SOLUTION BRIEF

KEYFACTOR

Keyfactor + HashiCorp Vault

Leverage the value of HashiCorp Vault without compromising enterprise security requirements

HashiCorp Vault enables DevOps teams to centrally store and access tokens, passwords, certificates and encryption keys they rely on to protect sensitive data and securely access the tools and platforms across their dynamic infrastructure. This enables developers with secure, API-driven access to secrets, without disrupting their natural workflow. With the Vault PKI Secrets Engine, developers can also generate short-lived certificates on-demand, while avoiding the usual manual processes involved in traditional PKI. However, enterprise teams still run into challenges when it comes to PKI operations and security.

While HashiCorp Vault meets the needs of DevOps teams, Vault alone often doesn't meet enterprise security requirements, and it is commonly deployed in a way that introduces risk caused by untracked or self-signed certificates. Without centralized visibility and control over certificates issued across all Vault instances, security teams lack the checks and balances they need to ensure that every certificate is trusted and compliant with enterprise policy.

ENTERPRISE SECURITY REQUIREMENTS

PKI and security teams lack visibility and control that the enterprise requires. To ensure that every certificate is trusted and complaint, they need to:

- Gain visibility into X.509 certificates issued across all Vault instances in their environment
- Enforce governance and compliance while allowing DevOps to use native Vault APIs and commands
- Ensure that certificates are issued from a secure root of trust, not an untrusted self-signed CA

WHAT DEVOPS NEEDS

DevOps teams are unable to take full advantage of Vault for all of their certificate needs. To leverage Vault for PKI, DevOps teams need to:

- Easily obtain X.509 certificates that comply with enterprise policy, without inhibiting workflows or delivery timelines
- Automate access to publicly-trusted certificates required for production environments directly from Vault
- Enable high-volume issuance of certificates at scale without latency or downtime

Unlock the Power of HashiCorp Vault with the Keyfactor Platform

Keyfactor Command delivers the most complete and scalable PKI as-a-Service platform for certificate lifecycle automation. This enables enterprises to find, monitor, and automate the lifecycle of keys and certificates at scale – supported by a privately-rooted, managed PKI service delivered from the cloud.

When integrated with HashiCorp Vault, Keyfactor Command enables DevOps teams to get seamless access to trusted internal and public certificates via native Vault API calls and commands, while security teams maintain complete visibility and control over backend PKI operations. The only platform tested and proven to enable thousands of operations per second in environments with 500M+ certificates, Keyfactor Command is purpose-built for high-volume operations of HashiCorp Vault. This enables DevOps teams to move fast and ensures that every certificate is trusted and compliant with enterprise requirements.

WHY KEYFACTOR + VAULT

GET COMPLETE VISIBILITY

Discover certificates across all Vault instances, namespaces, and CAs and bring them into a single enterprise-wide inventory.

MONITOR & REPORT

Continuously monitor certificates, generate reports for compliance, set alerts and notifications, and easily identify and revoke non-compliant or rogue certificates.

ENFORCE POLICY

Enforce certificate policies within native Vault workflows to ensure that every certificate complies with enterprise policy.

ENABLE AGILITY

Allow developers to use native Vault APIs to request certificates from trusted internal CAs, public CAs, or a privately rooted, cloud-hosted PKI as-a-Service platform.

MINIMIZE DISRUPTION

Leverage a simple, proven integration that delivers trusted certificates to DevOps teams without disruption, even at massive scale.

How We Integrate

Organizations that use the Keyfactor platform can leverage HashiCorp Vault to simplify and automate certificate requests for development teams and at the same time, provide infosec with the ability to define and enforce policies. Enterprise can augment the PKI Secrets Engine with more granular monitoring and reporting capabilities, or integrate directly with Keyfactor Command as a PKI backend. Using the Keyfactor Secrets Engine, all certificate requests are routed through the Keyfactor platform, and all certificates already issued by Vault instances are imported into the enterprise inventory.

KEYFACTOR ORCHESTRATOR

Use the Vault PKI Secrets Engine

The Keyfactor Orchestrator allows security teams to monitor and report on certificates issued by the Vault issuing CA.

- Inventory certificates across all Vault instances and bring them into the Keyfactor platform to actively monitor and report on them
- Add custom metadata (i.e. application, owner, location) and group certificates to simplify audits and easily identify and remediate risks
- Search and revoke certificates based on serial number, certificate status, owner, expiration date, key size, algorithm, and other attributes

KEYFACTOR SECRETS ENGINE

Use the Keyfactor Secrets Engine

The Keyfactor Secrets Engine enables DevOps teams to request certificates through Keyfactor Command via Vault.

- Provide a secure root of trust for Vault by integrating directly with your enterprise-supported PKI or a privately-rooted, cloud-hosted PKI managed 24/7 by Keyfactor
- Enforce consistent certificate policies and define request and approval workflows while still allowing DevOps teams to use the native Vault API, UI or CLI
- Deliver certificates via Vault from trusted public CAs configured in Keyfactor Command and automate the certificate lifecycle to prevent outages and downtime

Why Keyfactor

TECHNOLOGY POWERED BY DEEP PKI EXPERTISE

✓ PROVEN SCALABILITY

The only platform tested and proven to process thousands of operations per second in environments with 500M+ certificates.

✓ CLOUD-FIRST APPROACH

Keyfactor offers an integrated PKI as-a-Service platform for certificate lifecycle automation and IoT device security – delivered from the cloud.

✓ FLEXIBLE DESIGN

Our modular design enables enterprises to enable automation without the need to re-engineer workflows or re-issue certificates.

✓ EXTENSIBLE ECOSYSTEM

Our API-first approach allows customers to integrate with a growing number of enterprise infrastructure, tools, and applications.

✓ UNMATCHED SERVICE

Keyfactor customers benefit from world-class PKI experts and service – backed by 99% customer satisfaction and 98.5% customer retention.

✓ IN-DEPTH EXPERTISE

Our platform and services are built upon 20+ years of hands-on experience working with leading companies to build and run their PKI.

Ready to Get Started with Keyfactor and HashiCorp Vault?
Connect with one of our PKI Specialists to learn more.

CONTACT US

KEYFACTOR

Keyfactor empowers enterprises of all sizes to escape the exposure epidemic – when breaches, outages and failed audits from digital certificates and keys impact brand loyalty and the bottom line. Powered by the industry's only PKI as-a-service platform, IT and infosec teams can easily manage digital certificates and keys. And product teams can build IoT devices with crypto-agility and at massive scale.

▶ www.keyfactor.com
▶ +1.216.785.2990