HashiCorp Vault makes it easy for developers to secure secrets and protect dynamic infrastructure. This enables enterprises to secure, store and tightly control access to tokens, passwords, certificates and encryption keys for protecting secrets and other sensitive data using a UI, CLI or HTTP API. With Vault, developers can generate secrets like TLS keys and certificates. However, this approach alone often doesn't meet security requirements. Security teams increasingly require visibility over certificate issuance and that certificates must come from authorized public and private CAs.

In the past, obtaining security team-approved TLS keys and certificates required developers to connect with CAs using differing APIs. This creates new complexities for scaling Vault across dynamic infrastructure. With these limitations, DevOps teams can't use the full power of Vault to store all of their secrets. This leads to the following issues:

- DevOps teams using unauthorized CAs
- DevOps teams issuing noncompliant certificates
- DevOps teams not properly tracking their certificates
- DevOps teams wasting time implementing and maintaining their own siloed solutions
- Security teams being unable to enforce policy
- Security teams having no visibility into issued certificates

HashiCorp Vault makes it easy for developers to secure secrets and protect dynamic infrastructure. This enables enterprises to secure, store and tightly control access to tokens, passwords, certificates and encryption keys for protecting secrets and other sensitive data using a UI, CLI or HTTP API. With Vault, developers can generate secrets like TLS keys and certificates. However, this approach alone often doesn't meet security requirements. Security teams increasingly require visibility over certificate issuance and that certificates must come from authorized public and private CAs.

In the past, obtaining security team-approved TLS keys and certificates required developers to connect with CAs using differing APIs. This creates new complexities for scaling Vault across dynamic infrastructure. With these limitations, DevOps teams can't use the full power of Vault to store all of their secrets. This leads to the following issues:

- DevOps teams using unauthorized CAs
- DevOps teams issuing noncompliant certificates
- DevOps teams not properly tracking their certificates
- DevOps teams wasting time implementing and maintaining their own siloed solutions
- Security teams being unable to enforce policy
- Security teams having no visibility into issued certificates
Organizations using the Venafi Platform can now unlock the full power of Vault for TLS keys and certificates that meet security teams’ compliance requirements for policy and visibility. Using the Venafi Secrets Engine, all signing requests for TLS certificates are routed to the Venafi Platform. Signed certificates are delivered back to Vault and stored securely with the private key. The Venafi Secrets Engine is implemented using Vault’s plug-in system, and Venafi-issued certificates are requested using native Vault commands, so developers are not slowed down learning new processes.

How it Works

The Venafi Secrets Engine makes it easy to connect HashiCorp Vault’s credential and key management functions to an enterprise Machine Identity Protection service for TLS keys and certificates.

As a native Secrets Engine written in the Go language, the Venafi Secrets Engine abstract calls to the Venafi Platform using REST APIs.

Supported Vault Write Functions

- Issue: Request the Venafi Platform to issue a certificate according to Venafi Platform policy
- Sign: Submit externally generated CSR for certificate issuance according to Venafi Platform policy

Supported Vault List and Read Functions

- Certs: Returns list of certificates requested from the Venafi Platform
- Cert: Returns values, including certificates and private keys stored by the Venafi Platform

Figure 1: Venafi Secrets Engine: Usage and Architecture
The Benefits of Integration

DevOps teams want to run fast with their preferred tooling. HashiCorp Vault as an enterprise platform scales across cloud and hybrid infrastructures, eliminating wasted time on custom coding. The Venafi Secrets Engine lets DevOps standardize on a single, fast and simple way to automate keys and certificates that serve as machine identities. By implementing the Venafi Secrets Engine, security teams can ensure that certificate policies are always enforced while maintaining full visibility and inventory—all without impeding the speed of DevOps.

When the Venafi Platform and HashiCorp Vault are used together, developers are able to:

- Use native HashiCorp Vault API calls and commands to request certificates that comply with policy, using roles within HashiCorp Vault
- Request publicly trusted and internal certificates from any CA configured in the Venafi Platform
- Renew certificates at a configured time before expiration using HashiCorp Consul templates
- Use Venafi for certificate enrollment while storing certificates and private keys within HashiCorp Vault

Figure 2: Process for Key and Certificate Issuance Using the Venafi Platform and Vault

Technical Considerations

Compatibility

- Venafi Platform 18.1 or higher
- HashiCorp Vault or Vault Enterprise
- Linux or Windows
- X.509 certificates for TLS

Related Capabilities

- Monitor Vault: With the Venafi Monitor Secrets Engine, DevOps teams can use the built-in Vault PKI for highly distributed, low latency use of TLS keys and certificates. Security teams get complete monitoring of Vault to maintain governance and visibility of all TLS certificates generated by Vault. All certificates issued through Vault are automatically synchronized with the Venafi Platform.

- Build Infrastructure: Automate the build of complex infrastructure and issuance of certificates with the Venafi Terraform Provider.
Download from the Venafi Marketplace

Ready to use Venafi with your HashiCorp Vault instances? Download the Venafi Secrets Engine and access additional resources from the Venafi Marketplace https://marketplace.venafi.com

Resources

• Open source projects for Vault, Terraform, Ansible and more https://github.com/Venafi
• Technical support support@venafi.com

Venafi is Trusted by the Top:

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

About Venafi

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.