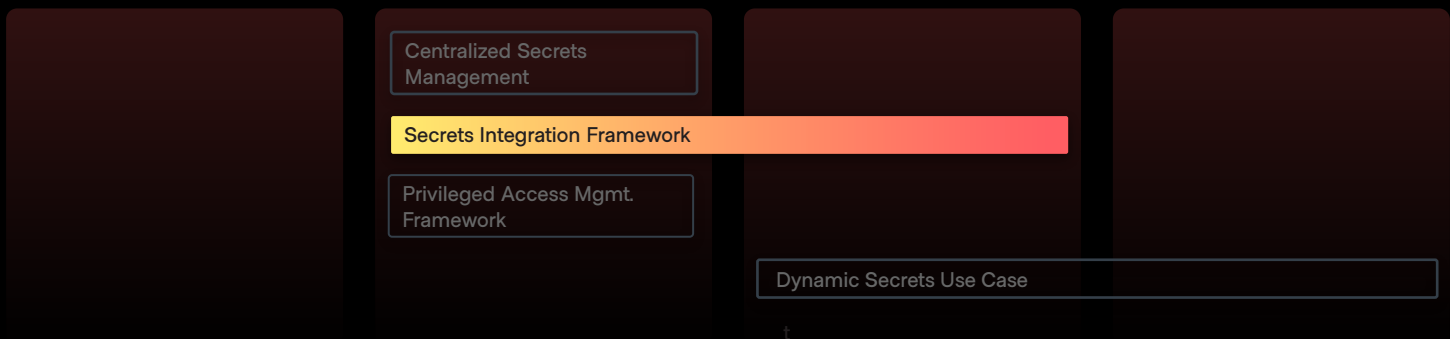


Secrets Integration Framework



Stage 0: Onboarding → Stage 1: Adopting → Stage 2: Standardizing → Stage 3: Scaling →



Service Scope

Assist in deployment of centralized secrets management so that applications and systems can consume secrets from HashiCorp Vault Enterprise.

Service Summary

- Help customers who are adopting centralized secrets management update their applications and systems to consume secrets from HashiCorp Vault Enterprise.
- Assist in the adoption of Vault Agent, Vault Secrets Operator on Kubernetes and/or Vault Secrets Sync to onboard applications to Vault Enterprise.
- Build customer confidence in their centralized secrets management strategy through successful deployment of dynamic secrets and secret rotation.

Key Benefits

- Automate consumption of secrets for applications, improving security and simplifying the alignment to compliance requirements.
- Leverage dynamic credentials and identity to ensure access to sensitive data is short-lived.

PHASE 1

Prerequisites



- Identify and interview stakeholders
- Identify current users and operators
- Set the stage with Cloud Operating Model (COM)
- Schedule Impact Assessment
- Vault Enterprise or HCP Vault deployed
- TPS execution

PHASE 2

Design



- Document current state Document usage patterns
- Project Delivery Document: Pre-Implementation Plan
- Architecture Design
- Scope build out
- Customer concurrence

PHASE 3

Deployment



- Knowledge transfer and enablement: Vault installation and configuration, authentication method(s) configuration
- Knowledge transfer and enablement: Secret engine configuration and enablement
- Knowledge transfer and enablement: Vault tooling installation and configuration
- Framework enablement for secret consumption or injection into targeted applications

PHASE 4

Close

- Executive Readout
- Feedback
- Recommendations
- Adoption Roadmap
- Training/Education Roadmap
- Project Deliver Document: Post Implementation
- Close-Out

