securosys

Solution Brief

HashiCorp Vault Enterprise and Securosys Primus HSM

Enhanced security for Vault Access and Secrets Management with Securosys Primus HSMs, on-premises or in the cloud

HashiCorp have partnered with Securosys to deliver enhanced security for their industry-leading HashiCorp Vault Enterprise solution. Through native support for Securosys Primus HSM and CloudHSM, Vault ensures that sensitive key material is securely offloaded and protected within tamper-resistant hardware security modules (HSMs). The high-availability capabilities of the Securosys Primus HSM, combined with FIPS and Common Criteria certifications, make it the ideal choice for secrets management deployments of all sizes. This integration strengthens the protection of cryptographic keys within HashiCorp Vault's security architecture.

Challenge

HashiCorp Vault provides centralized, well-audited privileged access and secrets management for mission-critical data – whether deployed on-premises, in the cloud, or across hybrid environments. However, if root keys are not adequately protected, the security of the entire solution can be compromised. Safeguarding these cryptographic keys is therefore essential to maintaining the integrity and security of your Vault installation.

Solution Benefits

Robust Key Protection: Primus HSMs ensure that your most sensitive keys always remain secured within the physical boundary of the HSM and are never exposed externally.

Automatic Unsealing: Vault Enterprise stores its Primus HSM-wrapped root key in storage, allowing for automatic unsealing.

Entropy Augmentation: Vault Enterprise can gather entropy generated by the HSM, providing a stronger source of randomness for cryptographic key generation.

Advanced Security Standards: Compliance with FIPS 140 Level 3 and Common Criteria EAL4+ delivers strong tamper protection and security assurance.

Seamless Integration: Full integration with HashiCorp Vault Enterprise for a streamlined setup and simplified management.

Flexible Deployment: Multiple deployment options available, including hardware and virtual appliances, with support for on-premises or CloudHSM environments.

Get started

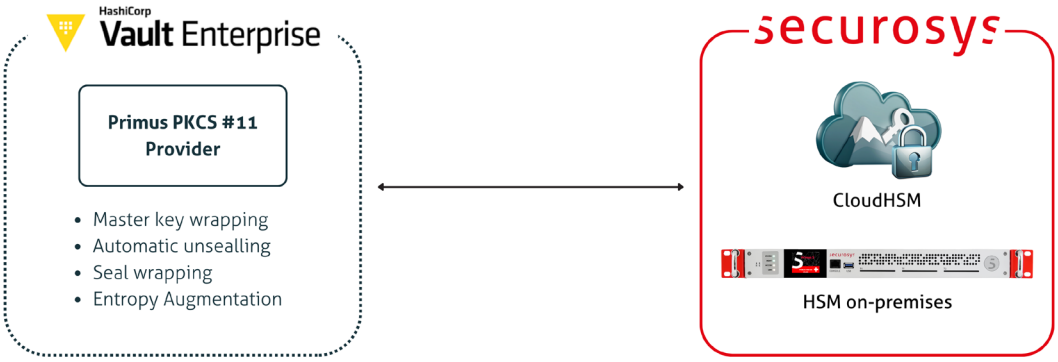
securosys

Solution Integration

Integrating Securosys Primus HSM with HashiCorp Vault enhances security by offloading critical cryptographic key material to a tamper-resistant environment. The HSM securely generates, stores, and manages sensitive keys. This approach ensures that keys remain secure and are never exposed outside the HSM, thereby significantly reducing the risk of key compromise and bolstering the overall integrity of the security architecture.

Vault Enterprise support for Primus HSMs also reduces the operational complexity associated with securing Vault unseal keys: Responsibility for securing those keys is delegated to trusted hardware rather than individuals. During startup, Vault connects to the delegated Primus HSM, providing an encrypted root key for decryption.

Securosys Primus HSMs integrate with HashiCorp Vault Enterprise through our PKCS#11 provider. All HashiCorp Vault HSM features are fully supported, from Vault Enterprise v1.7 onwards.



HSM Deployment Options

Use Cases

Secure Key Generation and Storage

Ensuring the security of cryptographic keys is critical for any organization. Securosys Primus HSM and CloudHSM provide high-entropy, hardware-based true random number generation and a tamper-resistant environment. While Vault Enterprise includes built-in key generation and storage capabilities, offloading this task to Securosys HSMs significantly enhances the underlying security of the solution.

Compliance with Security Standards

Meeting regulatory requirements such as PCI-DSS, HIPAA, and GDPR demands rigorous control over cryptographic key management. Integrating Hashicorp HashiCorp Vault Enterprise with Securosys Primus HSM or CloudHSM enables centralized key management on FIPS 140 Level 3 and Common Criteria EAL4+ certified hardware. This helps mitigate risks associated with key compromise and mismanagement while supporting compliance with stringent regulations.

About HashiCorp

About Securosys

HashiCorp