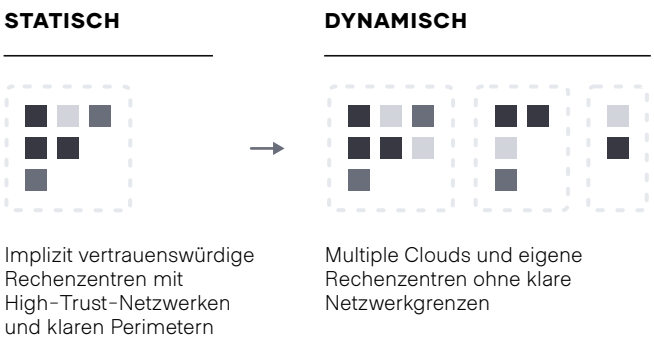
Vault

Cloud-Security-Automatisierung

Secrets Management und Schutz sensibler Daten
über Public und Private Clouds hinweg

Infrastruktursicherheit und ihre Herausforderungen

Die Einführung der Cloud bedeutet, dass sich Organisationen von statischer Infrastruktur verabschieden und auf die Bereitstellung und das Management dynamischer Infrastruktur umsteigen – auf grenzenlose Ressourcen und Dienste, ob flüchtig oder unveränderlich, in jedem Fall unabhängig von den anvisierten Zielumgebungen.

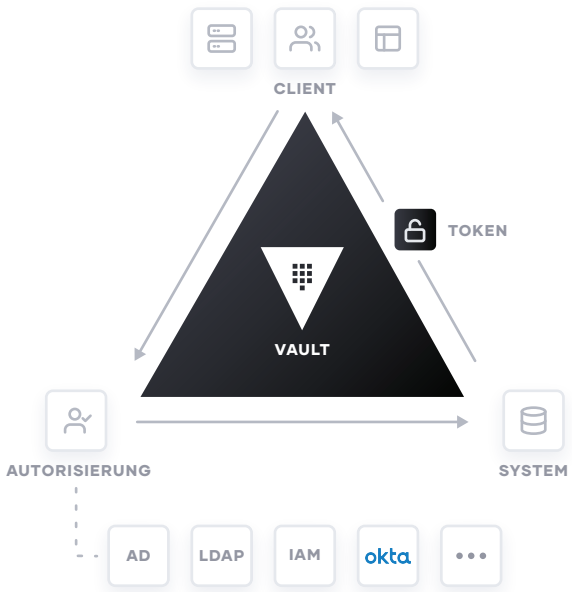


HashiCorp Vault

Mit Vault können Sie Tokens, Passwörter, Zertifikate, Schlüssel und andere sensible Daten sicher speichern und den Zugriff darauf streng kontrollieren, per UI, CLI oder per HTTP-API.

Das zentralisierte Secrets Management von Vault steigert die Produktivität und reduziert die Kosten für Systeme, Lizenzen und Overhead. Dadurch dass statische, hart codierte Anmeldedaten durch zentralisierte Zugangssicherheit ersetzt werden, trägt Vault auch dazu bei, das Risiko von Datenvorfällen zu verringern.

- **Identitätsabgleich** zur Authentifizierung bei mehreren Clouds, mit Richtliniendurchsetzung und einfacher Automatisierung.
- **Ein einziger Workflow,** der sich in jede Infrastruktur fügt, Kosten reduziert und eine einheitliche Prüfkette sicherstellt.
- **Offen und erweiterbar** durch die Open-Source-Community, das Parterökosystem und volle Multi-Cloud-Unterstützung.



Leistungen und Vorteile

Mehr Datensicherheit

Sensible Daten werden mit zentral verwalteten und gesicherten Schlüsseln codiert, sowohl at Rest als auch in Transit, mit einem einzigen Workflow und einem einzigen API.

Geringeres Risiko von Datendiebstahl

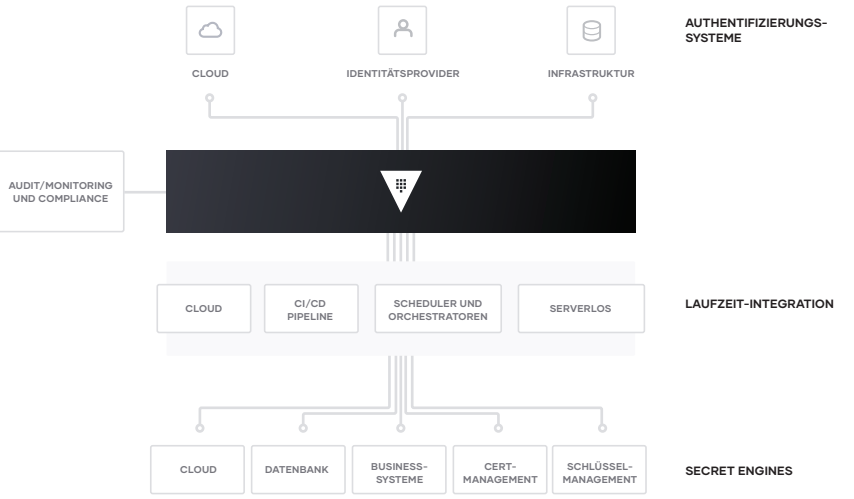
Das zentrale Secrets Management von Vault ermöglicht strenge Zugriffskontrolle auf der Basis vertrauenswürdiger Identitäten – anstelle statischer, hart codierter Anmeldedaten.

Mehr Produktivität

Entwicklerteams können Secrets bei der Anwendungsbereitstellung automatisiert nutzen. Sensible Daten bleiben programmatisch über eine einzige API geschützt.

Integration

- Zugriffskontrolle mit vertrauenswürdigen Identitäten für unterschiedliche Clouds, Systeme und Endpunkte
- Sicherheit für Anwendungsdadten durch zentrale Schlüsselverwaltung und einfache APIs zur Ver- und Entschlüsselung
- Ablage, Zugriff und Kontrolle: Dynamische Speicherung von Geheimnissen wie Tokens, Passwörtern, Zertifikaten und Schlüsseln
- Einheitlicher Support auch in heterogenen Umgebungen, nahtlose Integration in Workflows und Technologien, die Sie bereits nutzen



Referenzen

Adobe

BARCLAYS

SAP Ariba

SPACEFLIGHT

cruise

credit karma

Lösungen

Open Source Profis	**Enterprise** Organisationen	**Cloud*** HCP Vault auf AWS
Dynamische Secrets ✓	**Alle Open-Source-Funktionen** ✓	**Alle Open-Source-Funktionen** ✓
Secrets-Speicher ✓	Disaster Recovery ✓	Disaster Recovery ✓
Sichere Plugins ✓	Namensräume ✓	Namensräume ✓
Detaillierte Audit-Logs ✓	Replikation ✓	Clustering ✓
Secrets-Ausgabe & Widerruf ✓	Replikationsfilter ✓	Snaphots & Wiederherstellung ✓
ACL-Templates ✓	Replikationen lesen ✓	Audit-Logging ✓
Vault Agent ✓	Gruppenregeln ✓	Berichterstattung ✓
Init & Unseal Workflow ✓	HSM Auto-unseal ✓	
Rollierende Schlüssel ✓	Multi-Faktor-Authentisierung ✓	
UI mit Cluster Management ✓	Sentinel-Integration ✓	
Entitäten & Gruppen ✓	FIPS 140-2 & Seal Wrap ✓	
Zugriffskontrollrichtlinien ✓	KMIP-Support ✓	
Identity-Plugins ✓	Transform ✓	
Encryption as a Service ✓		
Transit-Backend ✓		
Rollierende Verschlüsselung ✓		
AWS KMS Auto-unseal ✓		
Azure Key Vault Auto-unseal ✓		
GCP Cloud KMS Auto-unseal ✓		
Integrierter Speicher ✓		

HashiCorp

www.hashicorp.com

* Derzeit in Beta-Version.