



HashiCorp Vault

Vorteile

- Dynamische, kurzlebige Secrets reduzieren Angriffsfläche
- Feingranulare Policies und vollständige Audit-Trails
- Breite Auth- und Plattform-Integrationen
- API-first, GitOps-/Automationsfreundlich

Nachteile

- Betriebsaufwand: Leases/Tokens erneuern und verwalten
- Abhängigkeit von externen IdPs bei Token-/Lease-Erneuerungen
- Einführung/Policy-Governance komplex
- Enterprise-Features kostenpflichtig

Eigenschaften

- Secrets-Management (KV, Versionierung)
- Dynamische Secrets, Lease/Renew/Revoke
- Auth-Methoden (Token, AppRole, LDAP, OIDC/Cloud IAM, Kubernetes)
- Policies/RBAC
- Audit Logging
- Transit (Encryption as a Service)
- PKI-Engine (Zertifikate)
- HA/Replication, Integrated Storage (Raft)

Einsatzgründe

- Zentrale Secret-Verwaltung in heterogenen Umgebungen
- Kurzlebige, automatisch revokierbare Credentials
- Compliance, Nachvollziehbarkeit, Audits
- Multi-Cloud-/Hybrid-Integration
- Identity-first/Zero-Trust-Architekturen
- API/CLI/Agent-Automatisierung