Unified identity-based secrets management

HashiCorp Vault

The standard for security automation to manage access to secrets and protect sensitive data

From perimeter security to identity-centric protection

Identity-based security moves beyond static perimeters and trusted networks to support dynamic infrastructure, non-human identities, and agentic AI. In environments with no clear boundary, security shifts from network location to verified identity, ensuring infrastructure and application services are protected based on who or what is accessing them.

Static

Datacenters with inherently high-trust networks with clear network perimeters

Traditional approach

- High-trust networks
- A clear network perimeter
- Security enforced by IP-address

Dynamic

Multiple clouds and private datacenters without a clear network perimeter

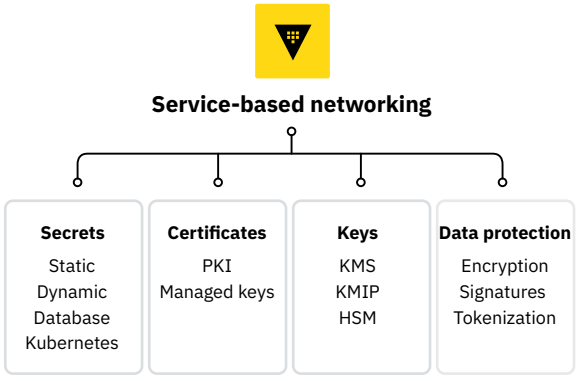
Vault approach

- Low-trust networks in public clouds
- Unknown network perimeter across clouds
- Security enforced by application identity

HashiCorp Vault

Secure, store, and tightly control access to tokens, passwords, certificates, encryption keys, and other sensitive data using a UI, CLI, or HTTP API.

- Centrally store, access, and distribute static and dynamic secrets
- Allow Kubernetes services to authenticate and request their owncredentials
- Automate service account rotation
- Protect data with centralized key management
- Enables NHIs to authenticate dynamically and receive least-privilege, short-lived secrets
- Secures agentic AI by brokering identity-based access for autonomous agents



Trillions+ Secrets managed/year

250M+ Downloads

70%+ of top 20 U.S. banks

Benefits

50% Less time spent

Reduce risk of data exposure

Encrypt sensitive data in transit and at rest using centrally managed and secured encryption keys in Vault, all through a single workflow and API.

100K Edge devices supported

Reduce the risk of a breach

Eliminate static, hard-coded credentials by centralizing secrets in Vault and tightly controlling access based on trusted identities.

0% Unplanned downtime

Increase productivity

Enable development teams to automatically consume secrets in their application delivery process and protect sensitive data programmatically through a single API.

Supported technologies and identities

Trusted by

Adobe

BARCLAYS

SAP Ariba

SPACEFLIGHT

cruise

credit karma

Compare Offerings

		HCP Dedicated SaaS	Enterprise Self-managed
Adopt Govern identities Establish trust	**Control human and NHI access**	✓	✓
	Set role-based policy	✓	✓
	Centralize management of secrets and data	✓	✓
	Enable visibility and traceability	✓	✓
Standardize Ensure continuity Enforce compliance	**Automate secret creation, rotation and revocation**	✓	✓
	Sync secrets from native secret managers	✓	✓
	Support policy as code to govern systems	✓	✓
	Create logic-based policies with Sentinel	✓	✓
	Performance replication and disaster recovery	✓	✓
	Modernize legacy applications with Vault agent	✓	✓
Scale Elevate secrity Enhance ecosystem	**PKI certificate mgmt (app, service and hardware)**	✓	✓
	SPIFFE and JWT auth support	✓	✓
	Key lifecycle management	✓	✓
	Encryption as a service	✓	✓
	Encrypt with tokenization, FPE and data masking	✓	✓
	Transparent Data Encryption for private infrastructure	✓	✓
	Support FIPS 140-3 compliance		✓
	Standardize AI platform integration with MCP server	✓	✓
	Private networking with BYO DNS and PrivateLink	✓	
	Automate credentials for private cloud and data center	✓	✓