HashiCorp

Dynamic Secrets Use Case

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

Centralized Secrets Management

Secrets Integration Framework

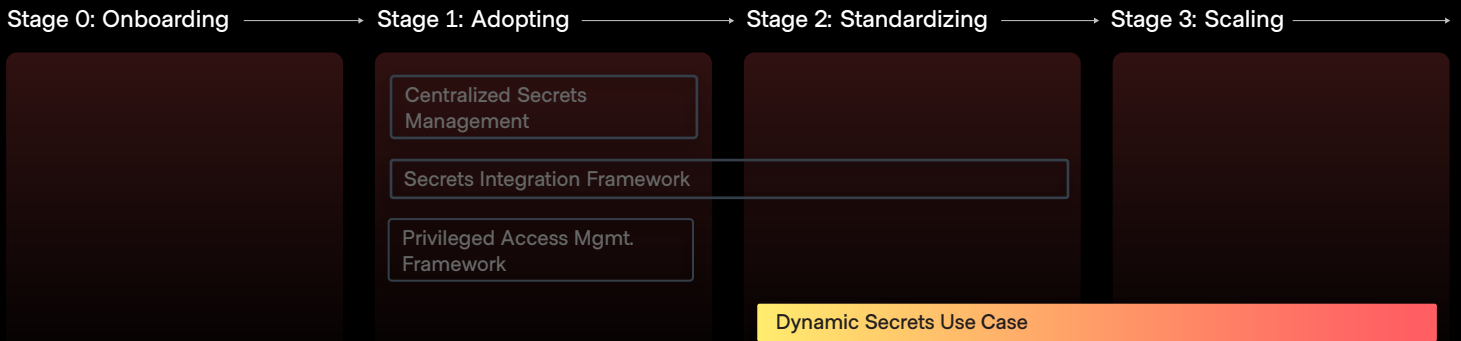Privileged Access Mgmt. Framework

Dynamic Secrets Use Case

Service Scope

Secure infrastructure with dynamic secrets generated by HashiCorp Vault.

Service Summary

- Equip the customer to create a process for moving static secrets to dynamic secrets with HashiCorp Vault.

- Enhance customer's security posture and secret consumption with Vault.

- Enable customer's organization to consume dynamic secrets generated by Vault directly through the API, CLI, UI, and/or a trusted orchestrator in their workflow.

Key Benefits

- Reduce risk and increase security by adopting dynamic secrets that are generated on demand and are unique to a client.

- Reduce risk and increase speed with Vault's dynamic secrets acting as a signing intermediary to generate short-lived certificates.

- Increase speed of secrets consumption within the organisation and provide greater application and functionality, including forensics, periodic rotation, or revocation.

HashiCorp

PHASE 1
Prerequisites

- HCP Vault or Vault Enterprise deployed and configured
- Identify current user(s) and/or operator

- Schedule Technical Planning Session (TPS)
- TPS execution

PHASE 2
Discovery

- Identify stakeholders
- 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

- Review and guidance on secret(s) consumption patterns
- Review and guidance on authentication method(s) for applications, machines, and people

- Review and guidance on Vault dynamic secret(s) engine (Database, LDAP, Cloud, etc.)
- Review and guidance on access patterns

PHASE 4
Close

- Executive readout
- Feedback
- Recommendations
- Adoption roadmap

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