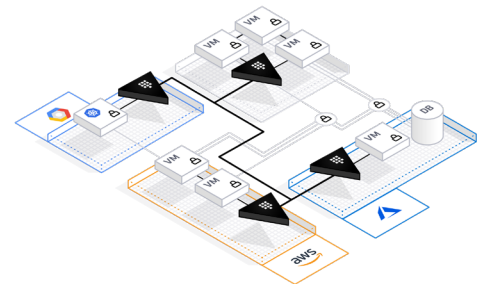
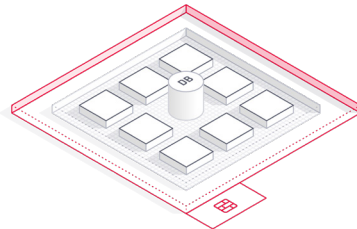


# Manage Secrets and Protect Sensitive Data

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

The shift  
from **static**  
to **dynamic**  
infrastructure



## Static Infrastructure

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 Infrastructure

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

## Vault Use Cases



### Secrets Management

Centrally store, access, and distribute dynamic secrets such as tokens, passwords, certificates, and encryption keys.



### Data Protection

Keep application data secure with centralized key management and simple APIs for data encryption.

## Vault Benefits



### 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.



### Reduce the risk of a breach

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



### Increase productivity

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

## Trusted by



[www.hashicorp.com](https://www.hashicorp.com)

## Supported Technologies and Identities



## Compare Offerings

	Open Source	Enterprise Pro	Enterprise Premium
	Individuals	Teams	Organizations
Secure Storage	✓	✓	✓
Vault Agent	✓	✓	✓
Credential Leasing & Revocation	✓	✓	✓
Detailed Audit Logs	✓	✓	✓
Secure Plugins	✓	✓	✓
ACL Governance & Templating	✓	✓	✓
Encryption as a Service	✓	✓	✓
Key Rolling	✓	✓	✓
Entities & Entity groups	✓	✓	✓
UI with Cluster Management	✓	✓	✓
Namespaces		✓	✓
Disaster Recovery (DR)		✓	✓
Auto-unseal AWS KMS		✓	✓
Auto-unseal GCP Cloud KMS		✓	✓
Auto-unseal Azure Key Vault		✓	✓
Silver Support: 9x5 w/ SLA		✓	✓
Sentinel Policy as Code Management			✓
Control Groups			✓
HMS Auto-unseal			✓
Multi-factor Authentication			✓
FIPS 140-2 & Cryptographic Compliance			✓
Read Replicas			✓
Replication			✓
Replication Filters			✓
Gold Support: 24/7 w/ SLA			✓