

Secrets Management

Vault-compatible · Multi-cloud · Zero Trust



Eliminate secrets sprawl. Centralize, rotate, and audit every credential across **public cloud, private cloud, on-prem, and air-gapped** environments — with zero code changes from HashiCorp Vault.

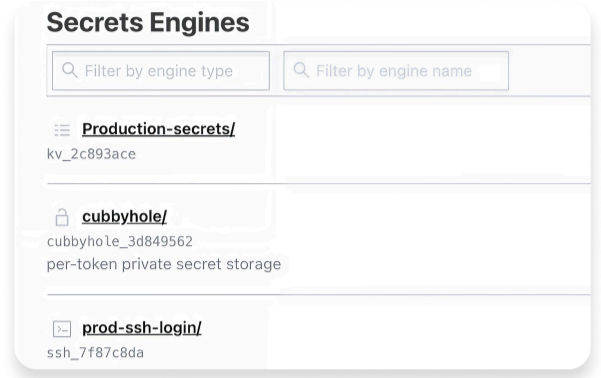
THE PROBLEMS

Secrets Hardcoding
Credentials in source code, config files, and CI/CD pipelines — a direct path to breaches.

Manual Rotation
Late or skipped rotation leaves compromised credentials active across all environm

Compliance Gaps
No visibility on who accessed what, when — failing GDPR, HIPAA, PCI-DSS, and DORA audits.

Inconsistent Access Control
Different auth methods per platform prevent unified policy enforcement at scale.

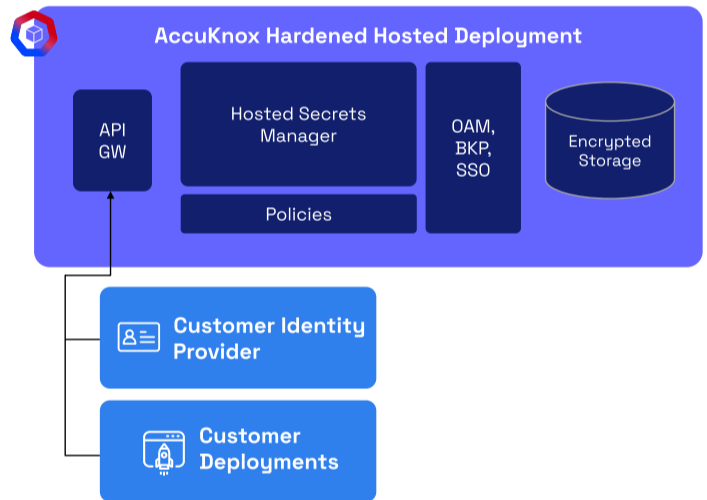


HASHICORP COMPATIBLE SECRETS MANAGER SOLUTION FOR MODERN TEAMS



WHY PICK ACCUKNOX SECRETS MANAGER SOLUTION

Feature	AccuKnox	HashiCorp Enterprise	CyberArk
Secure Secrets Storage	✓	✓	✓
Dynamic Secrets	✓	✓	✓
Encryption as a Service (Transit / PKI)	✓	✓	Add-on required
SIEM & CDR Direct Log Integration	✓ Native (Free)	Forwarding only	Forwarding only
OS-Level Hardening (CWPP)	✓ SW + OS	SW only	SW only
On-Prem / Air- Gapped	✓	✓	✓
Cost	\$ — From \$400/mo	\$\$\$	\$\$\$



DEPLOYMENT MODELS

Shared Instance
\$400 / month

- ✓ Single namespace (extras available)
- ✓ Daily automated backups
- ✓ Unlimited secrets, users & integrations
- ✓ NA, EU, ME & India regions
- ✓ Ideal for non-production workloads

Dedicated Instance
\$800+ / month

- ✓ Multiple namespaces, no API limits
- ✓ Backup frequency per client SLA
- ✓ Free SIEM/CDR log ingestion (5 GB/mo)
- ✓ Custom compliance controls (+\$200/mo)
- ✓ Custom branding · On-prem / air-gapped

Enterprise / On-Premises
Contact Sales

- ✓ Full air-gapped deployment
- ✓ Regional data residency compliance
- ✓ HA mode, CWPP-hardened instances
- ✓ OIDC · LDAP · Okta · K8s · AppRole
- ✓ Dedicated SLA & support

High Availability
All instances deployed in HA mode. Shared instances across NA, EU, ME & India regions.

Vault API Compatible
KV, Transit, PKI, Dynamic Secrets, AuthN methods — no major code changes required.

CWPP Hardened
Every instance is OS & software-hardened by AccuKnox's own CWPP engine.

Full Audit Trail
Every request logged — who, what, when — directly feeding AccuKnox SIEM & CDR.

“

Choosing AccuKnox was driven by opensource KubeArmor's novel use of eBPF and LSM technologies, delivering runtime security.

Golan Ben-Oni — CIO, IDT Corporation

“

AccuKnox excelled in all areas in our in-depth evaluation. We advocate for a comprehensive end-to-end methodology in application and cloud security.

Manoj Kern — CIO, Prudent

About AccuKnox

AccuKnox is a Zero Trust CNAPP Cloud Security protects API Security, CDR, SIEM, Public clouds, Private clouds, Kubernetes, VMs, Bare metals, IoT Edge, and 5G security.



in [linkedin.com/accuknox](https://www.linkedin.com/company/accuknox)

X @AccuKnox