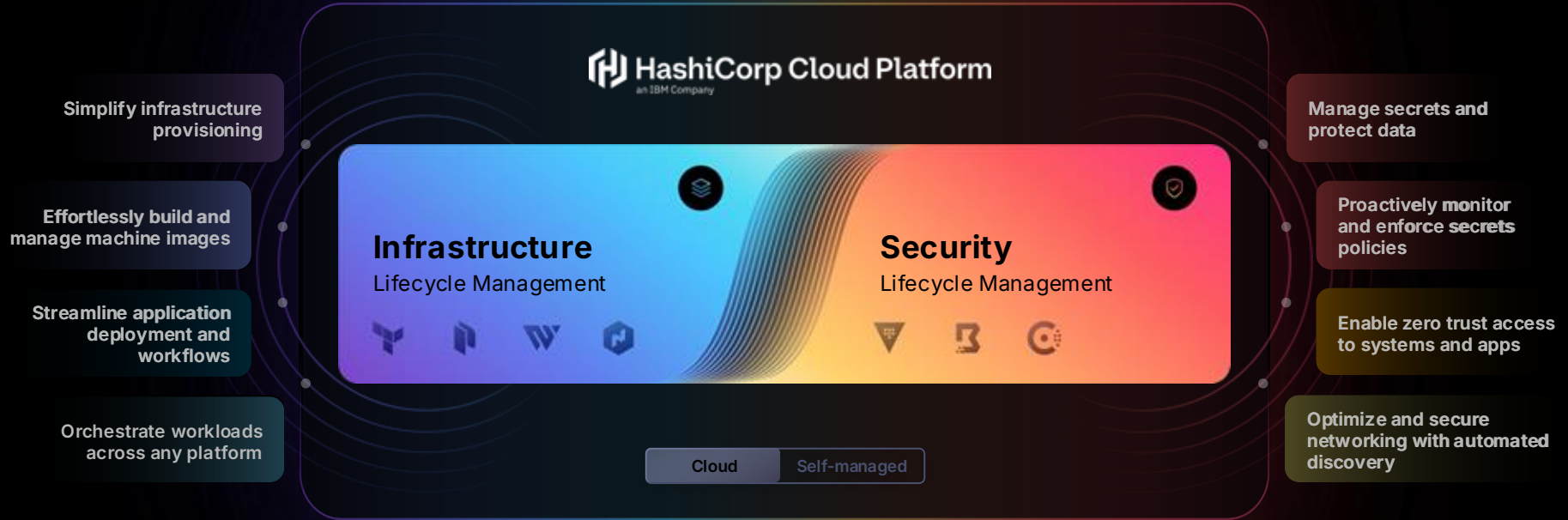


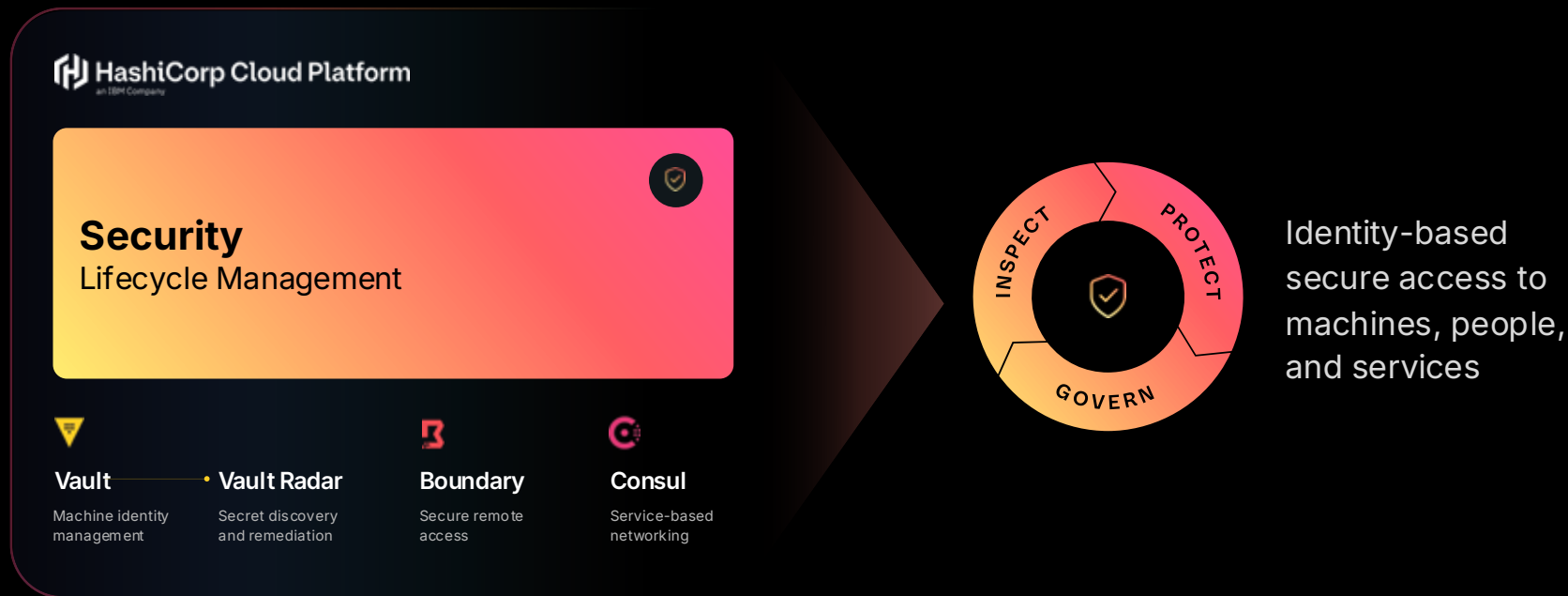
Vault Overview

Modernizing Secret Management

Delivering a portfolio of hybrid solutions



Reduce risk with Security Lifecycle Management



Hybrid Cloud growth requires resilient security



IT estates moving from **static** to **distributed** dynamic environments



Proliferation of cloud providers, tools, and apps exponentially increase threats



Increased investor and **regulatory scrutiny** on cybersecurity risk

Secure your hybrid and multi-cloud environments

Safeguard critical data and systems

 MANAGING DISTRIBUTED & DYNAMIC INFRASTRUCTURE

Minimizing your organization's attack surface while mitigating the risk of data breaches.

Set and enforce identity-based security policy

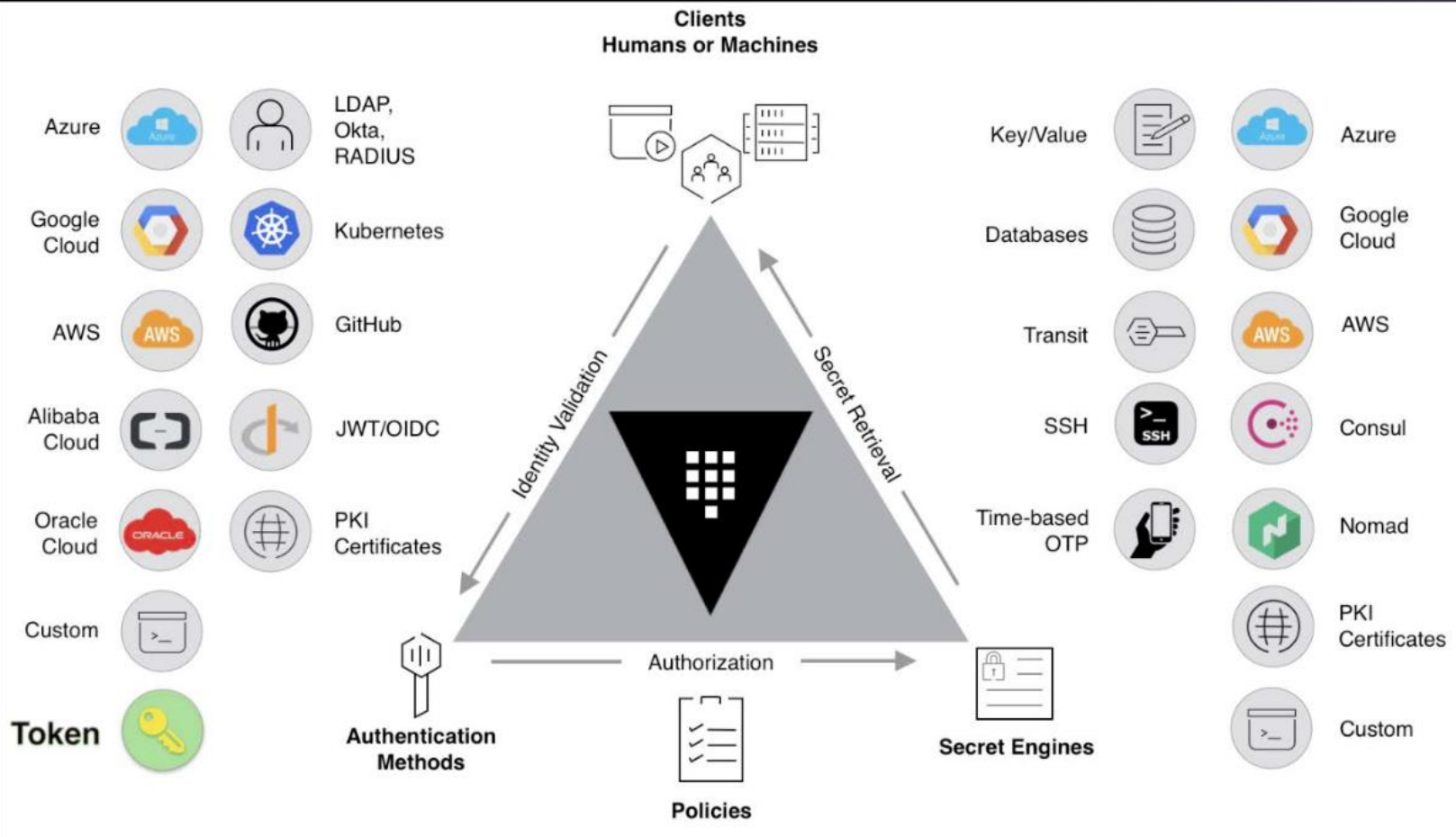
 CENTRALIZING POLICY FOR CLOUDS, APPS, AND TOOLS

Managing decentralized security policies is complex, costly, and hard to scale.

Achieve compliance across environments

 MEETING COMPLIANCE STANDARDS

Maintaining a robust security posture while meeting compliance regulations.



How Vault works



How Vault works

1

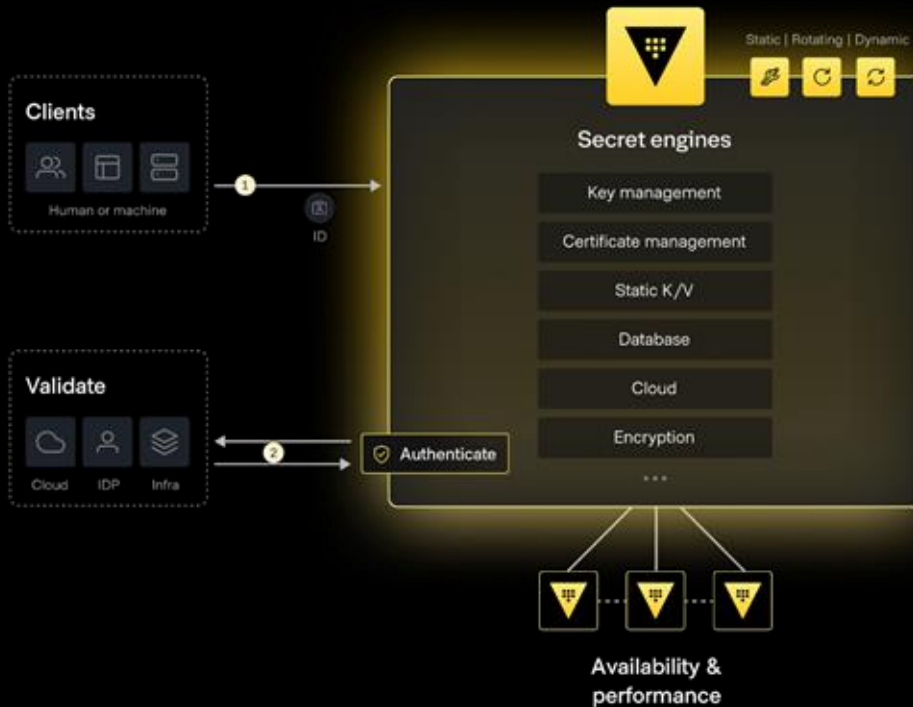
A client provides credentials (ID) to Vault requesting access.



How Vault works

2

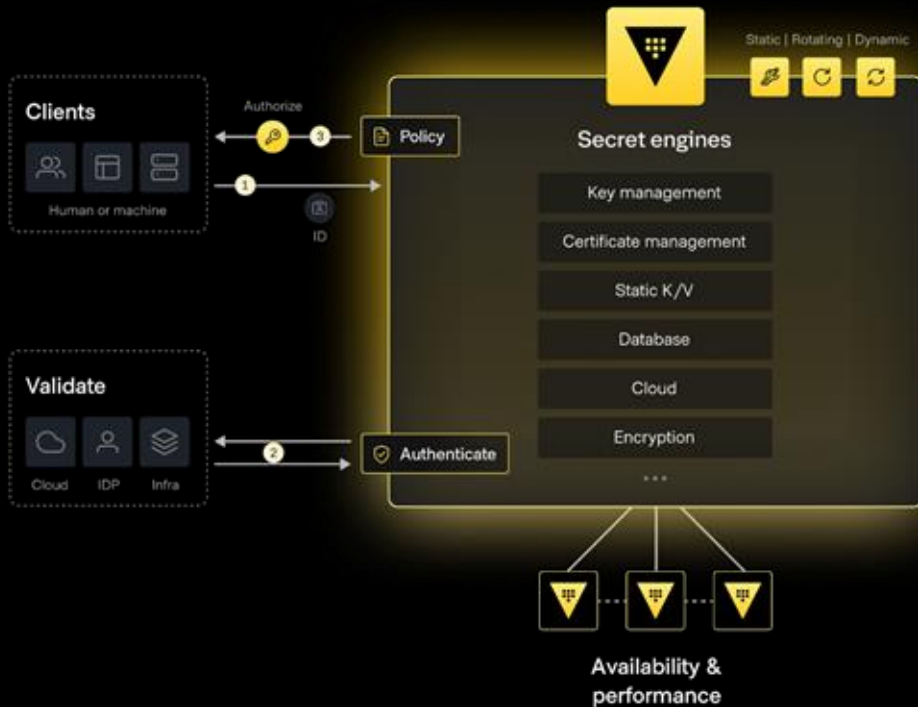
Vault uses authentication plugins to validate the client against the appropriate trusted third-party resource, such as GitHub, LDAP, CSP, or others.



How Vault works

3

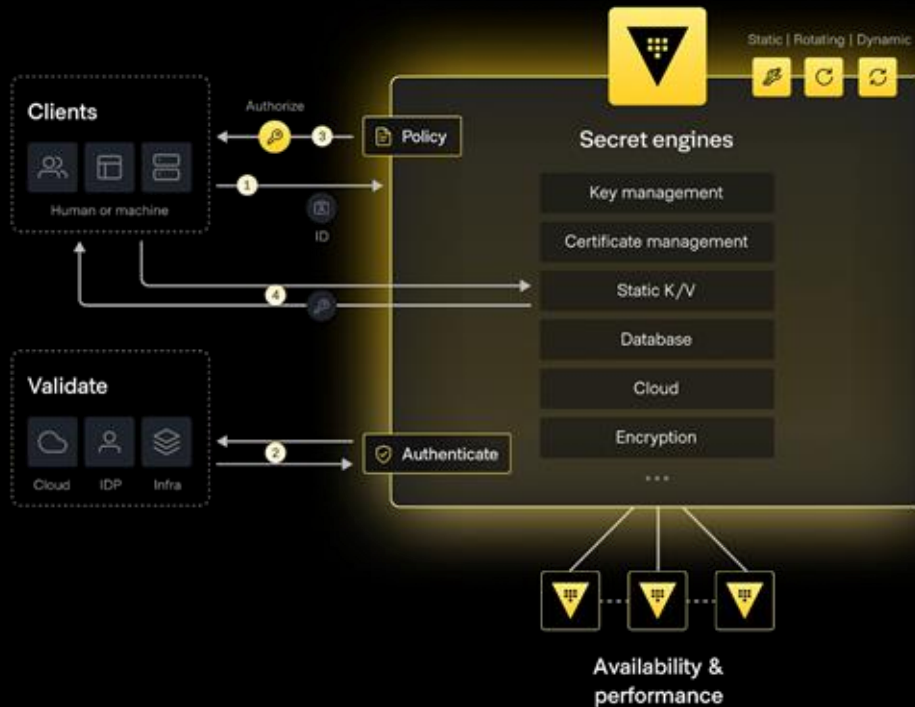
Vault grants access to secrets and encryption capabilities by issuing a token tied to policies associated with the client's identity.



How Vault works

4

Client uses policy-based access to retrieve secrets, keys, and certificates, and perform other operations like data encryption.



How Vault works

5

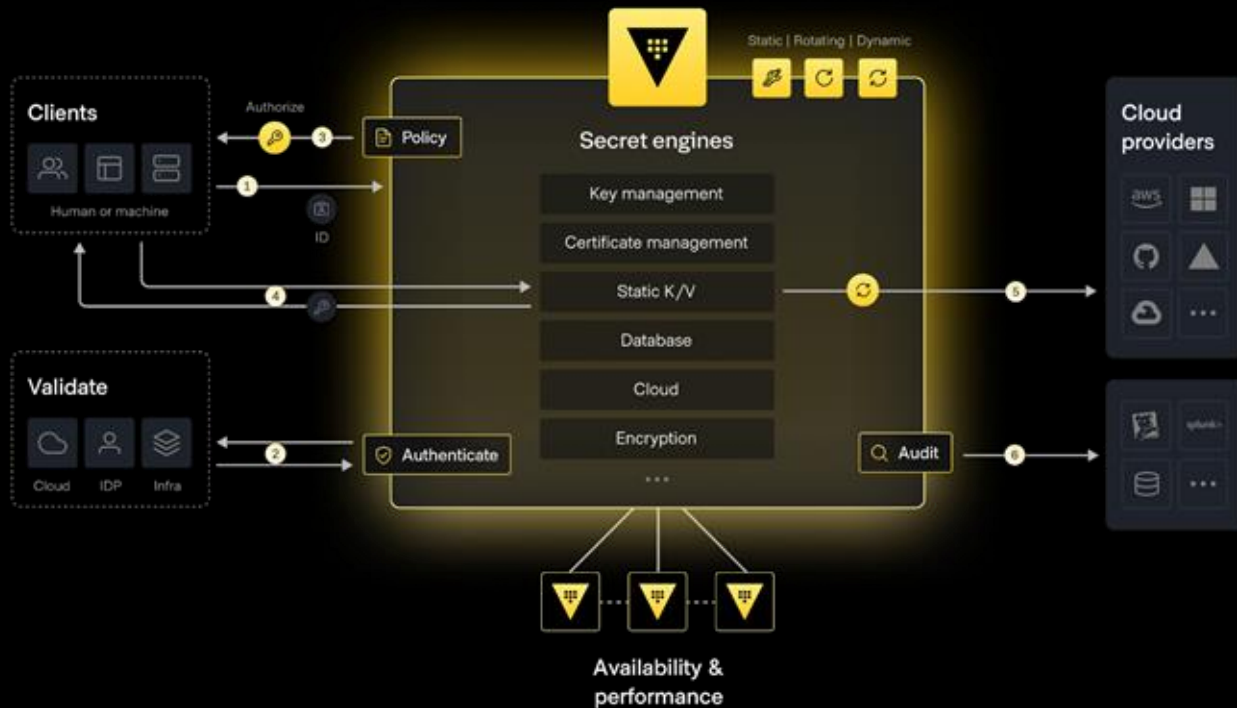
Static secrets can be centrally managed and automatically synced to destination sources.



How Vault works

6

Detailed logs retained for monitoring and compliance.



How Vault works

Secure, scalable access to secrets and sensitive data across multi-cloud and hybrid estates.

- Authenticate and validate using plugins for popular third-party identity providers
- Enforce policy-based access with a central policy store
- Gain visibility and control with audit logging and third-party tools integration for monitoring and compliance
- Enable disaster recovery, high availability, and performance replication



How Vault works

Secure, scalable access to secrets and sensitive data across multi-cloud and hybrid estates.

- Authenticate and validate using plugins for popular third-party identity providers
- Enforce policy-based access with a central policy store
- Gain visibility and control with audit logging and third-party tools integration for monitoring and compliance
- Enable disaster recovery, high availability, and performance replication



How Vault works

Secure, scalable access to secrets and sensitive data across multi-cloud and hybrid estates.

- Authenticate and validate using plugins for popular third-party identity providers
- Enforce policy-based access with a central policy store
- Gain visibility and control with audit logging and third-party tools integration for monitoring and compliance
- Enable disaster recovery, high availability, and performance replication



How Vault works

Secure, scalable access to secrets and sensitive data across multi-cloud and hybrid estates.

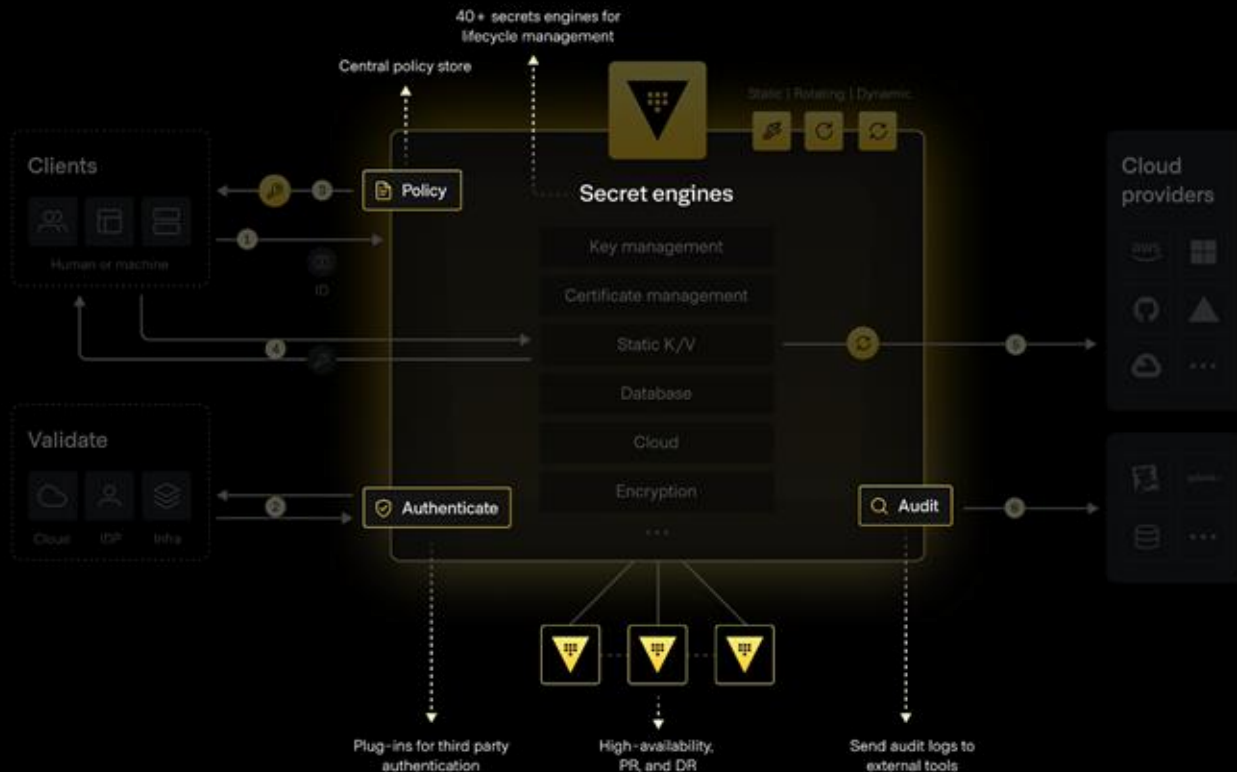
- Authenticate and validate using plugins for popular third-party identity providers
- Enforce policy-based access with a central policy store
- Gain visibility and control with audit logging and third-party tools integration for monitoring and compliance
- Enable disaster recovery, high availability, and performance replication



How Vault works

Automated workflows for dynamic credential provisioning, auto-rotation, and revocation.

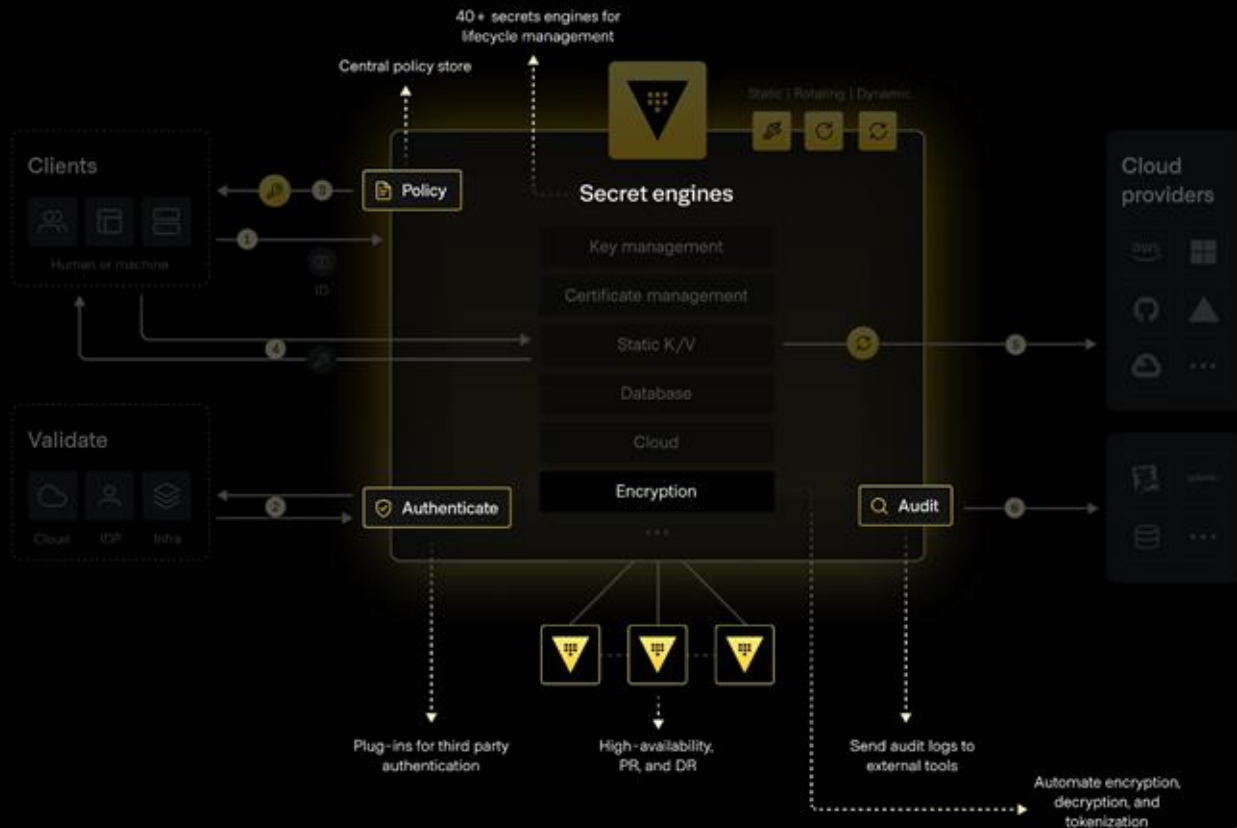
- Secrets engines enable automated lifecycle management of secrets, certificates, keys, and data protection
- Centralized static secrets management supporting native developer workflows with secrets sync



How Vault works

Automated workflows for dynamic credential provisioning, auto-rotation, and revocation.

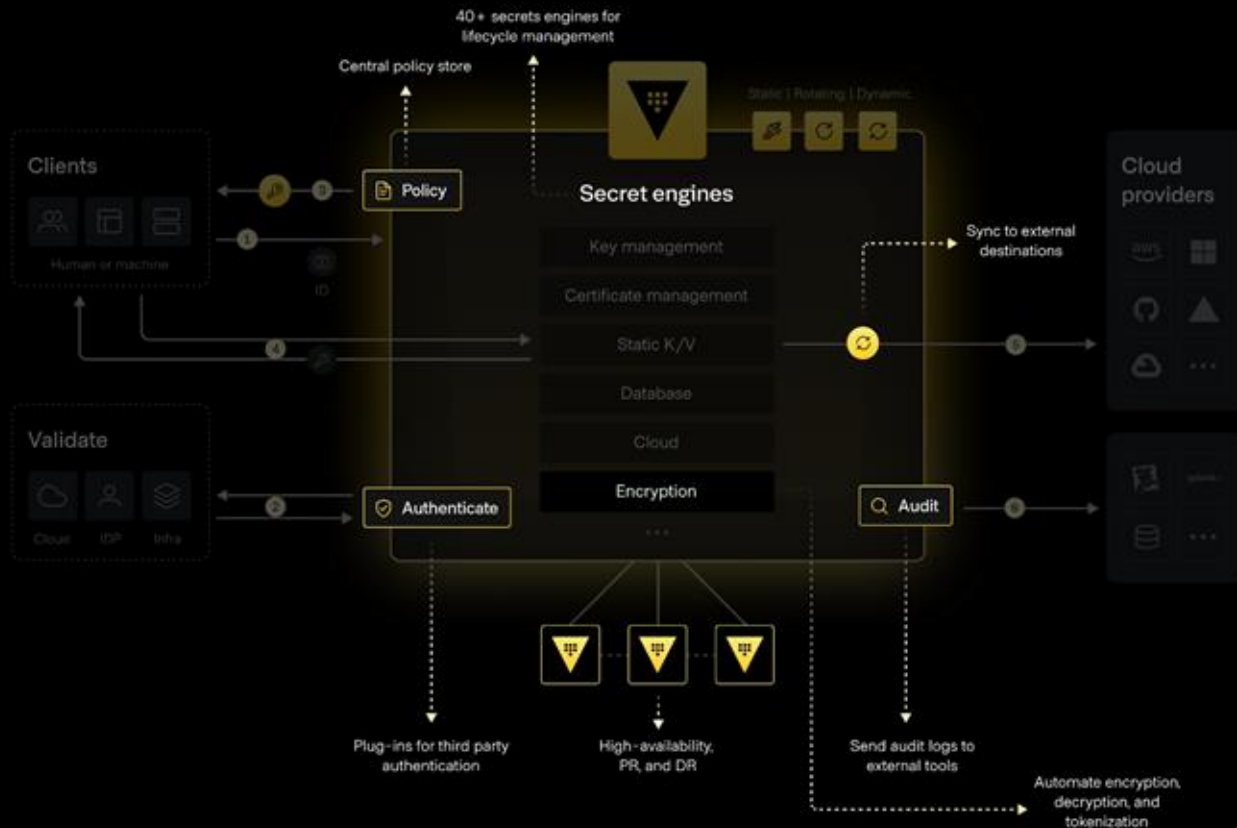
- Secrets engines enable automated lifecycle management of secrets, certificates, keys, and data protection
- Centralized static secrets management supporting native developer workflows with secrets sync



How Vault works

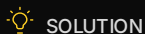
Automated workflows for dynamic credential provisioning, auto-rotation, and revocation.

- Secrets engines enable automated lifecycle management of secrets, certificates, keys, and data protection
- Centralized static secrets management supporting native developer workflows with secrets sync



Secure application identities & protect sensitive data

Secure based on least-privileged access



SOLUTION

Grant the minimum level of identity-based access required for machines across your organization.

Centralize & automate secrets lifecycle



SOLUTION

Automate complex secrets management tasks with centralized security policy from one platform.

Scale security without sacrificing control



SOLUTION

Scale security and across your hybrid estate while meeting strict compliance regulations.

Secure credentials across use cases



Secrets lifecycle management

Protect sensitive data by discovering, centrally storing, accessing, rotating, and distributing dynamic secrets.



Certificate management

Generate, rotate, and revoke certificates on demand, eliminating cumbersome manual processes.



Key management

Distribute, rotate, enable, and disable keys to maintain centralized control and full lifecycle management of cryptographic keys.



Data protection

Protect data in-transit and at rest by centrally managing and automating encryption keys to ensure security parameters are met.

Current Operational Challenges Mapped

Resiliency



Lack of DR reduces availability and makes the system vulnerable to outages.

Scalability



Without scalable architecture, operational burden increases as the organization grows.

RBAC



Manual handling shows a lack of proper access controls and automation around critical secrets.

Compliance



Lacking audit trails and access logs directly affects regulatory compliance readiness.

Governance, risk, & compliance



Unsupported software introduces governance and risk management issues over time.

Empower teams with Vault's capabilities

Resiliency



Disaster Recovery
Automatic Snapshots

Scalability



Performance
Replication
Performance Standby
Nodes

RBAC



Namespaces
Sentinel
Control Groups

Compliance

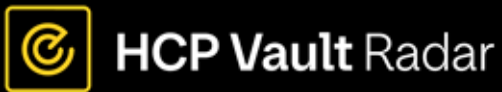


HSM integrations
FIPS 140-2
ISO
...

Governance, risk, & compliance



SOC Compliance
Auditing
24x7 Support



Discover unmanaged secrets

HCP Vault Radar leverages 300+ algorithms to discover sensitive data in Git-supported version control and collaboration platforms.

Scan diverse data sources

HCP Vault Radar integrates with common tools including Git-supported VCS, JIRA, and Confluence.

Remediate leaked secrets

HCP Vault Radar offers customizable remediation guidance based on secret type.

Securing sensitive data

Once sensitive data is identified, HCP Vault Radar provides functionality to secure data in Vault.



Dev



Production



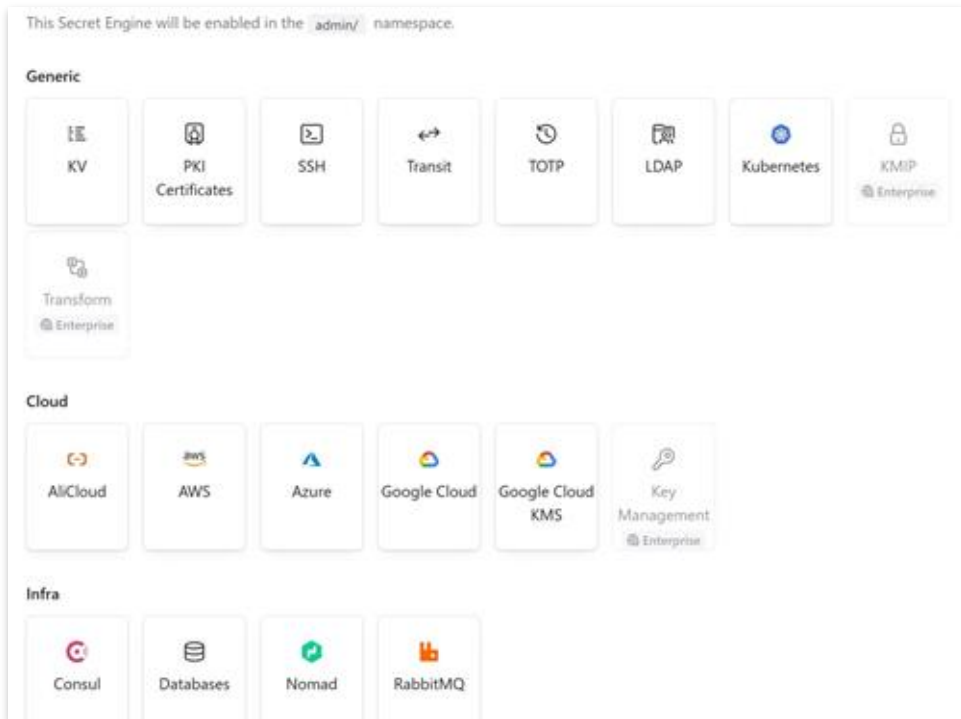
CI

Secrets engines

Vault secrets engine

Safely store credentials, keys, and other types of secrets without deploying and managing a complex key management infrastructure.

- Store secrets with the KV secrets engine to quickly store and retrieve sensitive information
- Orchestrate workflows with stored secrets for creating dynamic credentials (AWS), certifying transactions (SSH), or privileged access management (Active Directory)
- Manage access with ACL policies and audit all transactions via the audit log
- All data is automatically encrypted in flight (TLS) and at rest (AES 256 GCM)

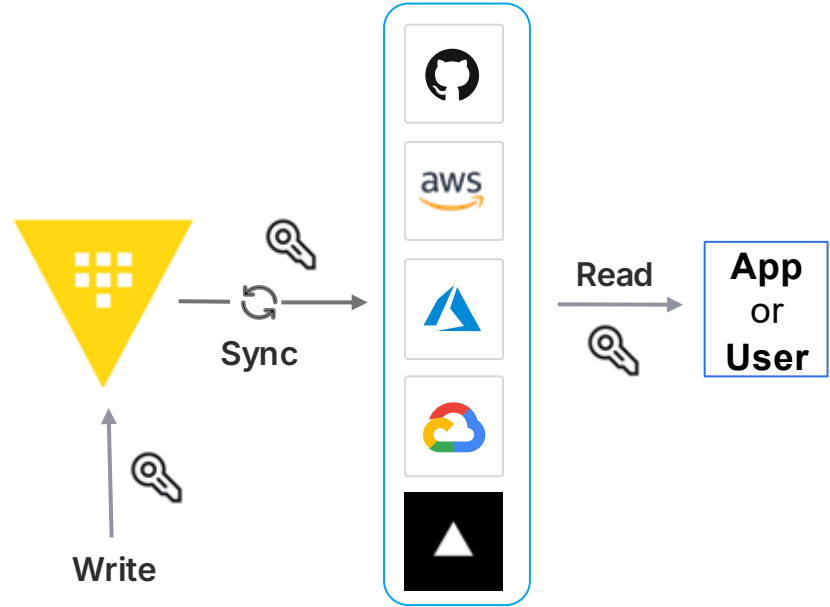


Secrets sync

Unified workflow

Keep secrets centralized in Vault while syncing secrets to native platforms and tools such as CSPs, GitHub, and Vercel.

- Easy to configure and sync with new interface
- Enable centralized visibility and control using current workflows with native tools
- Automatically propagate updates in all destinations
- Currently supports KVv2 secrets engine with more types coming

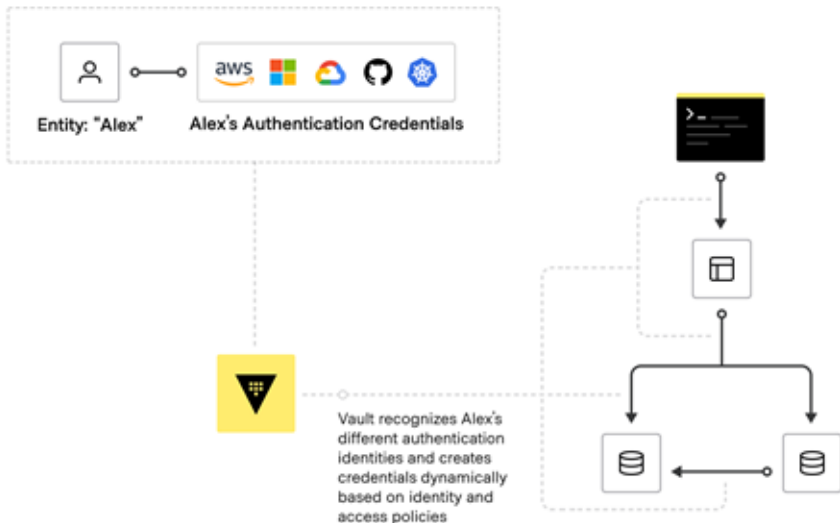


Identity-based access

Authenticate and access different clouds, systems, and endpoints

Leverage any trusted source of identity to enforce system and application access.

- Secrets management enables centrally managing secrets
- Encrypting data keeps application data secure
- Identity-based access allows easy integration across systems and clouds



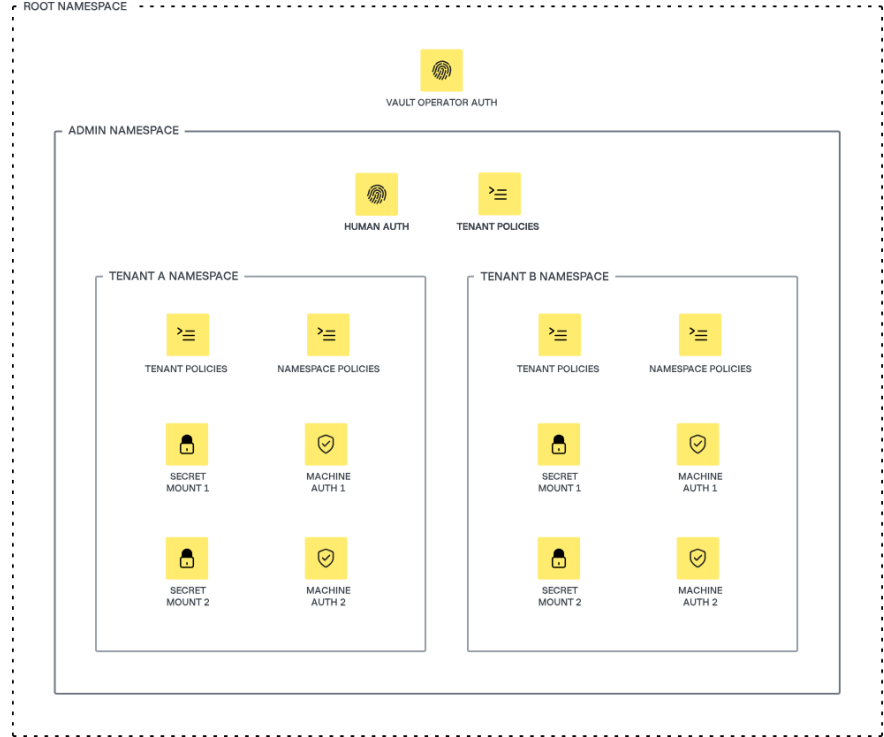
Namespaces

Namespaces for management, secure multi tenancy

Create isolated “Vaults within a Vault” that allow for parent admins to manage configurations but let teams manage their own policies, secrets, and identities.

Enterprise

- Allow teams to self-manage segmented Vault environments with their own auth methods, secret engines, and policy and identity infrastructures
- Isolate tenant environments for security and compliance
- Enforce organizational compliance across isolated teams



ACL policies and Sentinel

ACL policies and Sentinel

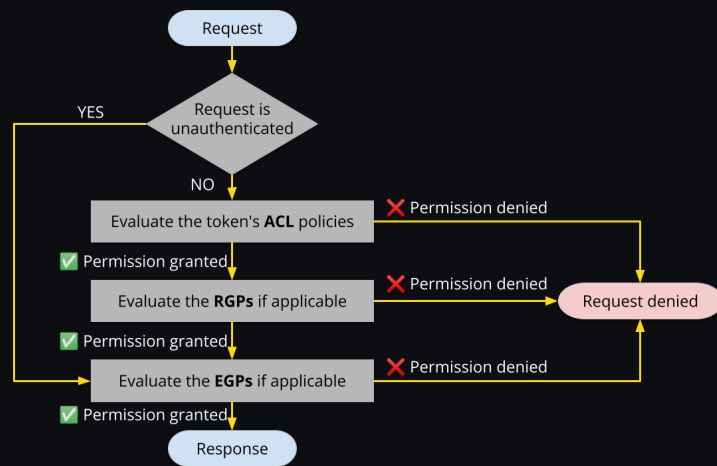
Vault provides the flexibility to easily apply policies to entities and groups across its unified identity infrastructure.

- Use ACL policies to control RBAC easily and logically for multiple credentials and applications in one line of code

Enterprise

- With Sentinel, apply additional policies on how users connect via specific authentication methods or on accessing specific secrets
- Apply additional controls requiring multi-factor authentication (MFA)

Vault Authentication → Authorization Flow

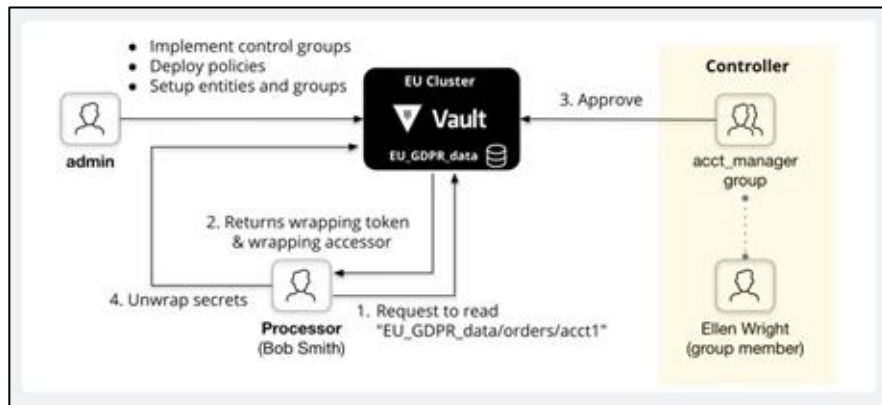


Control groups

Meeting GDPR requirements

Control groups add additional authorization factors to be required before processing requests to increase the governance, accountability, and security of your secrets.

- When a control group is required for a request, the requesting client receives the wrapping token in return
- When all authorizations are satisfied, the wrapping token can be used to unwrap the requested secrets

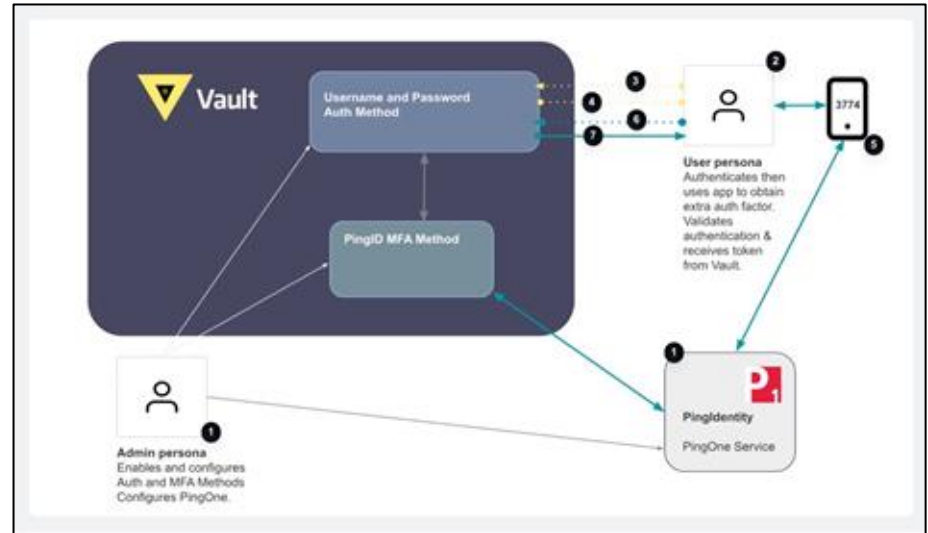


Secure access – Enterprise MFA

Access governance

Vault Enterprise provides multi-factor authentication (MFA), enabling path and namespace targeted granular access.

- Supported types
 - TOTP
 - Okta
 - Duo
 - PingID

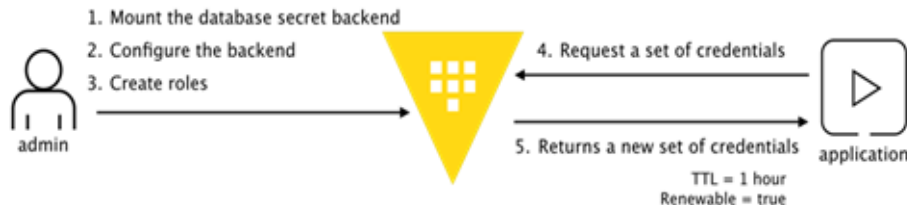


Dynamic secrets

Secure and automated

Vault grants tokens for access, not credentials, to ensure least privilege with security and ensure break-glass functionality.

- Secret created "just in time" at read time
- Set expiry to ensure that access is automatically revoked on time
- Revoke outstanding access at will
- Break-glass functionality to halt all access in critical situations



Dynamic secrets

Example: AWS credentials

- Easily generate time-based credentials based on your policy

```
$ vault read aws/creds/my-role
```

Key	Value
---	-----
lease_id	aws/creds/my-role/0bce0782-32aa-25ec-f61d-c026ff22106e
lease_duration	768h
lease_renewable	true
access_key	AKIAJELUDIANQGRXCTZQ
secret_key	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
security_token	<nil>

Ephemeral secrets

Secrets do not persist

Temporary secrets used during `terraform apply` are not persisted in the Terraform state. Secrets can be:

- Consumed at runtime only and never persisted to Terraform's state, leveraging [Terraform Ephemeral Resources](#).
- Safely handled in memory to reduce long-term exposure.
- Used without creating secret sprawl to keep your infrastructure code secure and clean.

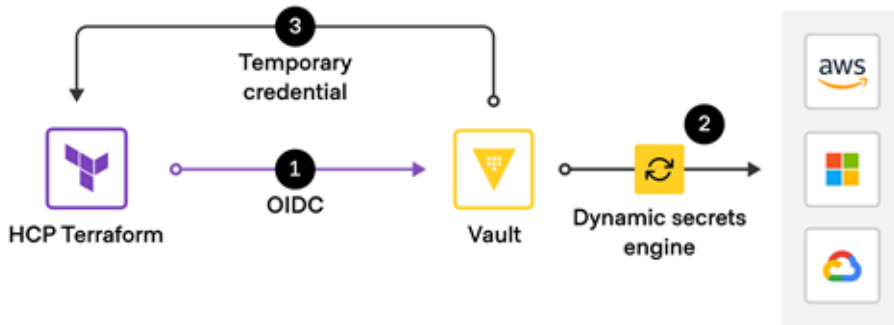


Vault-backed dynamic credentials

Centralized credential management

Combine the power of dynamic provider credentials and HashiCorp Vault dynamic secrets engines.

- Authenticate Terraform runs to Vault using JWT/OIDC auth method
- Vault generates temporary cloud credentials for AWS, Azure, or Google Cloud
- Secrets are injected into the Terraform agent environment for use with providers
- Credentials are revoked immediately after each run phase

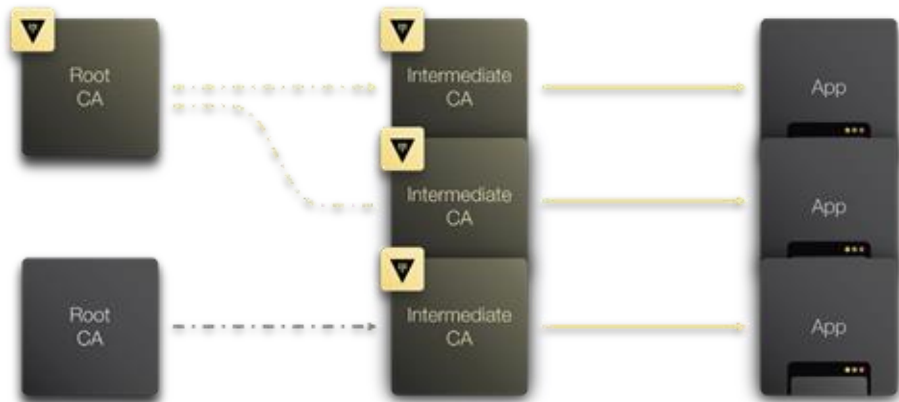


Certificate authority (TLS/SSH, PKI)

Dynamic configurable architecture

Vault supports a flexible architecture and hierarchy so it can be configured to work across your environments. Vault can be configured as the internal root CA or intermediate CA.

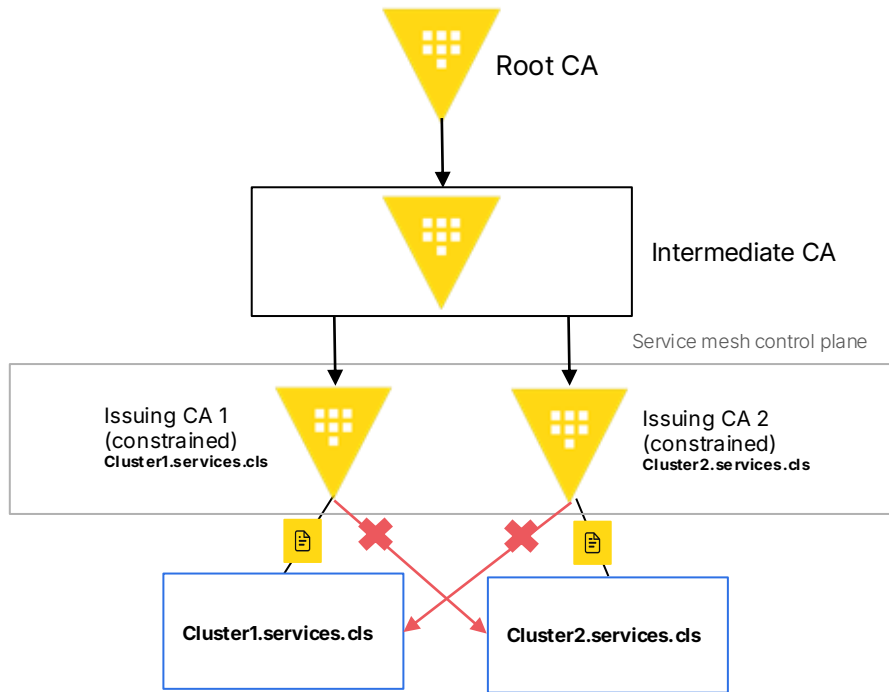
- Support for multiple root and intermediate CAs, depending on the needs of your environment
- Configure to work with existing external CAs



PKI support for constrained CA

Isolate PKI workloads with constrained CA's

- Vault PKI provides the capability to configure intermediate CAs with customer defined constraints (permitted URI , IPs, excluded DNS...).
- Enables customers to implement security best practices, and delegated administration of PKI.

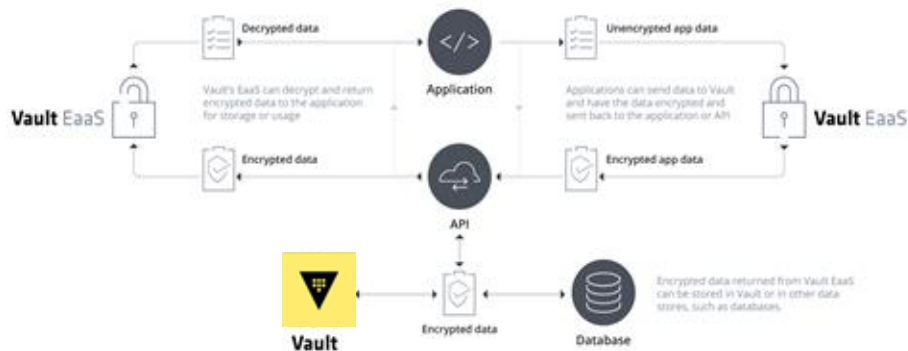


Transit secrets engine

Use the transit secrets engine to handle encryption, decryption, and cryptographic signing

With the transit secrets engine, Vault can enable users and applications to enable cryptographic workloads without a key management infrastructure.

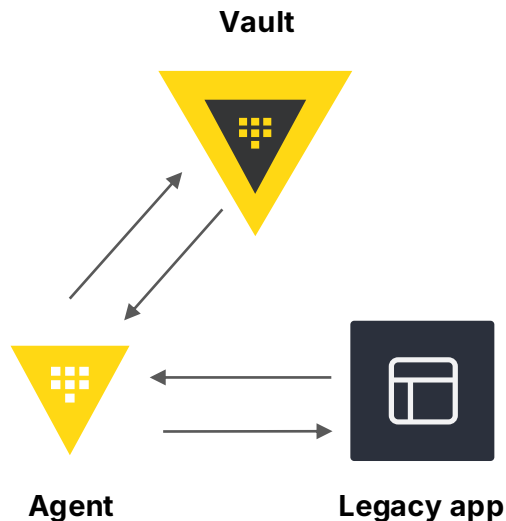
- Automate encryption, decryption, and cryptographic hashing and signing without deploying new infrastructure
- Quickly create and manage keys (including rotation) without deploying complex key management servers
- Support AES 256, RSA (2048 and 4096), ECDSA-p256, ed25519, ed25519PH, chacha20-poly1305, and more



Vault Agent

Vault Agent is a client daemon that provides the following features:

- **Auto-auth:** Automatically authenticates to Vault and manages token renewal for dynamic secrets
- **API Proxy:** Acts as proxy for Vault's API, allowing applications to communicate with Vault through the agent
- **Caching:** Provides client-side caching of responses, including newly created tokens and leased secrets, reducing load on Vault and improving performance
- **Templating:** Renders user-supplied templates using tokens generated by auto-authentication, facilitating application secret integration
- **Process supervisor mode:** Runs a child with Vault secrets injected as environment variables, ensuring secure and dynamic secret management

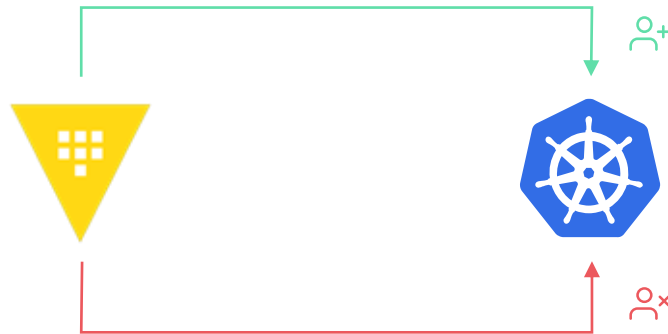


Kubernetes secrets management

Kubernetes

Instead of sharing credentials and tokens across pods and services, Vault enables applications and services to authenticate and request their own unique credentials. Vault also provides a variety of options for Vault and Kubernetes to securely introduce secrets into applications and infrastructure. Vault supports the following Kubernetes integrations:

- **Vault-k8s:** Provides access to Vault secrets by deploying a vault-agent sidecar into a Kubernetes Pod
- **Vault-csi-provider:** Fetches secrets stored in Vault and uses the Secrets Store Container Storage Interface (CSI) driver interface to mount them into Kubernetes Pods
- **Vault Secrets Operator (VSO) for Kubernetes:** More native method to retrieve and sync Kubernetes Secrets that include post-rotation updates

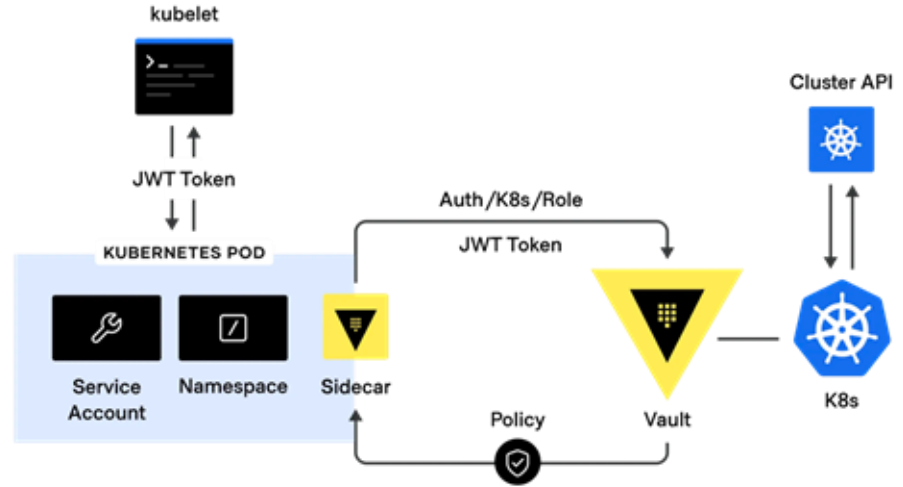


Kubernetes secrets management

Sidecar agent injector

Enable access to Vault secrets by Kubernetes applications that don't have native Vault logic built in.

- Allow automatic injection of secrets into the pod file system
- Allow applications to only concern themselves with finding a secret at a filesystem path, rather than managing the auth tokens and other mechanisms

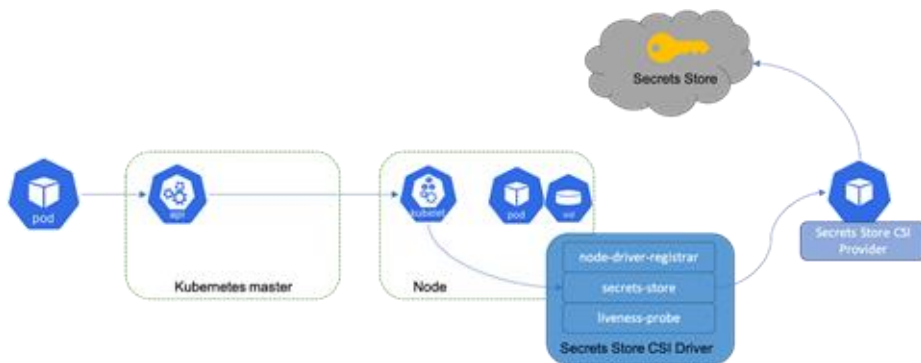


Kubernetes secrets management

CSI provider

Fetches secrets stored in Vault and uses the Secrets Store Container Storage Interface (CSI) driver interface to mount them into Kubernetes Pods.

- The Vault CSI Provider authenticates with Vault as the service account of the pod that mounts the CSI volume.
- Kubernetes and JWT auth methods are supported. The pod's service account must be bound to a Vault role and a policy granting access to the secrets desired.
- The secret is retrieved from Vault and populated to the CSI secrets store volume during the ContainerCreation phase. This means that pods will be blocked from starting until the secrets have been read from Vault and written to the volume.



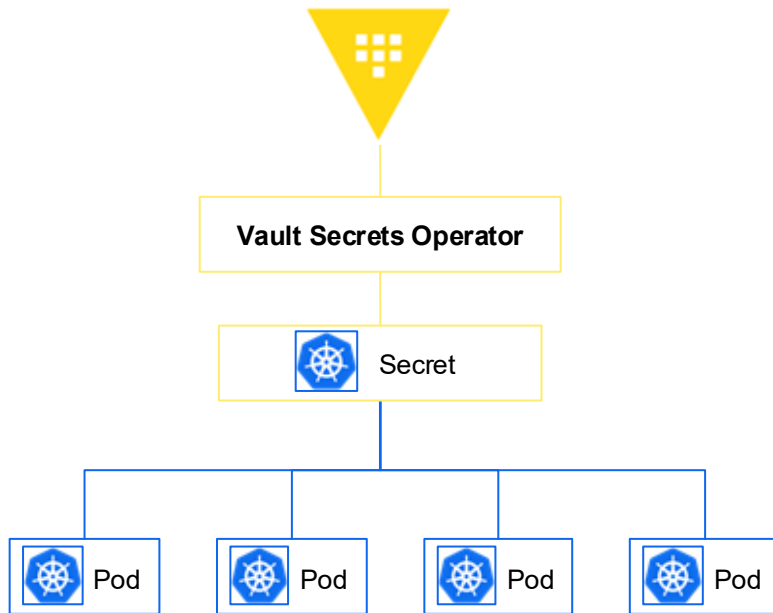
Kubernetes secrets management

Vault Secrets Operator for Kubernetes

Using controller-runtime and custom resource definitions to allow application developers to consume Vault secrets directly from Kubernetes. The operator ensures Vault secrets remain synchronized in the cluster.

Supports synchronizing all classes of Vault secrets:

- Dynamic: Database credentials, cloud credentials, etc.
- PKI: TLS certificates
- Static: Key-value
- Google auth for Workload Identity on GKE
- OpenShift OLM support for instant upgrades
- Secret transformation via templating
- Instant secret revocation, config updates



Pattern comparison

[Comparison Blog Article](#)

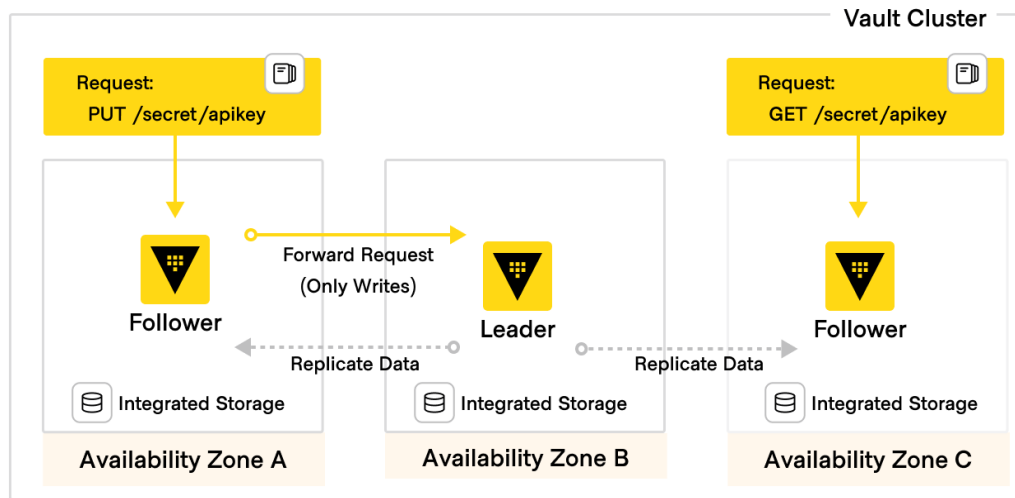
	Agent Sidecar	CSI	Vault Operator
Secret projection	Shared memory volume Environment variable	Ephemeral disk Environment variables Kubernetes Secrets	Kubernetes Secrets, Kubernetes Secret volumes Environment variables
Secret scope	Global	Global	Global
Secret types	All secrets engines (Static and dynamic)	All secrets engines (Static and dynamic)	All Vault secrets engines (Static and dynamic)
Secret templating	Yes	No	Yes
Secret size limit	No limit (both storage types)	No limit (both storage types)	No limit (both storage types)
Secret definitions	CLI / API / UI	CLI / API / UI	Vault CLI / API
Encryption	Yes (at rest and in transit)	Yes (at rest and in transit)	In transit via TLS, at rest ** only if 'etcd' storage is encrypted
Secret rotation	Yes	No	Yes
Secret caching	Yes	No	Yes
Auditability	Yes	Yes	Yes
Deployment method	1 shared Kubernetes cluster service + 1 sidecar container per application pod	Daemonset	Kubernetes deployment
Vault agent support	Yes	No	No
Helm support	Yes	Yes	Yes



Availability and resilience

High availability

- Vault can run in a high-availability (HA) mode to protect against outages by running multiple Vault servers
- Three types of nodes:
 - **Active:** Reads and writes in a basic cluster configuration
 - **Standby:** Forwards requests to Active Node in basic cluster configuration
 - **Performance standby:** Can process read requests; forwards write requests to active node. [Vault Enterprise]
- Storage backend must support HA



Availability and resilience

Performance replication

Secrets may be accessed from any location, through one to many replication, which asynchronously replicates changes to all of the secondary clusters.

Replication occurs for the following:

- Secrets
- Policies
- Secret, auth, and audit backends config
- Access tokens are NOT replicated



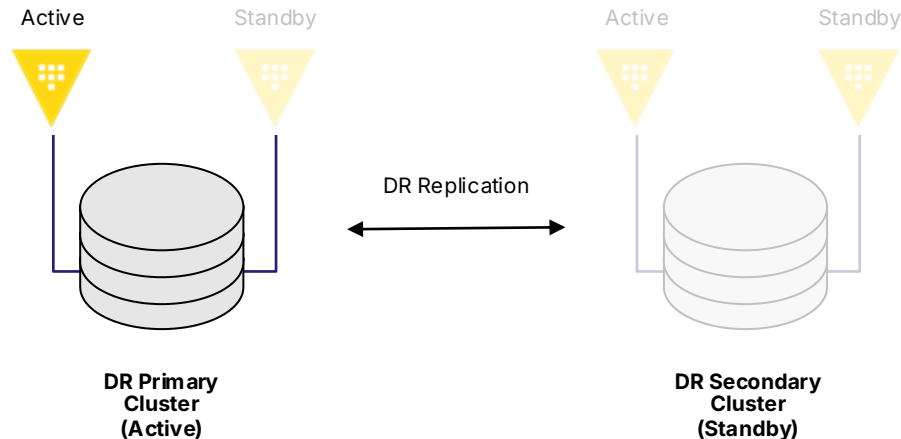
Note: To comply with **GDPR**, use Vault's **path filters** feature to abide by data movements and sovereignty regulations while ensuring performance access across geographically distributed regions.

Availability and resilience

Disaster recovery

All secrets and access tokens replicated to meet disaster recovery and business continuity requirements.

- Provides warm standby
- Protects against regional/datacenter outage
- Replicates everything
- Design clusters for HA per region/datacenter



Availability and resilience

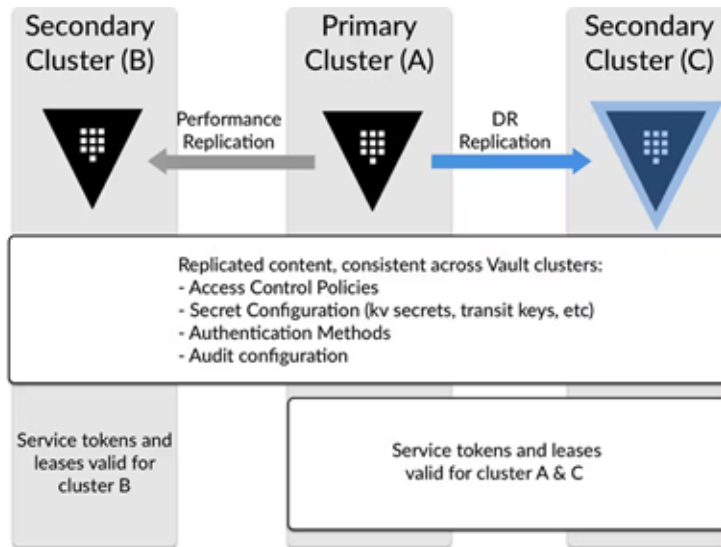
Performance vs. DR replication

Primary clusters

- Stream data to both disaster recovery secondary clusters and performance replication clusters

Secondary clusters

- In DR replication, secondary clusters do not forward service read or write requests until they're promoted and become a new primary — they essentially act as a warm standby cluster



Audit logs

Monitor events for security and compliance across infrastructures

With Vault's audit log, monitoring secret access across multiple clouds and environments is easy and automated.

- Push audit logs to syslog, file, or socket for easy consumption by SIEM or log management software
- One schema for all cloud environments and applications

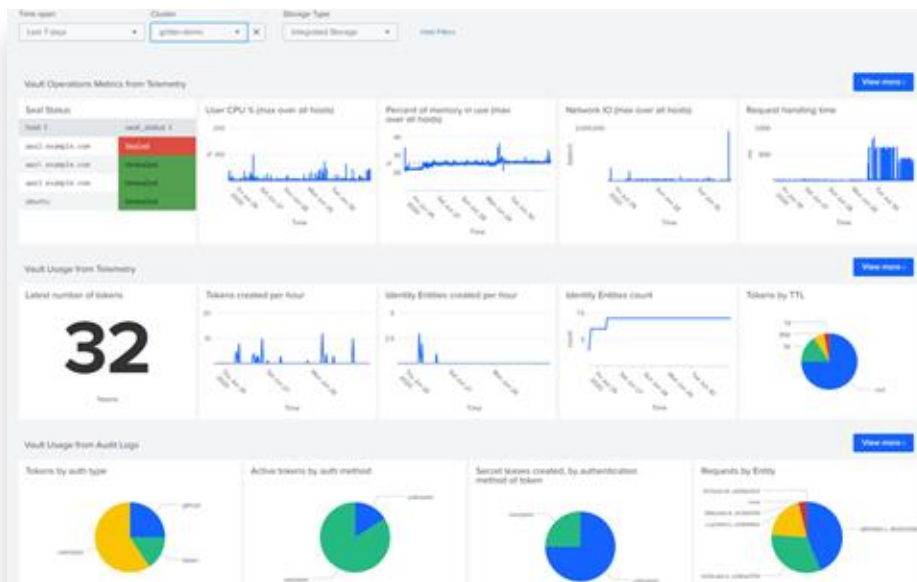
```
{
  "time": "2018-02-01T14:40:03.226772711Z",
  "type": "response",
  "auth": {
    "client_token": "hmac-
sha256:09b0c08f04bc69bf10a0b8c1d2fa3d84ad4efc470d4f3125950cb5979e606843",
    "accessor": "hmac-
sha256:34d5c7474ecac552772fbc091aee99dfc60b6461d42504a117b09928552cfad8",
    "display_name": "root",
    "policies": [
      "root"
    ],
    "metadata": null,
    "entity_id": ""
  },
  "request": {
    "id": "1af553d4-f2a8-4fac-66ec-b333b392011a",
    "operation": "create",
    "client_token": "hmac-
sha256:09b0c08f04bc69bf10a0b8c1d2fa3d84ad4efc470d4f3125950cb5979e606843",
    "client_token_accessor": "hmac-
sha256:34d5c7474ecac552772fbc091aee99dfc60b6461d42504a117b09928552cfad8",
    "path": "secret/audittest",
    "data": {
      "value": "hmac-
sha256:f0dbb2e3574400553d45f259391f17a2c09e7845deb310faf3151ea2527e6c51"
    },
    "policy_override": false,
    "remote_address": "172.28.128.6",
    "wrap_ttl": 0,
    "headers": {}
  },
  "response": {},
  "error": ""
}
```

Monitoring integrations

Splunk

An application is available in Splunkbase to easily extract metrics and provides the following dashboards:

- Cluster summary
- Operational metrics
- Usage metrics
- Audit log interpretation
- Backend storage

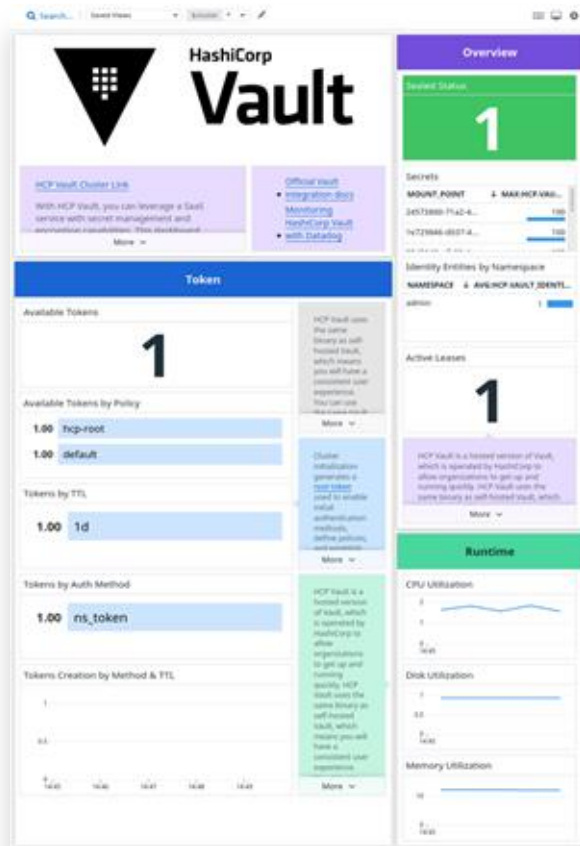


Monitoring integrations

Datadog

Datadog provides monitoring with 700+ turnkey integrations, sophisticated alerting, and log analytics. You can automatically:

- Detect potential security threats
- Correlate data across your stack
- Track long-term performance trends

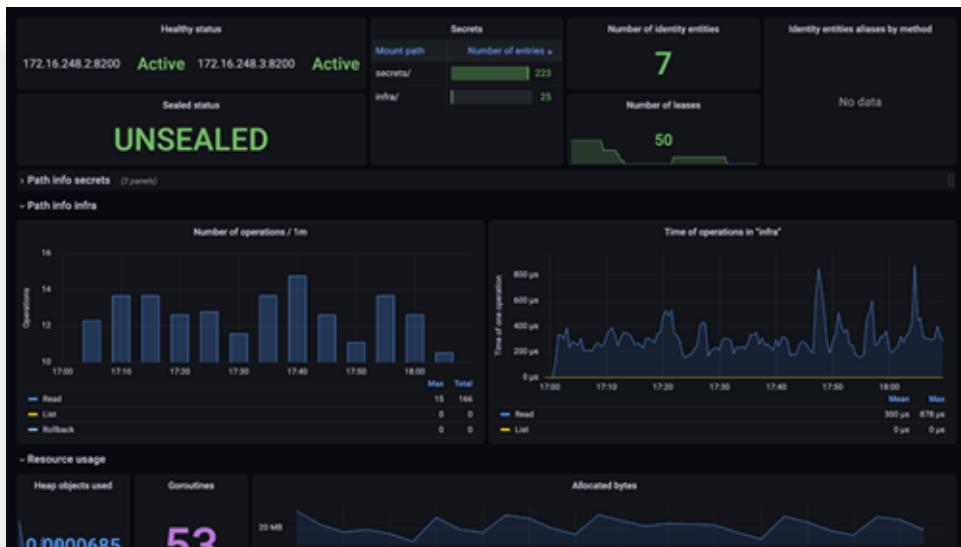


Monitoring integrations

Grafana

Preconfigured Grafana dashboards can be integrated with HCP Vault or Vault Enterprise to monitor:

- Number of secrets in KV storages
- Operations in KV storages
- Number of tokens by different types
- Operations with tokens
- Memory usage by Vault
- Requests to Vault



Advanced Data Protection

Advanced Data Protection (ADP) is a Vault Enterprise/HCP Vault Dedicated module focused on advanced data transformation and securely connecting to, controlling, and integrating with advanced encryption keys. ADP is comprised of three main components:

- Transform secrets engine
- Key management secrets engine (KMSE)
- Key management interoperability protocol secrets engine (KMIP)



Requires the following licenses

- Vault Enterprise + ADP
- HCP Vault Dedicated Plus

Transform secrets engine

Vault's transform secrets engine supports a broad range of capabilities to meet advanced data security requirements.

- Format-preserving encryption
- Tokenization
- Data masking

transform

template

Create Template

This transform template will be created in the `api` namespace.

Name

Templates allow Vault to determine what and how to capture the value to be transformed. This cannot be edited later.

phone-number-tmpl

Pattern

The template's pattern defines the data format. Expressed in regex.

1

(\d{3})

(\d{3})

(\d{3})

(\d{4})

Validation

Advanced templating

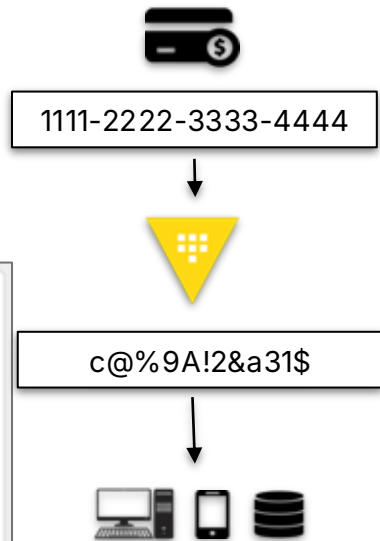
Alphabet

Alphabet defines a set of characters (UTF-8) that is used for HFE to determine the validity of plaintext and ciphertext values. You can choose a built-in one, or create your own.

buildingalphnumeric

Create template

Cancel

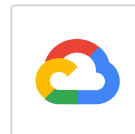


Key management secrets engine

The Vault key management secrets engine (KMSE) provides distribution and lifecycle management features for cloud provider keys.

Currently, it manages keys for the following cloud providers:

- Amazon AWS KMS
- Azure Key Vault
- GCP Cloud KMS



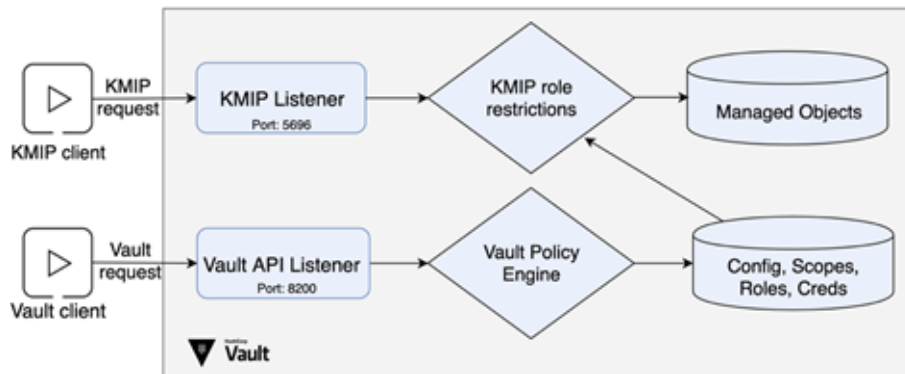
Key management interoperability protocol

KMIP support

The KMIP secrets engine allows Vault to act as a KMIP server for clients that retrieve cryptographic keys for encrypting data via the KMIP protocol.

Support four fundamental operations.

- **Import** - Imports a managed object into Vault
- **Query** - Displays Vault's capabilities as a KMIP server
- **Encrypt** - Performs an encryption operation on the provided data
- **Decrypt** - Performs a decryption operation on the provided data





Thank you

