Vault

Implementation Foundations

Module: Architecture

An Overview of Vault (1/2)

- The Vault Workflow
- Authentication
  - Policies
  - Secrets
- Vault Terminology

An Overview of Vault (2/2)

- Vault Server Architecture
  - High Availability Mode
  - Vault Integrated Storage
  - Network Connectivity
- Vault Replication
  - Disaster Recovery
  - Performance Replication

Introduction To Vault

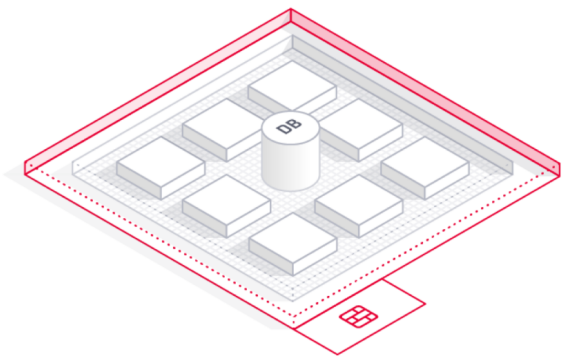
The Shift From Static to Dynamic

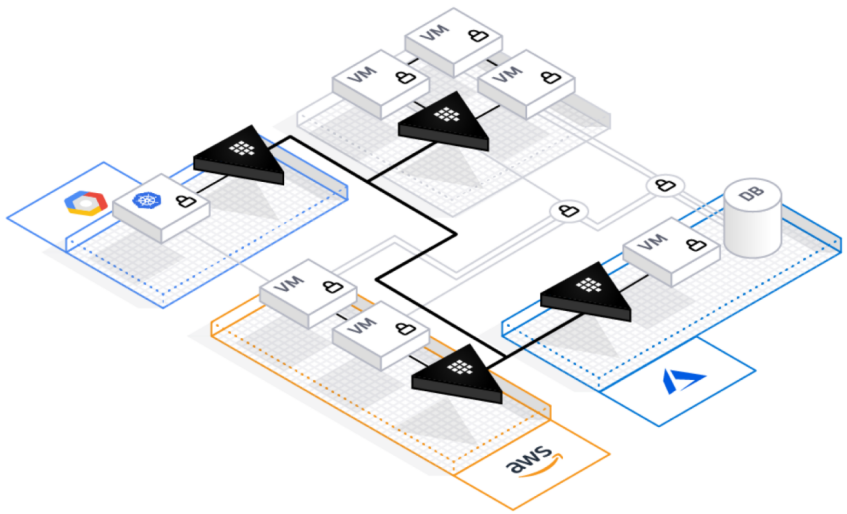
Static Infrastructure

Host-based identity

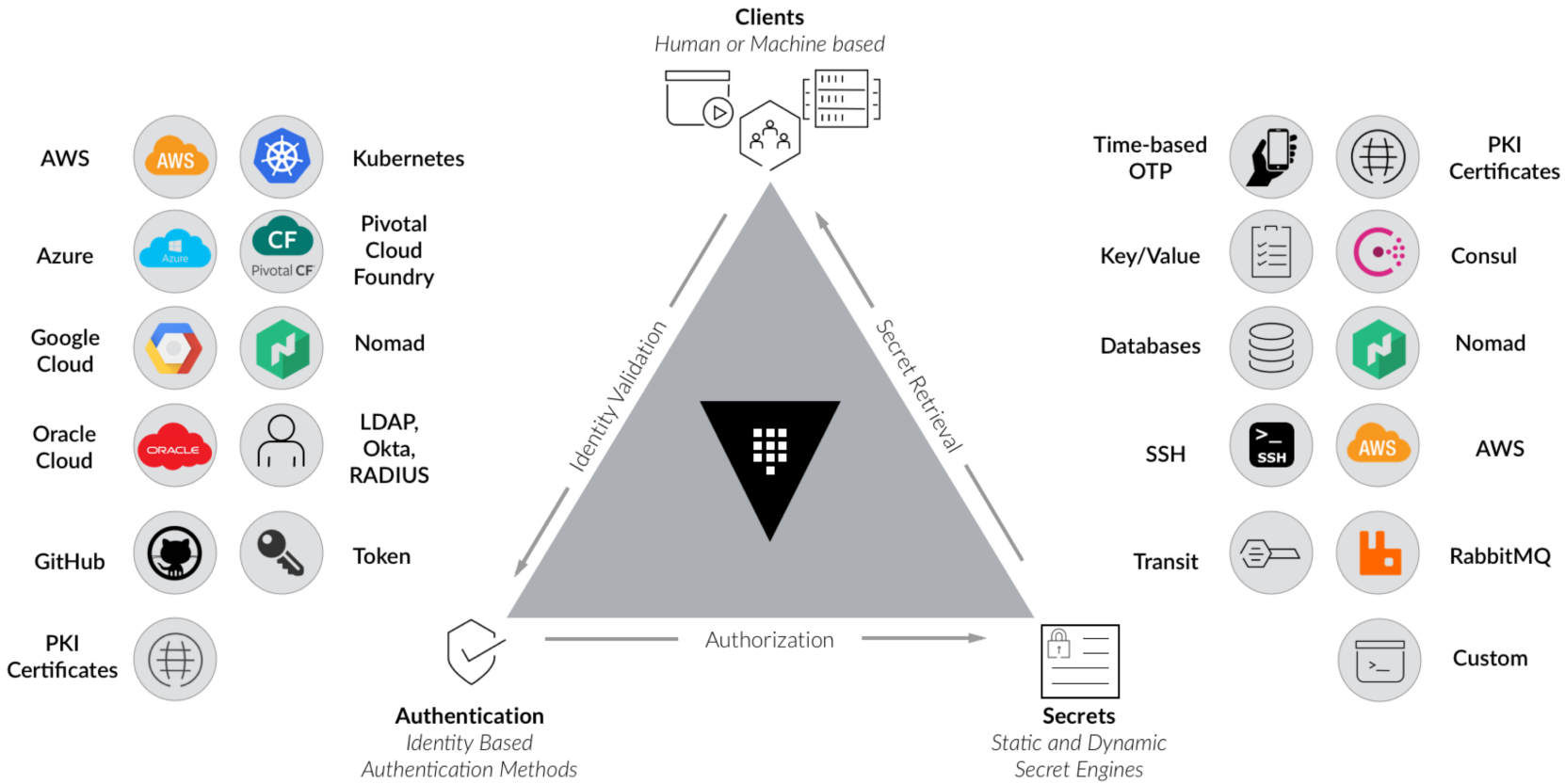
Dynamic Infrastructure

Service-based identity

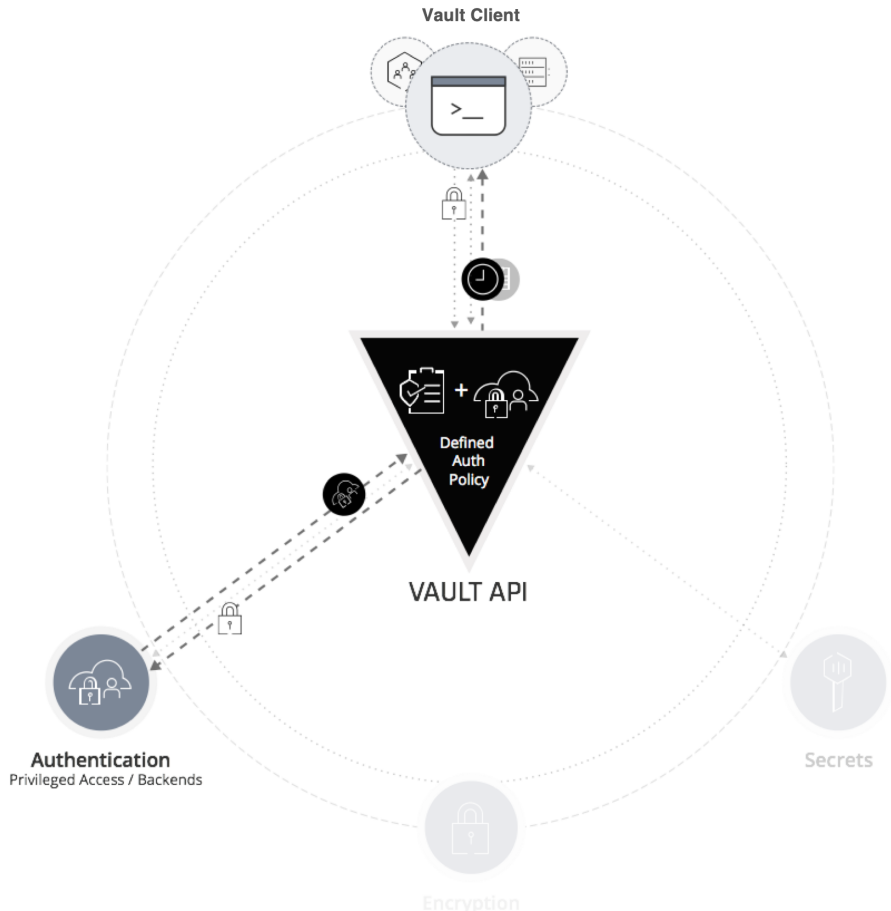




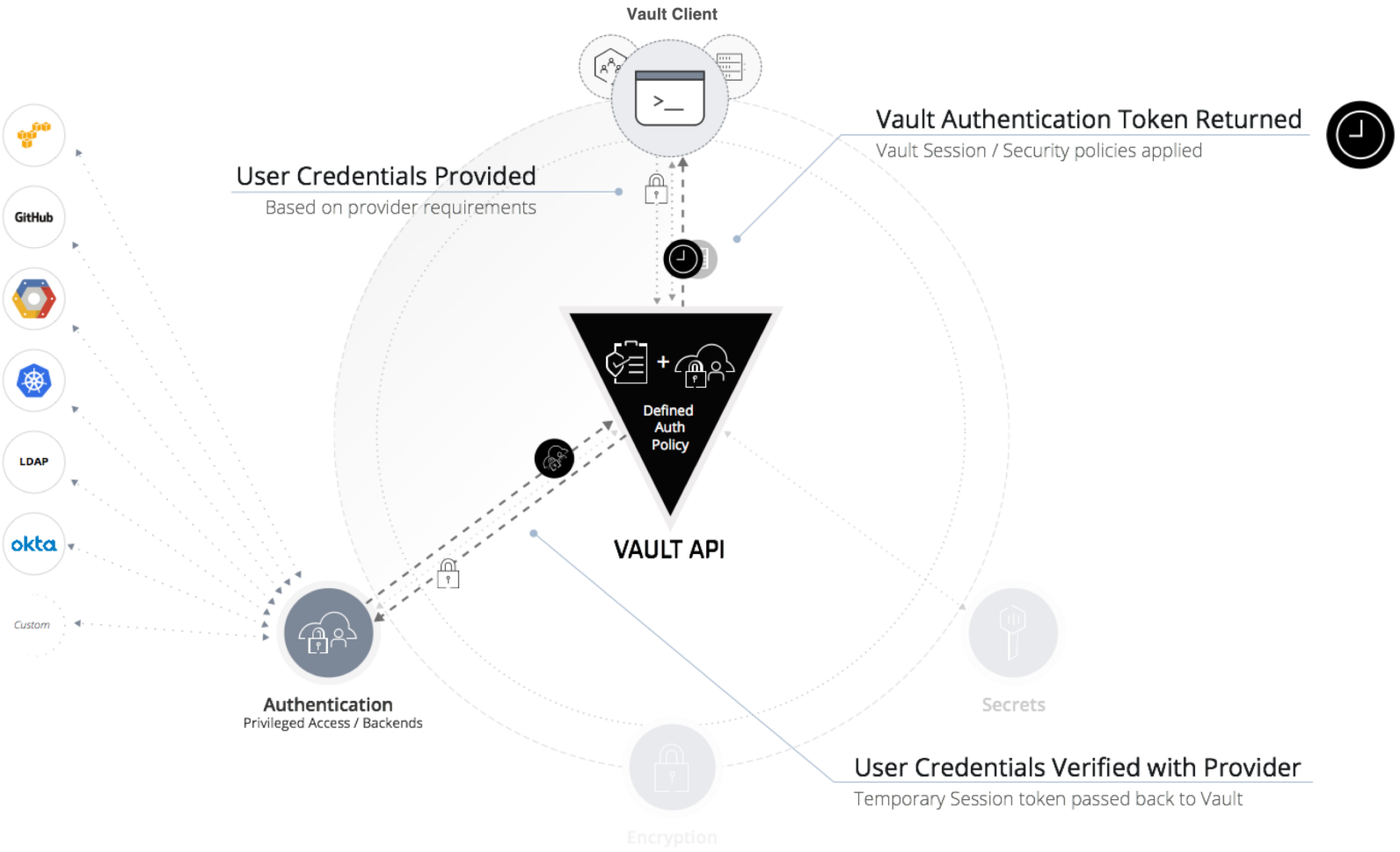
Vault Overview



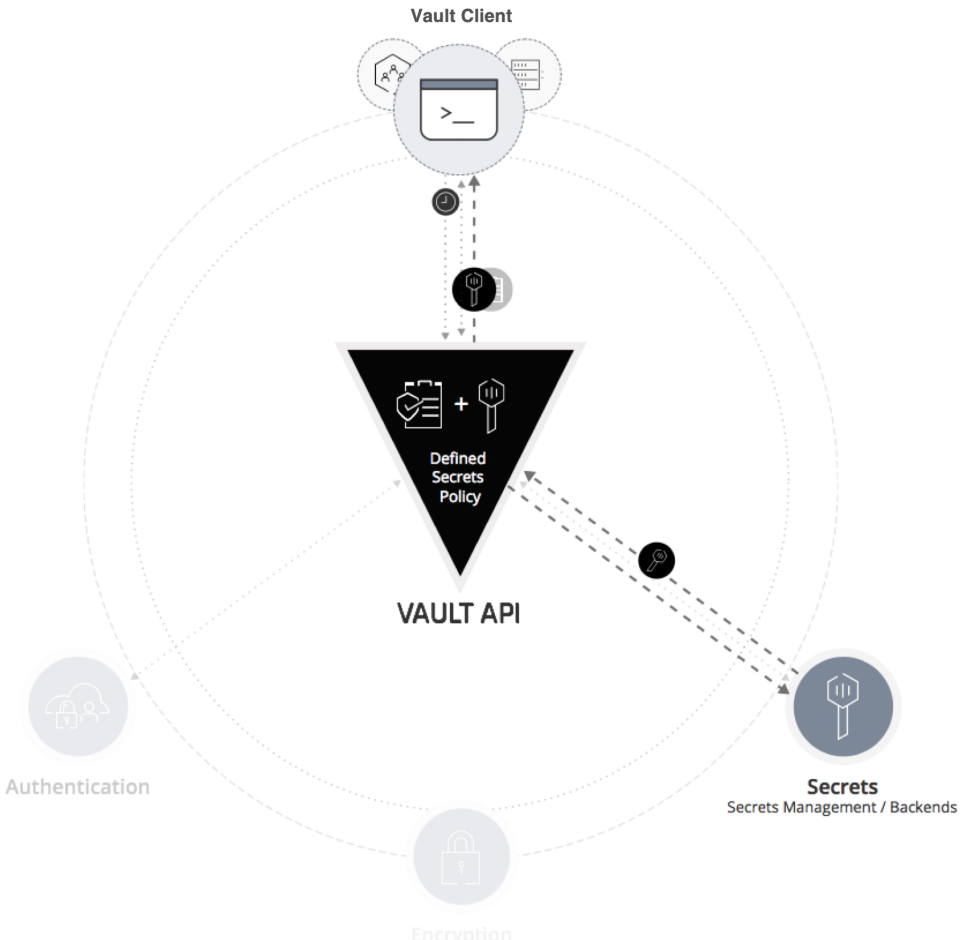
Client Authentication



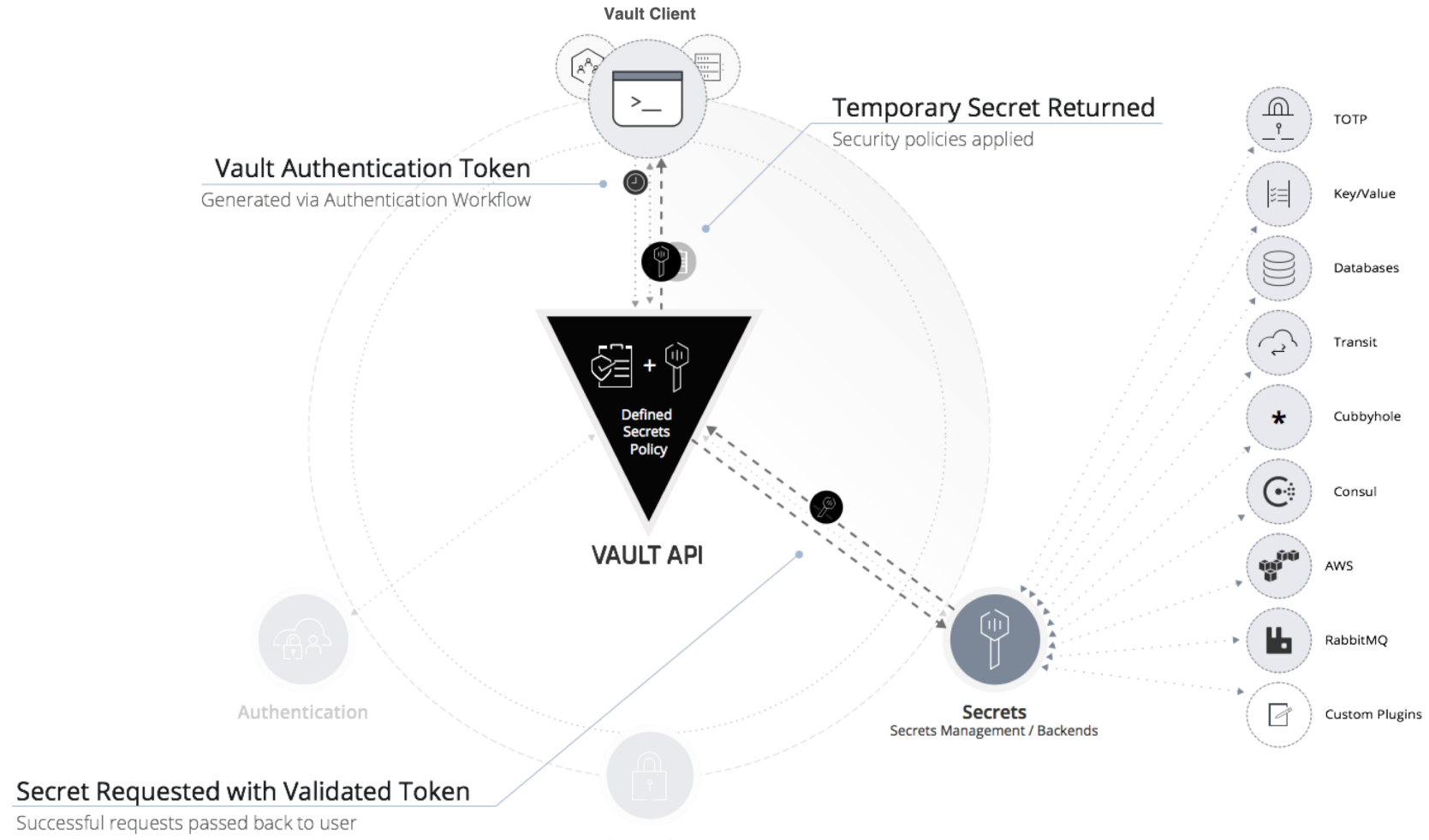
Trusted Source Of ID



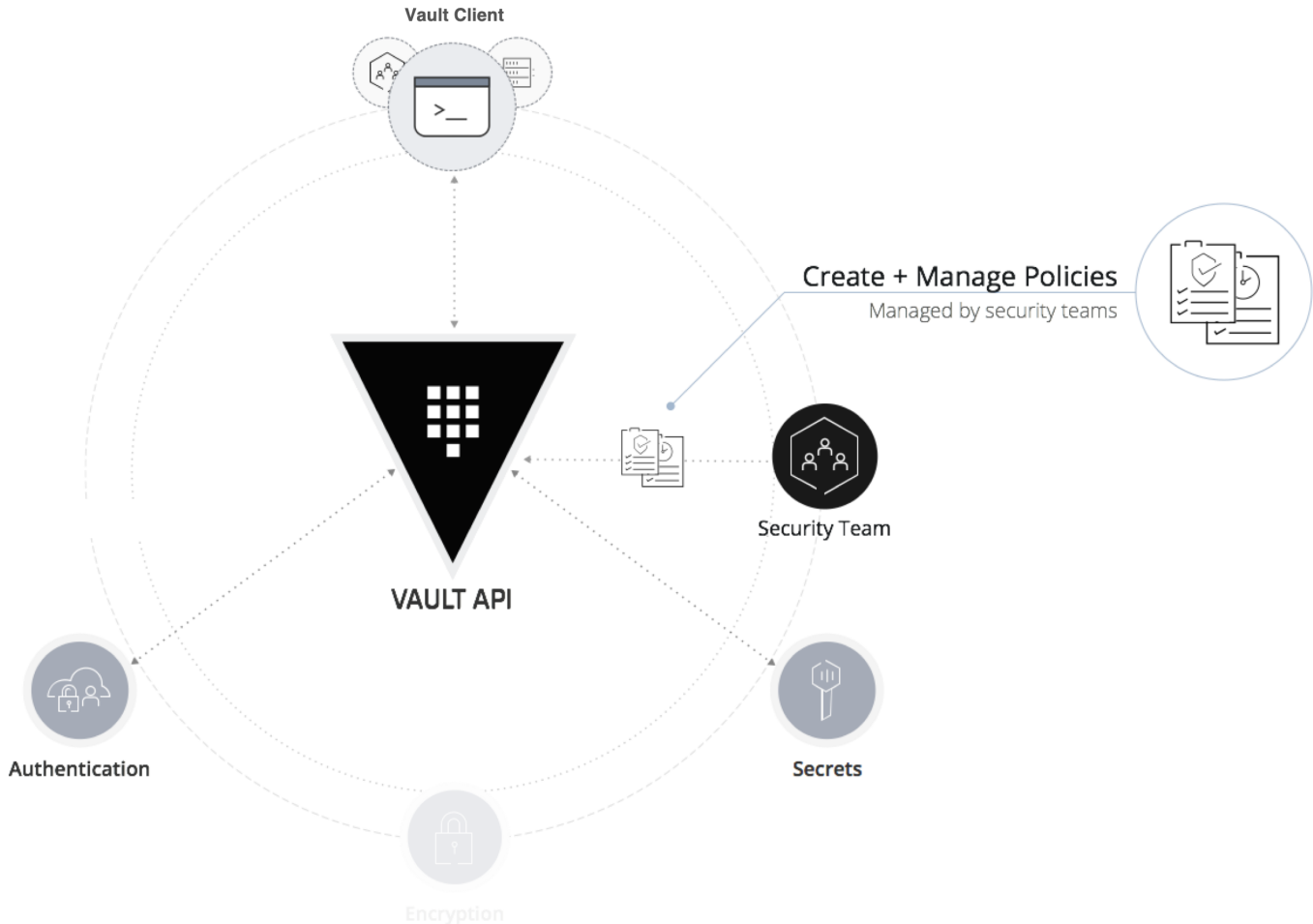
Vault Token



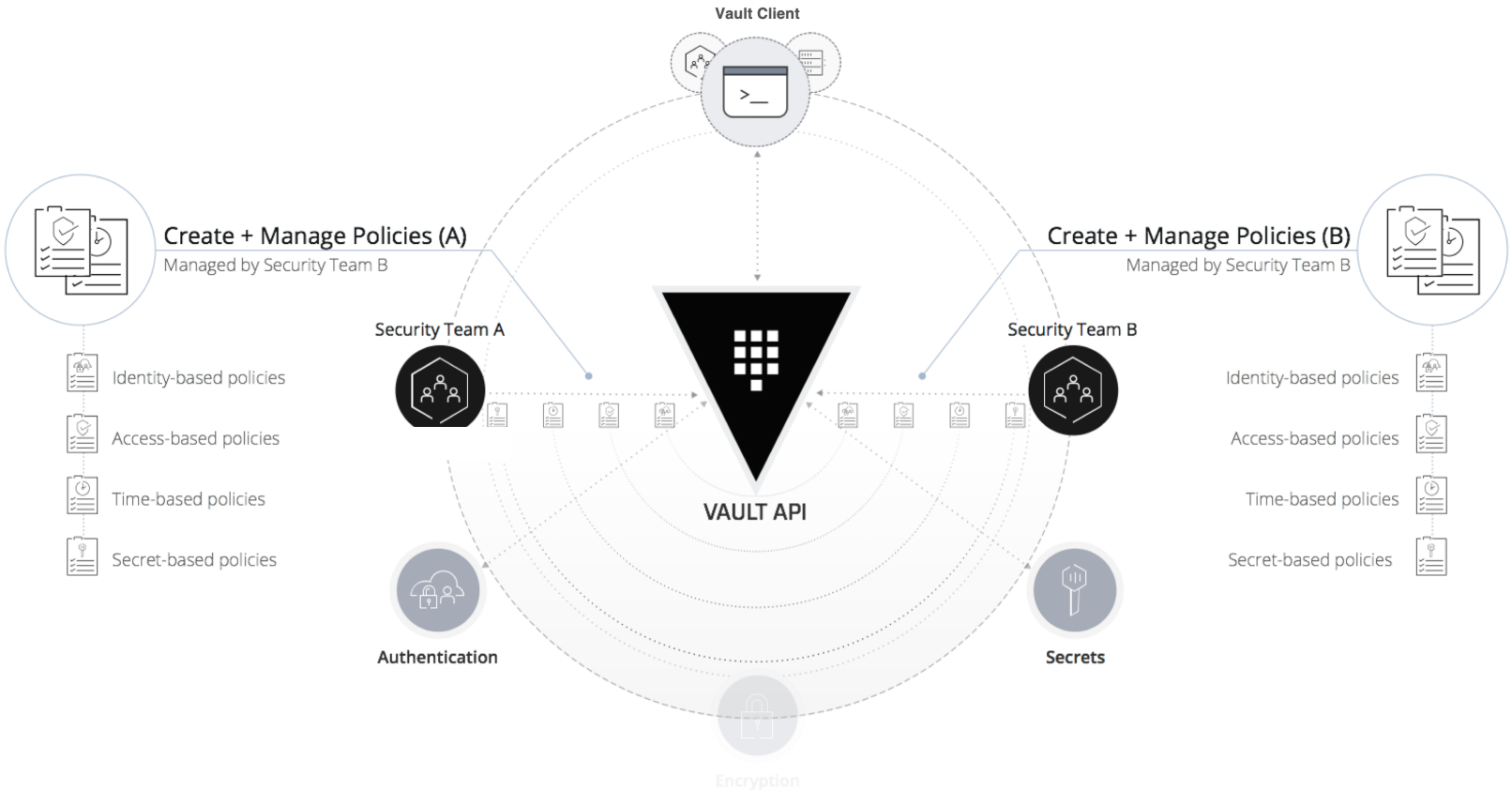
Secrets Engine



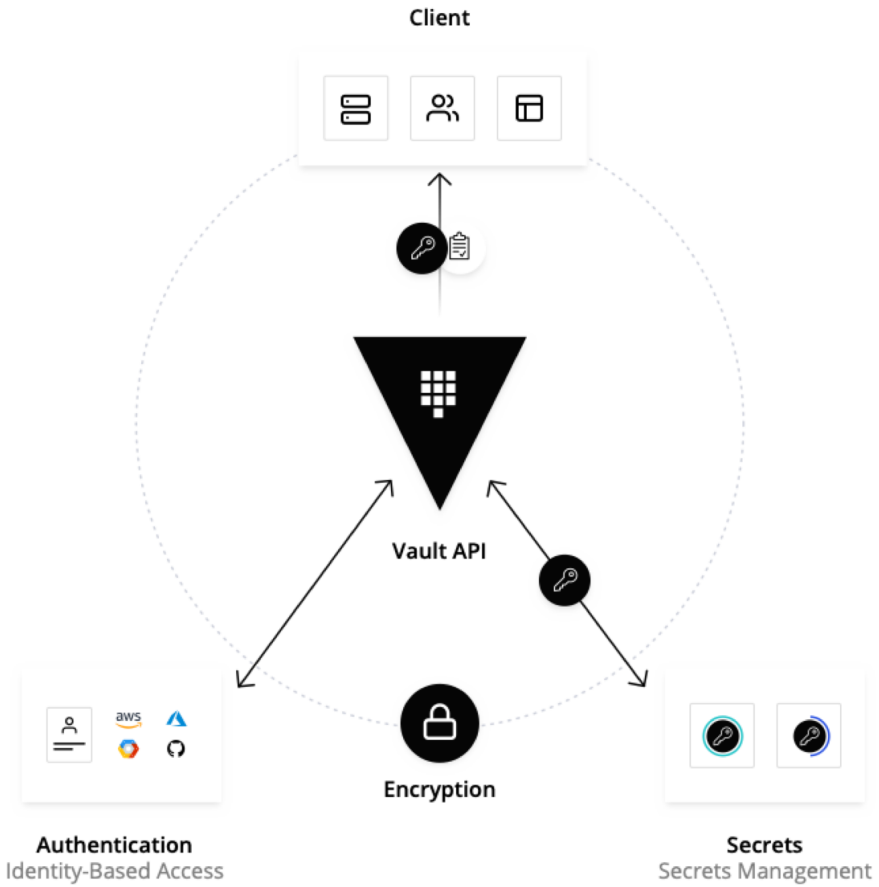
Vault Security Policies



Vault Namespaces

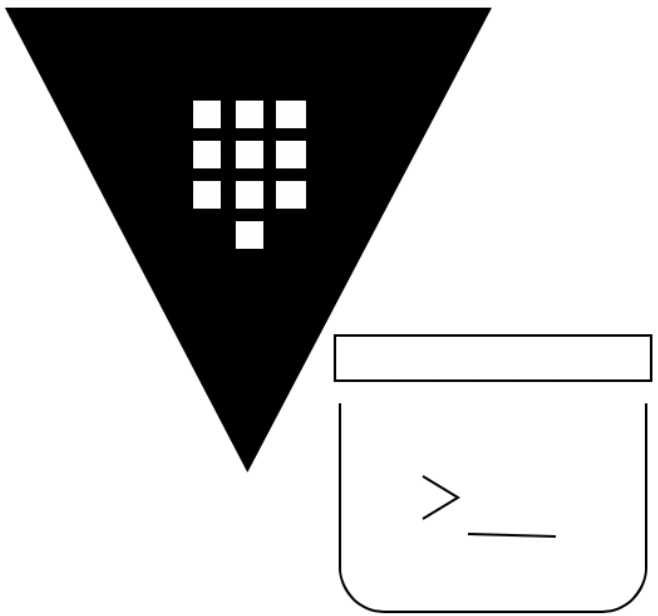


Vault Workflow



Vault Terminology

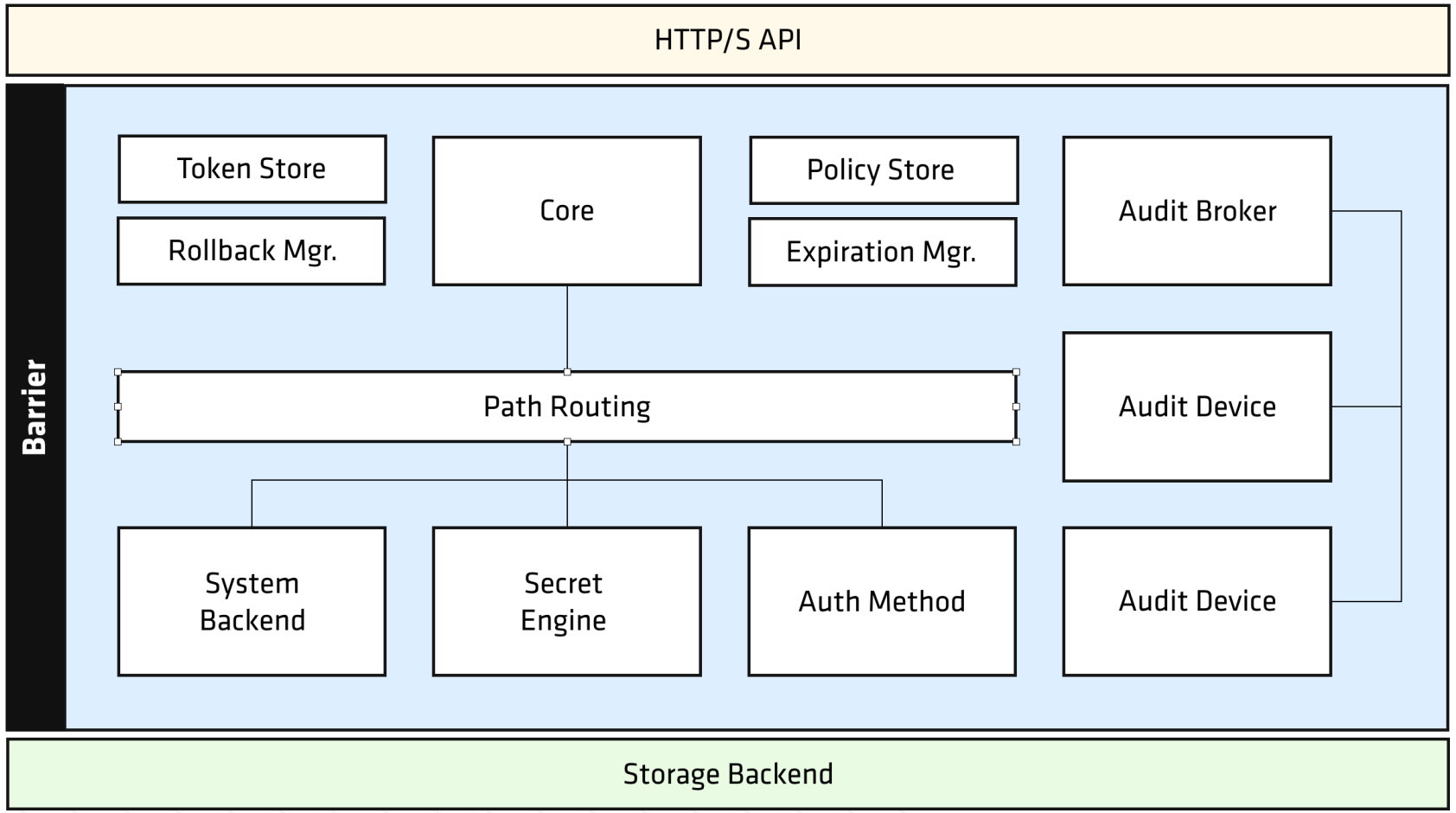
Vault Server



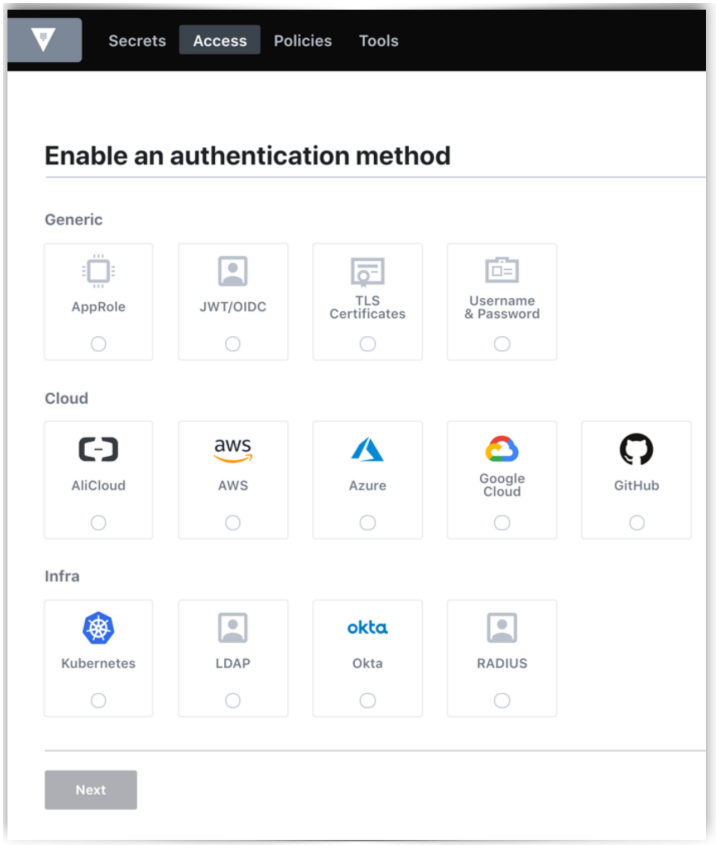
Manages all interactions

- Authentication Methods
- Policy and ACLs
- Secrets Engines
- Clients
- Tokens

Architecture

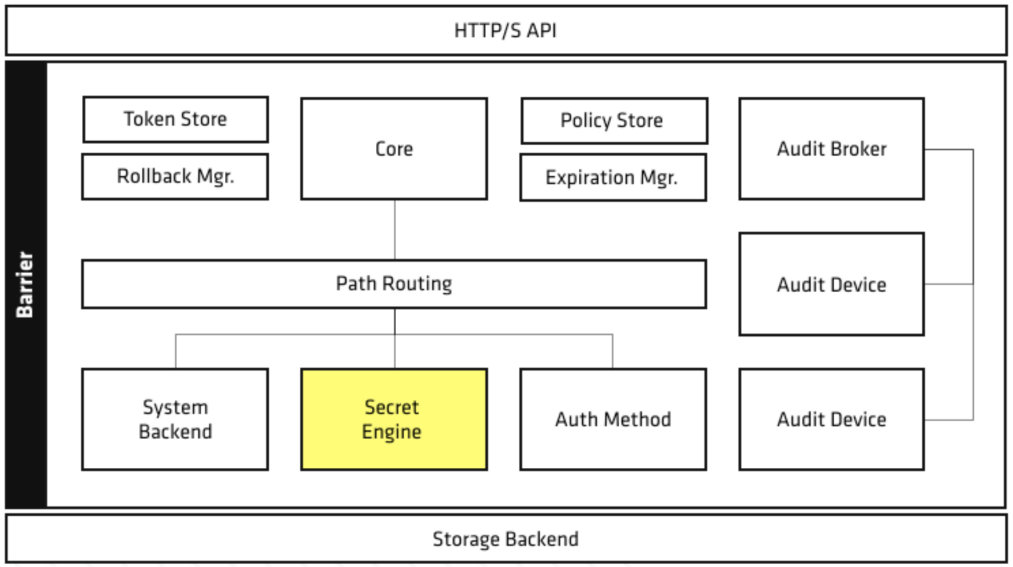


Authentication Methods



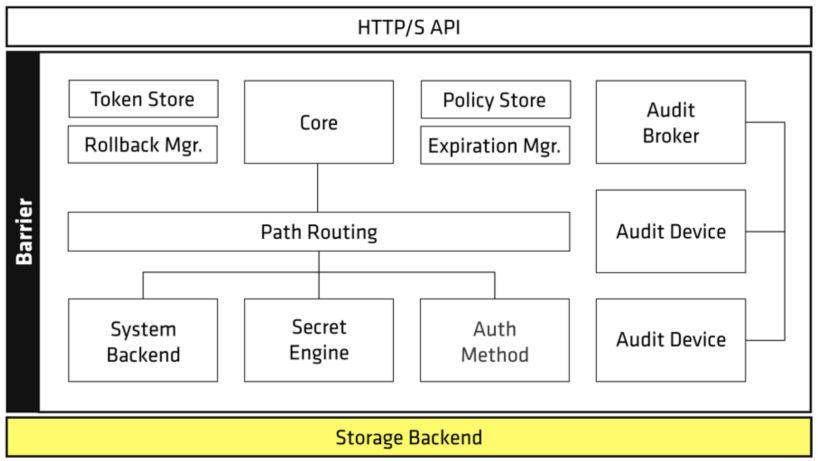
- Connects to trusted IDM
- Credential based
- Serves Clients
  - Operator
  - Machine
- Methods can be chained
- Must be enabled to use

Secrets Engine



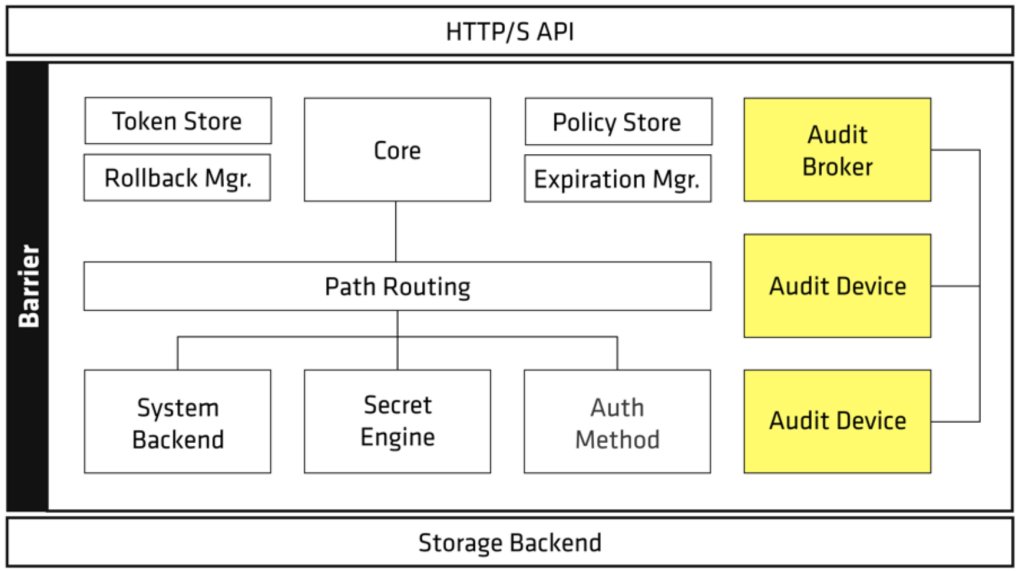
- Manages secrets
- Can have multiple
- Can store sensitive data
  - Static data
  - Dynamic data

Storage Backend



- Durable data storage
- Data is encrypted
- Backends include:
  - Consul
  - AWS S3
  - Cassandra
  - Raft

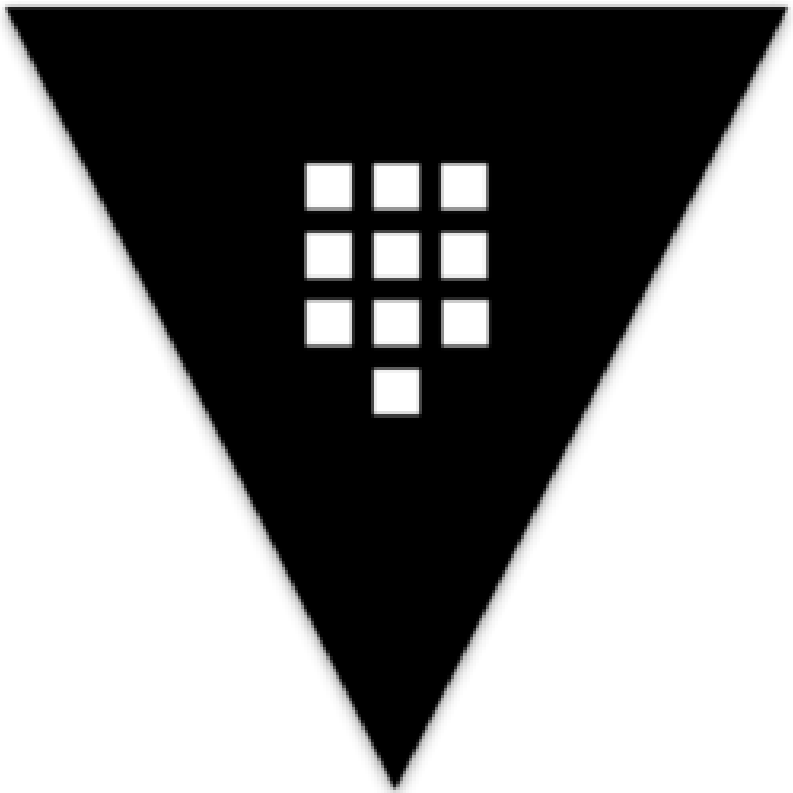
Audit Devices



- Must be explicitly enabled
- Records every interaction
- Can configure multiple

Clustering & High-Availability

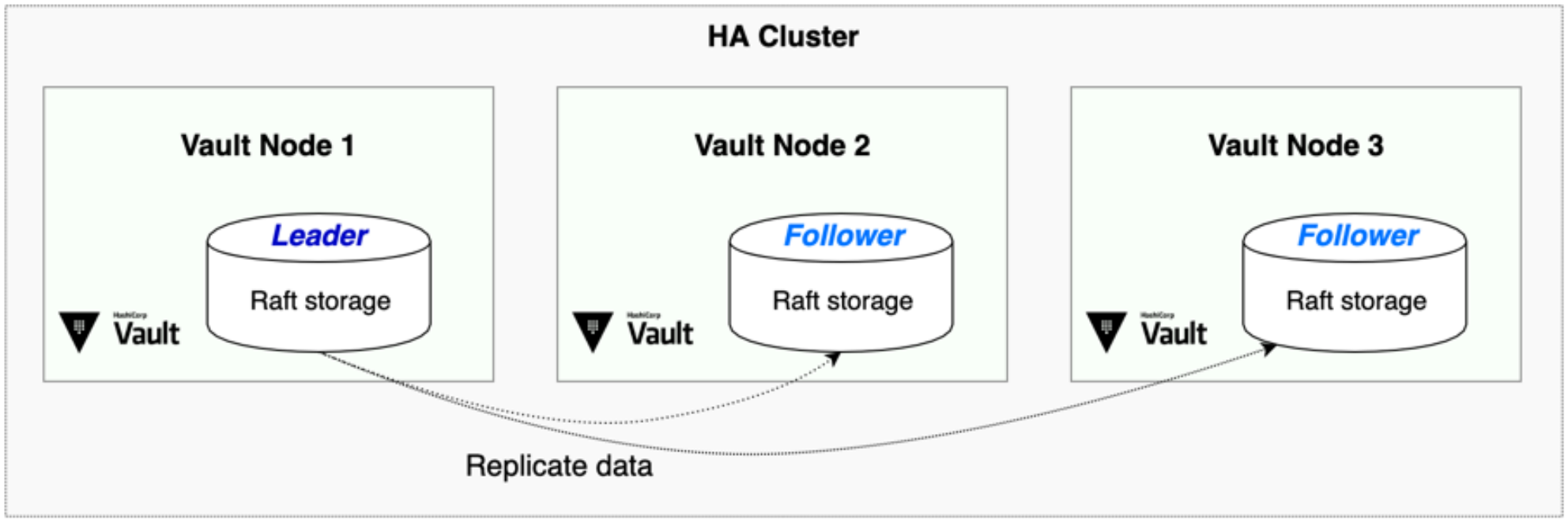
High Availability Mode



Multi-Server Mode

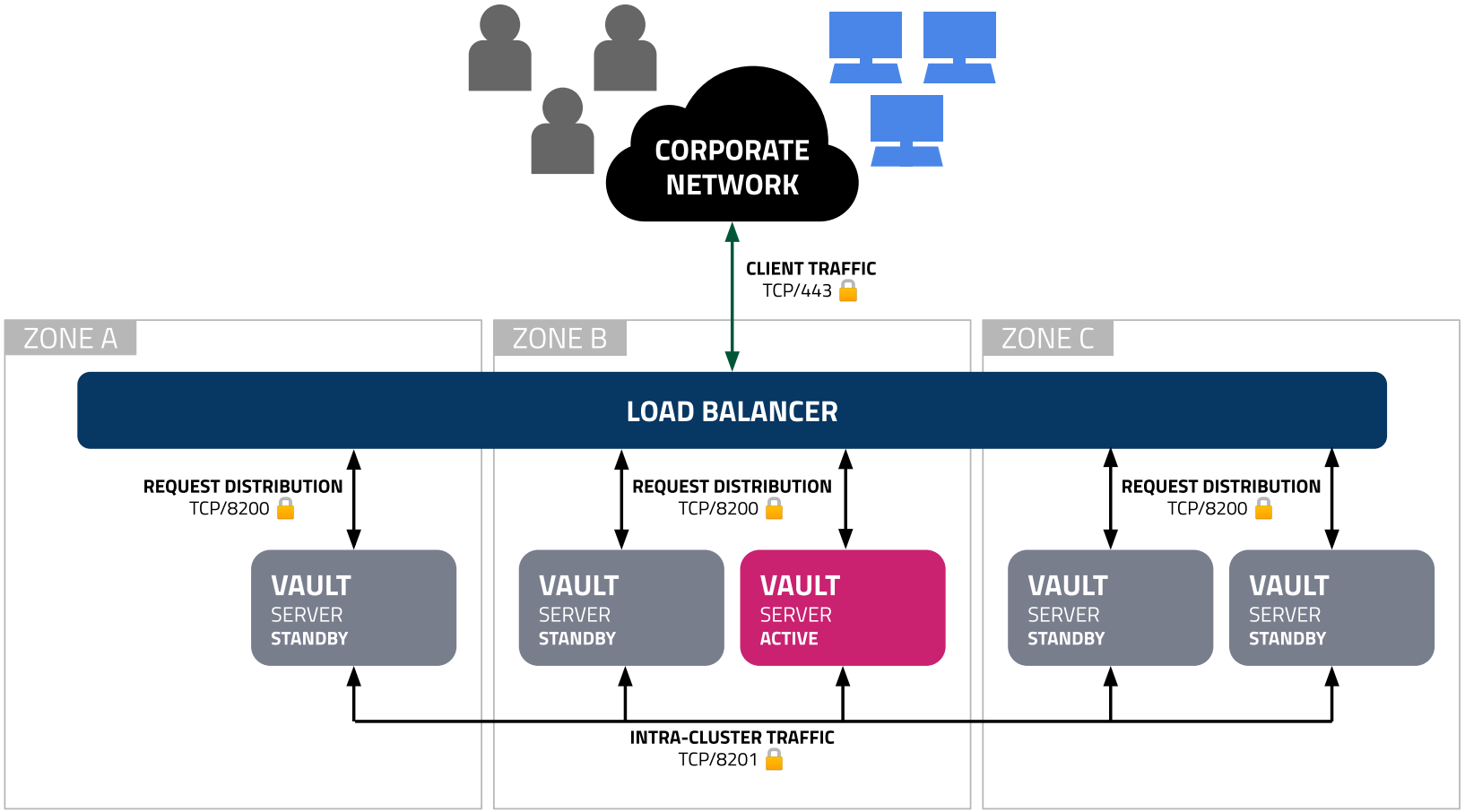
- Vault supports high availability
- Protects against local outages
- Automatically enabled with Vault Enterprise

Vault Reference Architecture



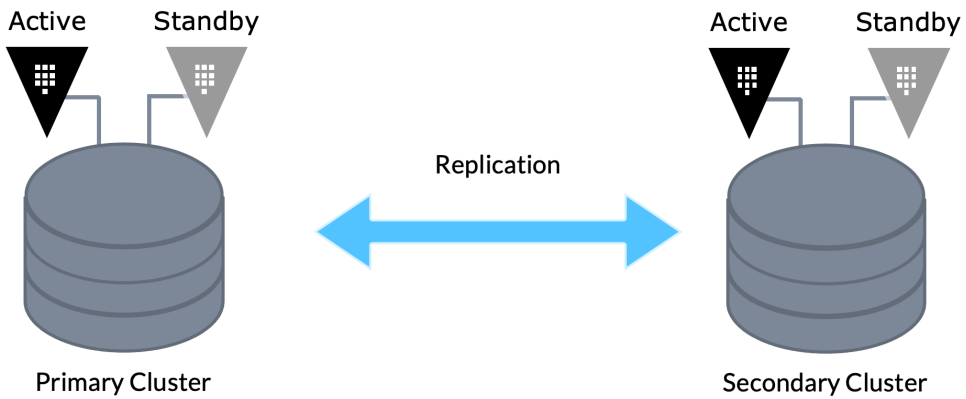
Integrated Storage Backend

Network Connectivity Details



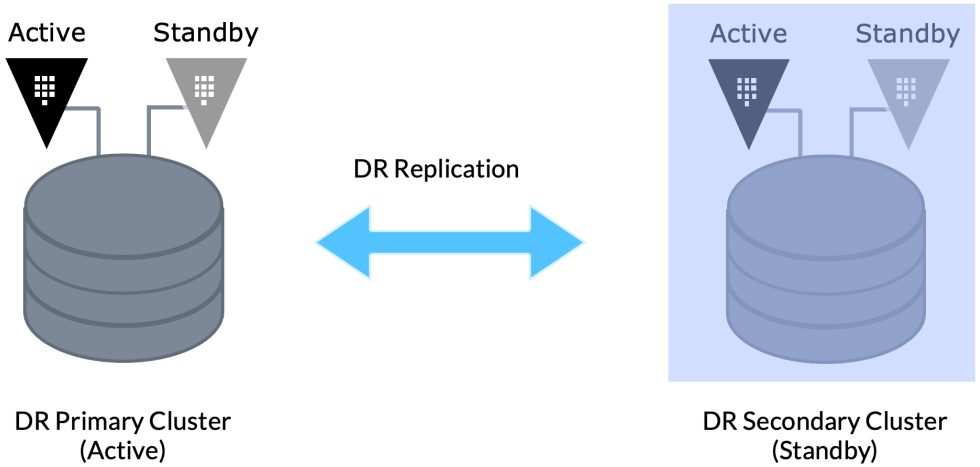
Disaster Recovery
&
Performance Replication

Replication - Vault Enterprise



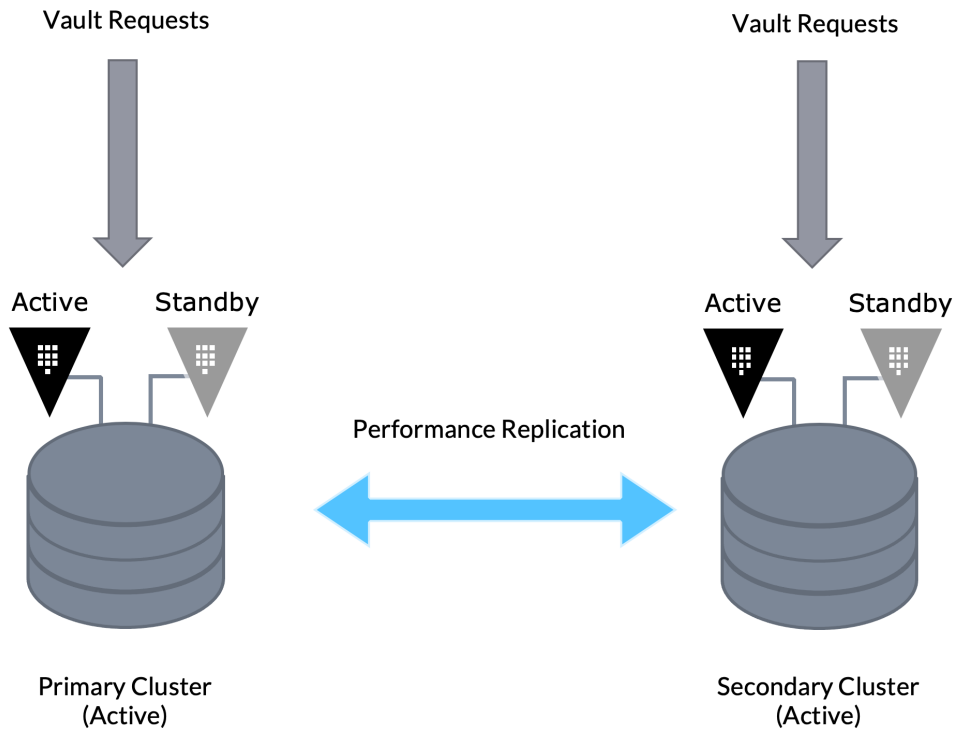
- Primary linked to secondaries
- Leader/follower model
  - Primary is system of record
  - Asynchronous replication

Replication - Disaster Recovery



- Primary services all requests
- One DR to one Primary

Replication - Performance



- Both service requests
- One Primary to many secondaries
- Primary replicates all data to all linked secondary

Replication - Comparison

Capability	DR Replication	Performance Replication
Configuration Mirroring	Yes	Yes
Secrets Configuration	Yes	Yes
Static Secrets	Yes	Yes
Dynamic Secrets	Yes	No
Token Replication	Yes	No
Secondaries Handle Requests	No	Yes

Chapter Summary

- Vault allows for securely storing and controlling access to tokens, passwords, certificates, encryption keys
- Vault uses:
  - Secrets Engines for secrets
  - Audit Devices for auditing
  - Auth Methods for Authentication
- Vault has two replication methods
  - Performance Replication for scaling availability and throughput
  - Disaster Replication for business continuity planning

Module 1 Reference links

- Vault Overview
- Vault Whitepaper
- Introduction to Vault with Armon
- Replication Concepts

Vault Architecture Module Complete!