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—infinitive volume and distribution of services, embracing ephemerality and immutability, and ability to deploy onto multiple target environments.

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

<table>
<thead>
<tr>
<th>Reduce risk of data exposure</th>
<th>Reduce the risk of a breach</th>
<th>Increase productivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt sensitive data in transit and at rest using centrally managed and secured encryption keys in Vault, all through a single workflow and API.</td>
<td>Eliminate static, hard-coded credentials by centralizing secrets in Vault and tightly controlling access based on trusted identities.</td>
<td>Enable development teams to automatically consume secrets in their application delivery process and protect sensitive data programmatically through a single API.</td>
</tr>
</tbody>
</table>
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

Offerings

<table>
<thead>
<tr>
<th>Open Source</th>
<th>Enterprise</th>
<th>Cloud*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practitioner</td>
<td>Organizations</td>
<td>HCP Vault on AWS</td>
</tr>
</tbody>
</table>

- Dynamic Secrets
- Secret Storage
- Secure Plugins
- Detailed Audit Logs
- Leasing & Revoking Secrets
- ACL Templates
- Vault Agent
- Init & Unseal Workflow
- Key Rolling
- UI with Cluster Management
- Entities & Identity Groups
- Access Control Policies
- Identity Plugins
- Encryption as a Service
- Transit Backend
- 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

- All Open Source Features
- Disaster Recovery
- Namespaces
- Replication
- Replication Filters
- Read Replicas
- Control Groups
- HSM Auto-unseal
- Multi-factor Authentication
- Sentinel Integration
- FIPS 140-2 & Seal Wrap
- KMIP Support
- Transform
- Resource Quotas - Lease Count
- Splunk Monitoring App
- All Open Source Features
- Disaster Recovery
- Namespaces
- Clustering
- Snapshot & Restore
- Audit Logging
- Reporting

* currently available in private beta