HashiCorp
Vault

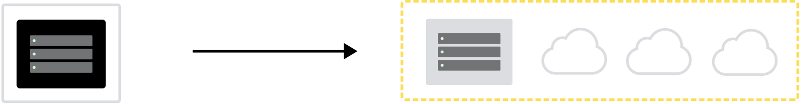
Standardize identity-based security management

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

Identity-based security has evolved with cloud

Identity-based security represents the shift from a static security model to one that accounts for dynamic IP addresses, and no clear perimeter. Instead of targeting on a secure network perimeter and trusted networks, the focus shifts to the notion that securing infrastructure and application services.

Static



Datacenters with inherently high-trust networks with clear network perimeters.

Traditional approach

- Hish trust networks
- A clear netowrk perimeter
- Security enforced by IP-ADDRESS

Dynamic

Multiple clouds and private datacenters without a clear network perimeter.

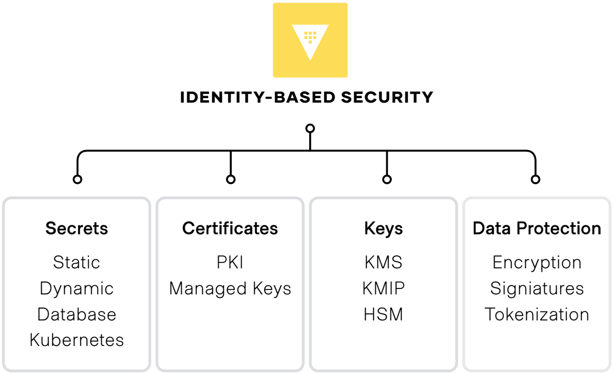
Vault approach

- Low trust netowrks in public clouds
- Unknown netowrk 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 & dynamic secrets
- Allows Kubernetes services to authenticate & request their own credentials
- Automated Service Account Rotation
- Protect data with centralized key management



IDENTITY-BASED SECURITY

Secrets
Static
Dynamic
Database
Kubernetes

Certificates
PKI
Managed Keys

Keys
KMS
KMIP
HSM

Data Protection
Encryption
Signatures
Tokenization

Trillions+
Secrets managed/year

250M+
Downloads

70%+
of top 20 US 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

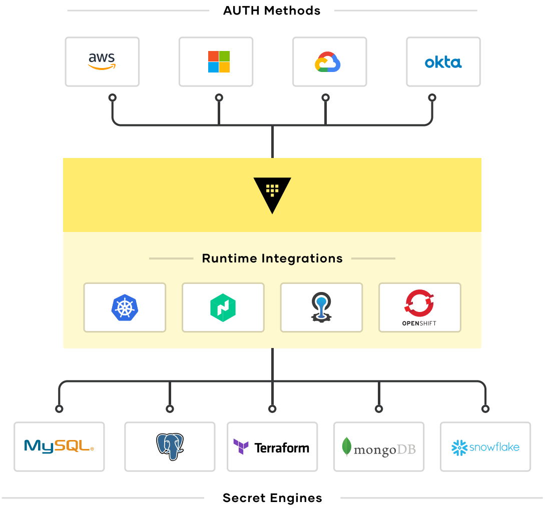
Enable development teams to automatically consume secrets in their application delivery process and protect sensitive data programmatically through a single API.

Ecosystem

HashiCorp Vault functionality can be broadly extended with API integrations, partners and plugins.

- 100+ Partner & Integrations
- 100+ OSS & Enterprise Integrations
- 35+ Plugins

For more information, please visit https://www.hashicorp.com/partners.



Trusted by

Adobe

BARCLAYS

SAP Ariba

SPACEFLIGHT

cruise

credit karma

Compare offerings

		Open Source Individuals	Enterprise Pro Teams	Enterprise Premium Organizations
Adopt Service registry and discovery	Secure storage	✓	✓	✓
	Vault agent	✓	✓	✓
	Detailed audit logs	✓	✓	✓
	Namespaces		✓	✓
	Silver support: 9x5 w/ SLA		✓	✓
	Gold support: 24/7 w/ SLA		✓	✓
Standardize Secure networking	Credential leasing & revocation	✓	✓	✓
	Secure plugins	✓	✓	✓
	Entities & entity groups	✓	✓	✓
	UI with cluster management	✓	✓	✓
	Control groups			✓
	Multi-factor authentication			✓
	Read replicas			✓
	Replication			✓
	Replication filters			✓
Scale Governance, compliance and reliability	ACL governance & templating	✓	✓	✓
	Encryption as a service	✓	✓	✓
	Key rolling	✓	✓	✓
	Disaster recovery (DR)		✓	✓
	Auto-unseal AWS KMS		✓	✓
	Auto-unseal GCP Cloud KMS		✓	✓
	Auto-unseal Azure Key Vault		✓	✓
	Sentinel policy as code management			✓
	HMS Auto-unseal			✓
	FIPS 140-2 & cryptogenic compliance			✓

HashiCorp
www.hashicorp.com