KEEPER SECRETS MANAGER

Schützen Sie Ihre IT-Infrastruktur vor Cyberkriminellen und Angriffen auf die Lieferkette

Der Keeper Secrets Manager bietet Ihren Teams in den Bereichen DevOps, IT, Sicherheit und Softwareentwicklung eine cloudbasierte Zero Trust-und Zero Knowledge-Sicherheitsplattform für die Verwaltung der Geheimdaten Ihrer Infrastruktur und den Schutz der hochsensiblen Daten Ihres Unternehmens.

VORTEILE

Sicherheit für hochsensible Systeme und Daten

Konsolidieren Sie Ihre IT-Geheimdaten in einer einheitlichen Plattform, und beseitigen Sie die unübersichtliche Verteilung dieser Daten, indem Sie fest codierte Zugangsdaten aus Ihrem Quellcode, Ihren Konfigurationsdateien und CI/CD-Systemen entfernen. Der Keeper Secrets Manager bietet Transparenz und Kontrolle über die Datenumgebung, die Sicherheit und das Auditing in Ihrem Unternehmen.

Flexible und schnelle Integration

Schnelle Integration in alle gängige CI/CD-Plattformen, wie Github Actions, Jenkins und Ansible. Die Entwickler-SDKs sind für alle gängigen Programmiersprachen verfügbar und bieten Schutz für jede Art von Umgebung.

Problemlose Einrichtung, einfache Nutzung

Als vollständig cloudbasierte Zero Trust- und Zero Knowledge-Plattform erfordert der Keeper Secrets Manager keine On-Premise-Infrastruktur, wodurch eine komplexe Netzwerk-, Speicher- und HA-Konfiguration überflüssig wird. Dank eines fortschrittlichen Verschlüsselungsmodells beseitigt Keeper das Risiko einer Kompromittierung des zentralen Tresors.

SCHLÜSSELFUNKTIONEN

- ✓ Endnutzer erhalten einen persönlichen, verschlüsselten Tresor zum Speichern und Verwalten von Passwörtern, Anmeldedaten, Dateien und gemeinsam genutzten Geheimdaten – auf allen Geräten.
- ✓ Teammitglieder können eine unbegrenzte Anzahl von Geheimdaten, Anwendungen und Umgebungen verwalten.
- ✓ Entwickler verfügen über SDKs in den gängigen Programmiersprachen, um Geheimdaten in nur wenigen Code-Zeilen abrufen und aktualisieren zu können.
- ✓ Plugins und Integrationen stehen für beliebte CI/CD-Plattformen und Build-Tools, wie Docker und Kubernetes, zur Verfügung.
- ✓ Die zentrale Admin-Konsole bietet rollenbasierte Zugriffskontrolle (RBAC), Provisionierung, Reporting, Auditing und Benutzerverwaltung.
- ✓ Das Advanced Reporting & Alerts Module (ARAM) ermöglicht granulare Event Reporting- und Alerting-Funktionen mit SIEM-Integration.
- ✓ BreachWatch® schützt Zugangs- und Geheimdaten durch Dark Web Monitoring.