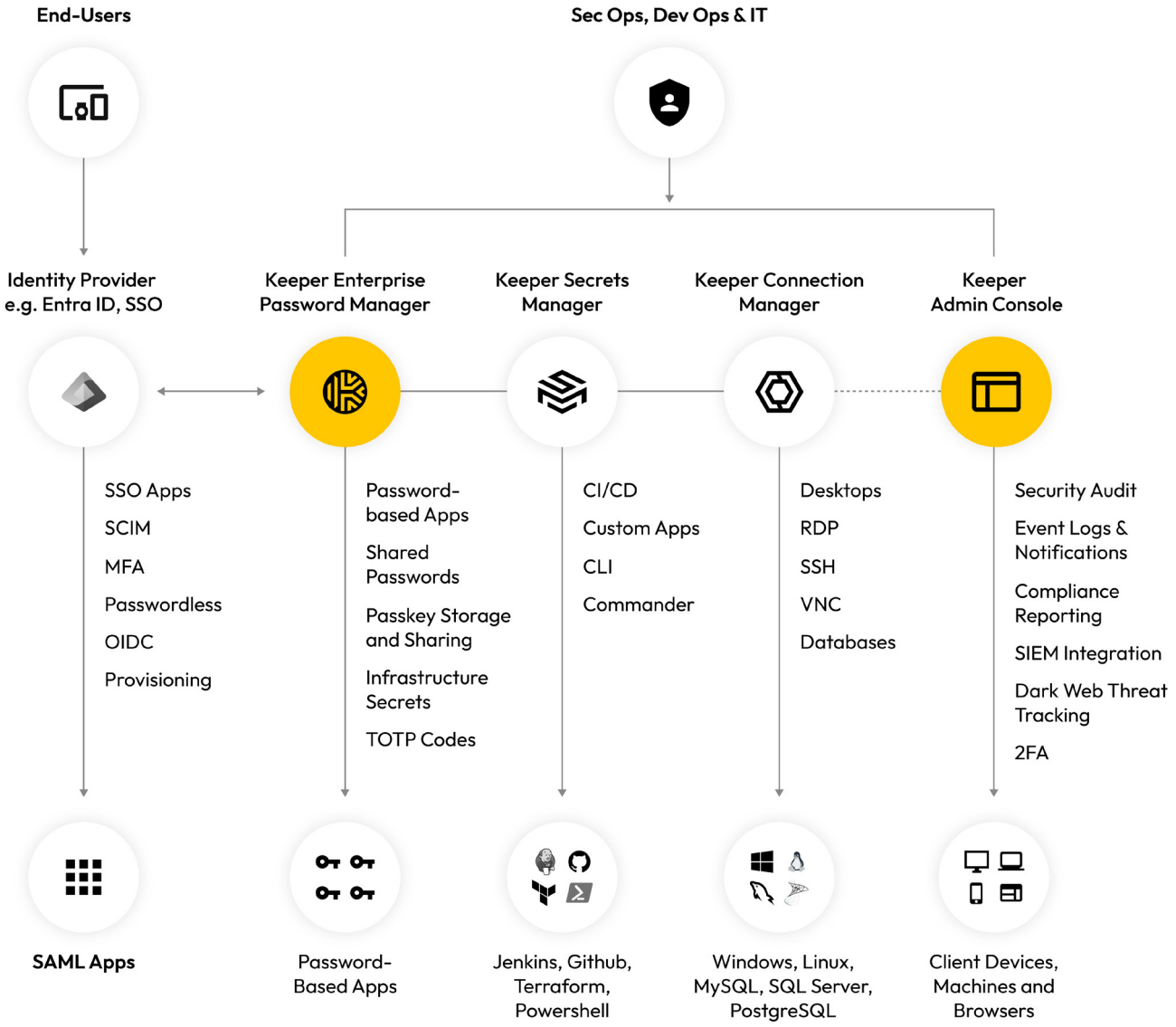
Keeper Security wird von den führenden Private-Equity-Firmen Insight Partner und Summit Partner unterstützt.

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

- Verhindern Sie Ransomware und Cyberangriffe im Zusammenhang mit Anmeldeinformationen.
- Schützen Sie jeden Benutzer auf jedem Gerät und an jedem Standort.
- 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

Key Capabilities

- 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
- Intuitive Adminkonsole
- Nahtlose Bereitstellung und Integrationen
- Rollenbasierte Zugriffskontrollen (RBAC)