

Machen Sie sich nicht zum nächsten Opfer eines Ransomware-Angriffs.

Keeper schützt Ihr Unternehmen vor den wichtigsten Datenverletzungen und Cyberbedrohungen.



Führende Unternehmen nutzen die Enterprise Password Management-Plattform (EPM) von Keeper.

Schutz Ihres Unternehmens vor Ransomware-Angriffen

Keeper schützt Ihr Unternehmen vor Ransomware-Angriffen mit robuster Administration, Kontrolle und Transparenz durch eine hohe Passwortsicherheit und Dark Web-Echtzeitmonitoring.

Mehr Sicherheit und Datenschutz

Jeder Mitarbeiter erhält einen privaten, verschlüsselten Tresor zum Speichern und Verwalten seiner Passwörter, Zugangsdaten, Dateien und privaten Kundendaten.

Gesteigerte Mitarbeiterproduktivität

Keeper reduziert Helpdesk-Kosten, spart Mitarbeitern Zeit, vermeidet Frustration und macht das Mehrfachverwenden und Merken von Passwörtern für Mitarbeiter überflüssig.

Gesicherte Freigabe von Zugangsdaten und IT-Geheimnisse

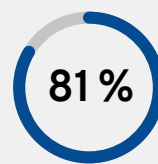
Mit Keeper gewährleisten IT-Administratoren eine gesicherte, granulare und kontrollierte Freigabe von Zugangsdaten, IT-Geheimnisse und Tresoren an Mitarbeiter und Teams.

Weniger Risiken durch Datenverletzungen

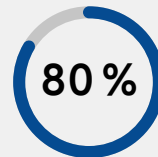
Keeper verwendet eine proprietäre Zero Knowledge-Sicherheitsarchitektur, die On-Premise-, Cloud- und Hybrid-Cloud-Umgebungen für die kundenseitige Verwaltung von Verschlüsselungscodes unterstützt.

Zuverlässigkeit in Sachen Compliance, Reporting und Auditing

Keeper unterstützt rollenbasierte Zugriffskontrollen, 2FA, Auditing, Event Reporting und Branchen-Compliance mit SOX, NIST, PCI DSS, SOC 2, ISO 27001, HIPAA, DPA, FINRA und GDPR.



der Datenverletzungen sind auf schwache, standardmäßige oder gestohlene Passwörter zurückzuführen¹



verwenden Passwörter mehrfach, speichern Geheimiten an mehreren Orten und spielen Cyberkriminellen somit in die Hände²



kostet ein Datendiebstahl im Durchschnitt³

Erfüllt die Bedürfnisse Ihres Unternehmens mit robusten Funktionen

Single Sign-On-Integration (SSO)

Implementieren Sie Keeper über bestehende SAML 2.0-kompatible SSO-Lösungen mit nahtloser Authentifizierung. Keeper unterstützt die gängigen IdPs, wie Microsoft Azure, ADFS, Okta und Google Workspace.

Hardware-Sicherheitsmodul-Integration (HSM)

Keeper SSO Connect lässt sich vollständig in On-Premise- und Cloud-HSM-Lösungen integrieren und bietet somit zusätzlichen Schutz für Verschlüsselungscodes.

Rollenbasierte Zugriffskontrollen

Mitarbeiterberechtigungen können durch fein abgestufte Zugriffskontrollen auf der Grundlage der jeweiligen Rollen und Zuständigkeiten der Teammitglieder präzise angepasst werden.

Versionskontrolle und Datensatzhistorie

Mitarbeiter können auf eine lückenlose Historie ihrer Datensätze zugreifen, frühere Versionen einsehen, Änderungen nachvollziehen und diese Datensätze jederzeit wiederherstellen.

Sicherheit für mehr als nur Passwörter

Mitarbeiter können Dateien und Metadaten jeder Art in ihren Keeper Tresoren verschlüsseln und ablegen, z. B. private Schlüssel, digitale Zertifikate, Notizen, Listen, Codes, vertrauliche Dokumente und Mediendateien.

Skalierbare Benutzer-Provisionierung

Keeper rationalisiert das Onboarding durch die Admin-Konsole und die erweiterte Integration mit Active Directory, SSO, SCIM und Entwickler-APIs.

Gemeinsame Nutzung mit Kollegen und Teams

Mit Keeper können Sie sowohl einzelne Datensätze als auch verschlüsselte Ordner für Teams oder einzelne Benutzer sicher erstellen, freigeben und verwalten.

Auditing, Analysen und Reporting

Die Enterprise Password Management-Plattform (EPM) von Keeper bietet transparente Passwortpraktiken mit robusten Reporting- und Auditing-Tools, damit Sie die Bedrohung durch Cyberangriffe reduzieren und Compliance-Standards einhalten können.

Erweiterte DevOps-Tools

Das Keeper Commander SDK bietet IT-Administratoren und Entwicklern Open Source-Codes, Kommandozeilen-Tools und APIs für die Passwortverwaltung und -rotation.

Separate Datentresore auf Unternehmens- und Personenebene

Mitarbeiter haben Zugang zu separaten Tresoren zum Schutz von geschäftlichen und persönlichen Daten und können von beliebig vielen Geräten aus problemlos zwischen ihnen wechseln.

Branchenspezifische Compliance und Verschlüsselung



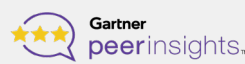
Höchste Auszeichnungen und Bewertungen in der Branche



2021 Enterprise Leader
4,7 von 5 Sternen



Editors' Choice
4,5 von 5 Sternen



Gartner Peer Insights
4,6 von 5 Sternen



Spiceworks
4,9 von 5 Sternen

Quellen: ¹Verizon Breach Incident Report ²Keeper Branchenumfrage ³Ponemon Institute