HashiCorp

Centralized Secrets Management

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

Centralized Secrets Management

Secrets Integration Framework

Privileged Access Mgmt. Framework

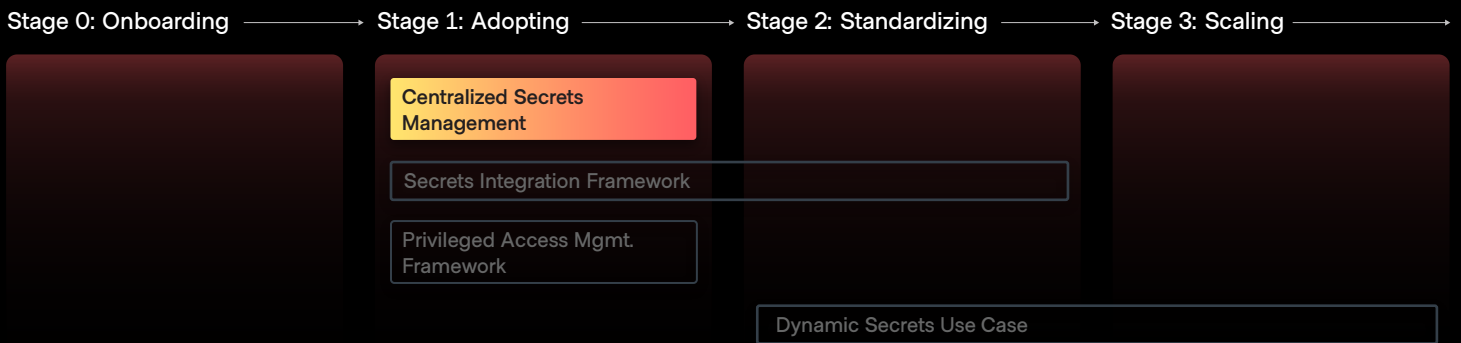Dynamic Secrets Use Case

Service Scope

Creates a centralized secrets management service that consolidates all your secrets into a single, secure repository for either public or private clouds using HashiCorp Vault.

Service Summary

- Enable the customer to create a centralized secrets management service utilizing HashiCorp Vault.

- Equip customers with HashiCorp Validated Designs where appropriate and accelerate their adoption, consumption and development.

- Provide knowledge share to enable adoption and utilization.

Key Benefits

- Adopt a single, platform-agnostic secrets and identity management solution, improving security posture and saving precious development time on integration.

HashiCorp

PHASE 1
Prerequisites

- Identify current user(s) and/or operator(s) for Academy training
- Current user(s) and/or operator(s) attend Academy
- Schedule Technical Planning Session (TPS) after completion of Academy

- HCP Vault or Vault Enterprise deployed
- TPS execution

PHASE 2
Discovery

- Identify stakeholders
- Set the stage with Cloud Operating Model (COM)
- Document current and/or desired state
- Document usage patterns

- Project Delivery Document: Pre-Implementation Plan
- Architecture Design
- Scope build out
- Customer concurrence

PHASE 3
Delivery

- Knowledge transfer and enablement: authentication method and secret engine configuration
- Knowledge transfer and enablement: policy configuration via CI/CD pipelines

- Knowledge transfer and enablement: Vault agent configuration
- Knowledge transfer and enablement: Vault audit and metrics configuration

PHASE 4
Close

- Executive readout
- Feedback
- Recommendations
- Adoption roadmap

- Training/education roadmap
- Project Delivery Document: Post Implementation
- Close-out