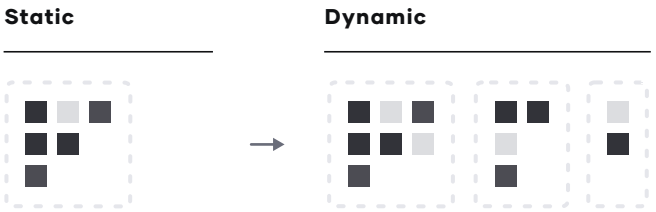
Vault

Cloud Security Automation

Manage Secrets and Protect Sensitive Data across public and or private clouds

The Challenges of Infrastructure Security

The adoption of Cloud means organizations shift away from static infrastructure to now provisioning and managing dynamic infrastructure—infinite volume and distribution of services, embracing ephemerality and immutability, and ability to deploy onto multiple target environments.



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

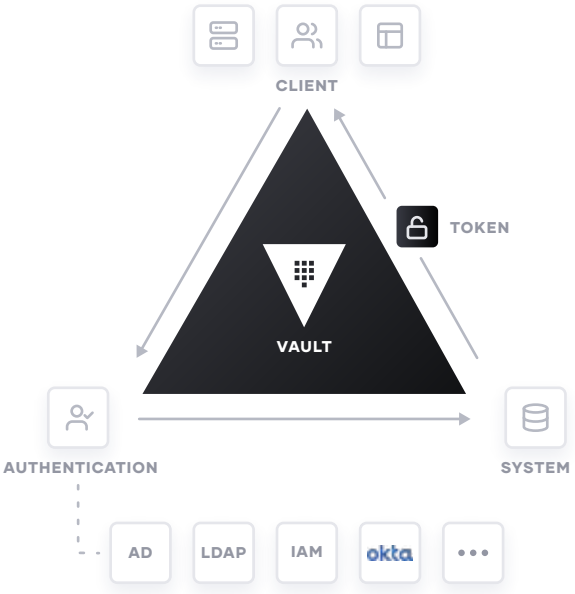
Multiple clouds and private datacenters without a clear network perimeter.

HashiCorp Vault

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

You can increase productivity, control costs by reducing systems, licenses and overhead by centrally managing all secrets operations. Vault can also assist with reducing the risk of breach by eliminating static, hard-coded credentials by centralizing secrets.

- **Identity Brokering** for authentication and access different clouds, policy enforcement, and easy automation.
- **Single Workflow** that integrates with existing infrastructure, reduces costs, and provides a unified audit trail.
- **Open & Extensible** strong open source community, large partner ecosystem, and full featured multi-cloud secrets engines.



Solutions and 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.

Integrations

- Authenticate and access different clouds, systems, and endpoints using trusted identities
- Keep application data secure with centralized key management and simple APIs for encrypt/decrypt data
- Centrally store, access, and distribute dynamic secrets such as tokens, passwords, certificates, and encryption keys
- Provides unified support across heterogeneous environments. Integrates with workflows and technologies you're already using

Trusted By

Adobe

BARCLAYS

SAP Ariba

SPACEFLIGHT

cruise

credit karma

Offerings

Open Source Practitioner		Enterprise Organizations		Cloud* HCP Vault on AWS	
Dynamic Secrets	✓	**All Open Source Features**	✓	**All Open Source Features**	✓
Secret Storage	✓	Disaster Recovery	✓	Disaster Recovery	✓
Secure Plugins	✓	Namespaces	✓	Namespaces	✓
Detailed Audit Logs	✓	Replication	✓	Clustering	✓
Leasing & Revoking Secrets	✓	Replication Filters	✓	Snapshot & Restore	✓
ACL Templates	✓	Read Replicas	✓	Audit Logging	✓
Vault Agent	✓	Control Groups	✓	Reporting	✓
Init & Unseal Workflow	✓	HSM Auto-unseal	✓		
Key Rolling	✓	Multi-factor Authentication	✓		
UI with Cluster Management	✓	Sentinel Integration	✓		
Entities & Identity Groups	✓	FIPS 140-2 & Seal Wrap	✓		
Access Control Policies	✓	KMIP Support	✓		
Identity Plugins	✓	Transform	✓		
Encryption as a Service	✓	Resource Quotas-Lease Count	✓		
Transit Backend	✓	Splunk Monitoring App	✓		
Encryption Key Rolling	✓				
Entities & identity groups	✓				
Access Control Policies	✓				
Identity plugins	✓				
AWS KMS Auto-unseal	✓				
Azure Key Vault Auto-unseal	✓				
GCP Cloud KMS Auto-unseal	✓				
Integrated Storage	✓				
Resource Quotas-Rate Limit	✓				

HashiCorp

www.hashicorp.com

* currently available in private beta