| Objections & Responses |
| --- |

BUSINESS

O. We use Vault Community Edition for PKI. What’s different here? (Also see Technical response)

R. Once automated certificate renewal has been adopted, Vault needs to be considered a tier zero service where downtime can lead to a production outage due to a failed certificate renewal. Vault Enterprise can provide scalability and availability to prevent revenue loss. Here are some compelling reasons to consider Vault Enterprise:

* Horizontal Scaling: Vault Enterprise enables every node in a cluster to handle certificate issuance under certain configurations (especially when dealing with short-lived certificates).
* Performance Replication: Vault Enterprise offers performance replication, which allows for read scalability and service durability. This is crucial for PKI use-cases where high availability and low latency are required for certificate issuance and management.
* Namespace Support: With Vault Enterprise, you can create isolated environments within a single Vault cluster using namespaces. This is particularly useful for organizations that need to manage PKI for multiple teams or departments with distinct security requirements.
* Support and SLAs: With Vault Enterprise, you receive professional support and service level agreements (SLAs) from HashiCorp, ensuring that you have expert assistance available when needed.
* Disaster Recovery : ensure that your Vault deployment is resilient and can handle high availability and disaster recovery scenarios, which are critical for business continuity.

O. We use another vendor (Venafi, Digicert, GlobalSign, Keyfactor) for certificate management. Why do I need Vault? - Two possible responses below

Competitive Takeout R.   
These vendors provide siloed solutions designed for specific tasks, which often require additional tooling, integrations, and infrastructure to manage effectively. This fragmentation complicates management and increases the risk of errors because each solution operates in its own separate environment. Vault Enterprise, on the other hand, offers a unified platform that manages all types of secrets—static keys like passwords and encryption keys, dynamic tokens such as API keys, and PKI certificates—all under one roof. By consolidating secret management into a single platform, Vault Enterprise simplifies operations, reduces the number of tools to manage, and enhances security by minimizing potential points of failure or attack. This centralized approach allows organizations to eliminate the complexity introduced by managing separate siloed solutions while maintaining robust security practices.

Cooperative R.

These vendors provide an impressive suite of capabilities when it comes to certificate lifecycle management, however they have gaps when it comes to complete automation, high performance, and tight integration with modern apps. These gaps are where Vault excels and it’s likely Vault integrates with your current CLM Platform.

While your CLM platform has its place, Vault can supplement it by addressing your DevOps PKI use cases. Vault’s developer centric design is best suited for microservices and immutable systems. Vault is able to treat certificates as ephemeral credentials with rapid expiration which can keep pace with your development teams.

O. Vault Enterprise is too expensive to only use for PKI.

R. For customers using Vault for the sole use case of automated certificate renewal, the client model can be a blocker. HashiCorp has recognized this and created a new model that focuses around the total number of PKI certificates issued within dedicated namespaces. This alternative model brings all the benefits of automated certificate renewal at a potentially lower price point. I would love to explore the model with you to see if it might be a fit for your consumption pattern.  
  
([See exception process pricing here](https://docs.google.com/document/d/1u0L68TT0rBrMjdUilRGgaWAQC62yI7-F6yh9C9s9Wz0/edit?usp=sharing), please obtain approval first)  
  
 While considering only PKI might seem like a large investment, Vault Enterprise offers far more value than just certificate management. Certificate management is crucial for enterprises because manual processes are prone to errors, which can lead to service disruptions and missed Service Level Agreements (SLAs). When you take into account the comprehensive lifecycle management that Vault Enterprise provides—such as creating, distributing, renewing, and revoking certificates— you begin to appreciate the risks and potential costs of relying on single use tooling such as a certificate lifecycle management (CLM) platform, kv store, pam vault, and more. Automating these processes not only strengthens security but also eliminates the inefficiencies of fragmented tools, ensuring greater operational stability and efficiency.

O. My consumers can already generate certificates via a self service portal. Why would I introduce a new tool like Vault ?

R. Leveraging a self-service portal to generate or renew certificates does not scale with cloud native services (containers, microservices..etc) that require short-lived, automatically generated certs without involving manual processes or personnel. However, if you need to continue supporting existing manual use-cases and your consumers are already capable of generating certificates through a self-service portal, there may be no immediate need for Vault Enterprise unless it adds significant value beyond what you already have. However, manual processes (e.g., point-and-click portals) can be error-prone and inefficient. For example, a user may inadvertently copy the wrong values when submitting Keys and Certificate Signing Requests (CSR). This is just one of many manual steps in the process.   
  
Vault Enterprise can provide comprehensive automation of certificate management tasks, such as generating, delivering, and renewing certificates securely and on time. In short, while your existing portal may handle certificate generation, Vault Enterprise can enhance the process by automating and simplifying certificate management tasks, ensuring a more secure and efficient end-to-end experience for consumers.

O. Adding certificates renewal and machine identity use-case would inflate our Vault Enterprise client count, and we are already concerned with the current consumption costs.

R. We understand that the machine identity and certificate management requires a different operating and licensing model. That’s why we have created a competitive licensing offering with that in mind. More details [here](https://docs.google.com/document/d/1u0L68TT0rBrMjdUilRGgaWAQC62yI7-F6yh9C9s9Wz0/edit?tab=t.0).

TECHNICAL

O. We use Vault Community Edition for PKI. What’s different here? (Also see Business response)

R. Automated Certificate Renewal brings quick success to an organization, but you need to be prepared to handle issues that you will encounter at scale. Vault Enterprise provides essential solutions for manageability and security at scale. Vault will need to be approachable and simple to use for end users while also providing the security tools to audit and protect your production services.

* PKI Specific Vault Enterprise Features:
  + HSM-and Cloud KMS- backed PKI key generation, certificate signing, and verification
  + Support for Certificate signing with Certificate Issuance External Policy Service (CIEPS)
  + Support ACME with extended certificate lifetime, EST, CMPv2, and SCEP
  + Support for custom certificate metadata which Vault will retain the metadata along with the issued certificate, which can then be ingested into external systems for further processing.
  + FIPS compliance for PKI operations using managed keys and FIPS-Compliant HSM
  + Support for a unified CRL and OCSP with cross-cluster revocation
* Namespace Support: With Vault Enterprise, you can create isolated environments within a single Vault cluster using namespaces. This is particularly useful for organizations that need to manage PKI for multiple teams or departments with distinct security requirements.
* Advanced Audit Logging: Vault Enterprise provides detailed audit logging capabilities with advanced filtering, which are essential for compliance and security monitoring. You can track who accessed what secrets and when, providing a clear audit trail.
* Sentinel Policies: Vault Enterprise provides advanced policy enforcements that take into account requester or target secret properties such as source IP, time of request, MFA validation.

O. We’re inclined to adopt SPIFFE/SPIRE for machine & workload identity management. We don’t need Vault.

R. Let’s first start with some context, SPIFFE is an open-source standard developed by the Cloud Native Computing Foundation (CNCF) that provides a framework for securely identifying and authenticating workloads across dynamic and heterogeneous environments and SPIRE is an open-source implementation of it. Adopting SPIFFE is ideal for modern and cloud-native workloads only. SPIFFE is a great step in the right direction for granular machine and workload identity. However, adopting SPIFFE is a process requiring extensive work, supportability, application/services changes. It may not be ideal for systems, machines, and workloads that don’t have native support or integration with SPIFFE (for example COTS applications).. For these systems, you need to continue supporting existing machine identification frameworks and workflows with enterprise-ready PKI. Additionally, there is a learning curve associated with understanding and implementing SPIFFE, which may require additional training and resources to implement and manage SPIRE which would require high availability and maintenance. Hence, it’s recommended to leverage Vault Enterprise as the sole central identity management system for various use-cases including machine identity with PKI eliminating the need for point single-use-case solutions.

However, there are certainly some benefits to adopting SPIFFE especially for cloud-native infrastructure and workloads. If that’s something that you are directionally inclined to do, Vault Enterprise can help enable & accelerate SPIFFE adoption. While SPIFFE offers a robust framework for modern identity management, it requires a secure and scalable solution for the storage and management of cryptographic material linked to these identities. Typically enterprises have to deploy and operate something like SPIRE as a standalone distributed system which requires high availability, replication, and ongoing operations. Vault Enterprise not only enables the secure storage and management of cryptographic keys and certificates needed for issuing SPIFFE identities, but it also integrates with several identity providers to offer a range of authentication methods for workloads running across different environments.

O. Is Vault capable of scaling to support my business for certificates?

R. The [Starbucks case study](https://www.hashicorp.com/resources/starbucks-secrets-at-the-retail-edge-with-hashicorp-vault) highlights Vault Enterprise's scalability and efficiency in managing automated certificate renewal by supporting 100,000+ retail edge devices. Vault's dynamic secrets and automated certificate renewal reduce manual intervention, ensuring security and compliance. Its ability to scale horizontally allows it to handle high request volumes, making it ideal for growing organizations like Starbucks. Centralized management simplifies compliance and auditing, while seamless integration with existing systems minimizes infrastructure changes. Vault's robust security features ensure that all credentials and certificates are protected, supporting enterprise-level operations.