DATASHEET

Secrets Management with Vault Integration Service

Business challenge

Data security is a top concern for every organization. As your infrastructure grows, so does the number of sensitive data points, and it becomes harder to ensure that sensitive information is stored, transmitted, and accessed safely.

Many organizations solve this problem by using a tool like HashiCorp Vault to store and control access to secrets, such as encryption keys and application credentials. Integrating Vault and Puppet enables Puppet to securely retrieve sensitive information used in defining configurations and to distribute that data in a secure manner, providing a high level of security across environments.

A Puppet professional will evaluate your current processes for handling and securing secret data throughout its lifecycle, and help improve your organization's security posture by integrating Puppet with HashiCorp Vault in alignment with your current architecture and workflows.

Customer benefits

- Expert review of data management strategy
- Improve security posture and implement secure automation best practices
- Increase user control over secrets that affect nodes managed by Puppet
- Leverage secrets from Vault according to best practices and your organization's security policy

puppet

Learn more at puppet.com

Who will benefit?

- Organizations looking to improve practices for storing and managing sensitive data like encryption keys, certificates, or application credentials.
- Teams that lack the skills or resources to integrate secrets management into their infrastructure automation workflows.

What you can expect

A Puppet consultant will:

- Evaluate your organization’s current data management practices and policy for deploying secrets via Puppet.
- Implement an integration between Puppet Enterprise and Vault to leverage and distribute secrets on configured infrastructure at scale.
- Create and/or modify Puppet code to leverage secrets from Vault in accordance with best practices and your organization’s requirements for secret distribution.

Expected outcomes

- Functioning integration between Puppet and Vault
- Enable Puppet Enterprise to use Vault for secrets management alongside hiera-eyaml
- Creation or modification of relevant Puppet code
- Identify current status of secrets stored in Puppet and move them to Vault

Assumptions

- This is at minimum a week-long engagement, but can be extended at customer direction.
- The current environment is functional, with Puppet workflows in place
- This service will be delivered remotely.
- Customer has administrative access to HashiCorp Vault.
- Customer understands the basic usage of HashiCorp Vault and is actively using it to store secrets.