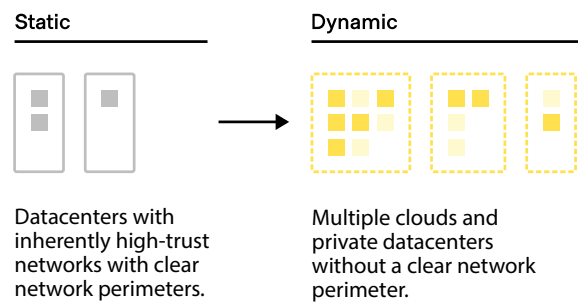# HashiCorp Vault

Vault on HashiCorp Cloud Platform

All of the power and security of Vault, without the complexity and overhead of managing it yourself

The Challenges of Infrastructure Security

The adoption of Cloud requires a shift away from static infrastructure to now provisioning and managing dynamic infrastructure. The ephemeral nature, infinite volume, and distribution of services create additional overhead and management requirements resulting in increased costs, risk, resources, and increased attack surface. Secrets and sensitive data may now become sprawled across different systems, files, and repos, creating opportunities for attackers.

Static

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

Dynamic

Multiple clouds and private datacenters without a clear network perimeter.

Vault on HashiCorp Cloud Platform

Vault running on the HashiCorp Cloud Platform (HCP) is fully managed by HashiCorp and provides push-button deployment, fully managed clusters, upgrades, backups, and monitoring. HCP Vault enables organizations and developers to focus on adoption and integration instead of operational overhead.

HCP Vault enables users to secure, store, and tightly control access to tokens, passwords, certificates, and encryption keys within one unified cloud-based platform. HCP Vault clusters fit into any workload and automatically scale with clusters that can be deployed in minutes.

- 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.

Client

Token

Vault

Authentication

System

AD   LDAP   IAM   okta   •••
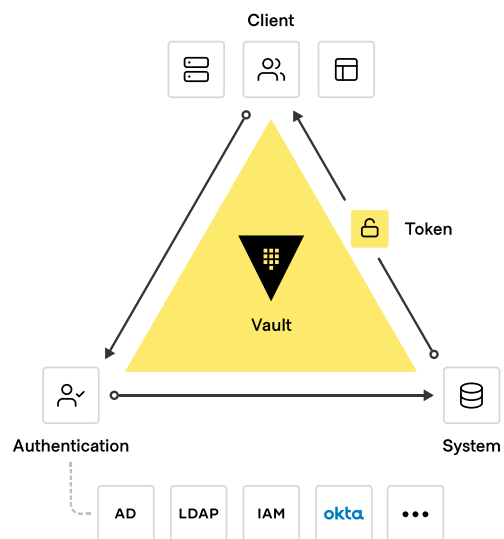
Solutions and Benefits

Reduce operational overhead

Push-button deployment, fully managed upgrades, and backups mean organizations can focus on adoption and integration instead of operational overhead

Increase security across clouds and machines

Secure your infrastructure across all your environments through a single interface and globally control and restrict access to sensitive data and systems

Control costs

Reduce the number of systems, licenses, and manual overhead by centralizing secrets management with HCP Vault

Day Zero Readiness

Modern cloud security to quickly secure applications, access, and data from day zero.

Reliability

We've supported thousands of commercial Vault clusters and HCP Vault brings that expertise directly to users

Ease of Use

HCP Vault is built around making cloud security automation simple. Get up and running instantly and onboard applications and teams easily.

Trusted by

Adobe®

BARCLAYS

SAP Ariba

SPACEFLIGHT

cruise

credit karma

Compare offerings

Development

Single-node clusters aimed at development (non-prod) workloads and enterprise features and capabilities.

Self-serve available via monthly, pay-as-you-go billing (credit card)	✓
Single-node clusters	✓
Vault OSS	✓
Namespaces	✓
Up to 25 clients (soft limit)	✓
Email support	✓
Login Multi-factor Authentication	✓

Annual Contract

Mix and match Development, Standard and Plus cluster options into a custom package that suits the needs of organizations as they scale.

Dedicated HashiCorp Contact	✓
12-month or multi-year deal	✓
Discounts are available	✓

Standard

Highly available, fully managed production clusters available in different sizes to suit the needs of organizations as they scale.

Fully managed, HA (3-node) clusters	✓
Vault OSS	✓
Namespaces	✓
24/7 Monitoring	✓
Daily backups	✓
Enterprise/Cloud SLA	✓
Login Multi-factor Authentication	✓

Plus

High availability replication of secrets and policies across multiple data centers to boost performance and lower latency.

Fully managed, HA (3-node) clusters	✓
All Standard features	✓
Vault OSS	✓
Namespaces	✓
24/7 Monitoring	✓
Daily backups	✓
Cross-region cluster performance replication	✓
Replication path filters	✓
Enterprise/Cloud SLA	✓
Login Multi-factor Authentication	✓

HashiCorp

* Current AWS regions: Regions: Oregon (us-west-2), Virginia (us-east-1), Dublin (eu-west-1), London (eu-west-2), Frankfurt (eu-central-1), Singapore (ap-southeast-1), Sydney (ap-southeast-2)