

Enhanced Data Security with HashiCorp Vault and Thales HSMs



Organizations today are faced with a paradigm shift where data is becoming the core of their business. As information increases in volume and value, enterprises are overwhelmed with the challenges of protecting and managing data sprawl. The problem of data protection is compounded as businesses adopt the cloud to host their infrastructure and information. With an ever-increasing data footprint and a fluid enterprise perimeter, defending and anticipating threat vectors is becoming more and more difficult.

Compliance and regulation offer significant guidance in attempting to limit the impact of breaches. Financial, Healthcare, and Government are just a few verticals that are strictly governed by how data can be stored, who has access to it, and its integrity, throughout its entire lifecycle. This helps to secure data and limit risk to all parties with access—organizations and their customers, however, compliance can provide challenges to organizations as well.

Meeting Increased Demand for Data Security is a Significant Challenge for Customers

As breaches increase in number and impact, so does the demand for encryption and strong key management across all infrastructure and workflows.

Although enterprises have moved a wide range of business services and workloads into the cloud, they still handle encryption and

key management much as they did several years ago: relying on traditional or custom solutions. These deployments are often costly, inflexible and unable to keep up with the evolving threat landscape and the increasing adoption of 'everything to the cloud'.

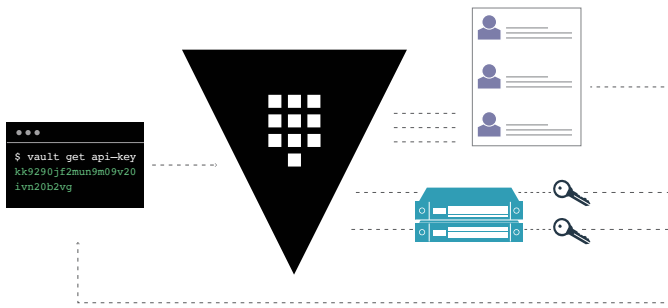
Compliance Best Practices & Overview:

- Growing emphasis on leveraging data encryption and/or anonymization techniques to safeguard data
- Best practices dictate that encryption keys should be stored securely
- Privacy regulations have become increasingly widespread
- Penalties are increasing for organizations that fail to meet compliance requirements

Security Best Practices:

- Identify and protect data where it matters, when it matters
- Leverage centralized key management with proper identity and access management
- Encrypt data with industry-compliant and certified solutions and algorithms
- Partner with best-of-breed security vendors to protect the entire ecosystem
- Revisit business processes and encryption strategy periodically to accommodate evolving threat landscape

Security Management Made Simple with Thales Luna Network HSM and Luna Cloud HSM services with HashiCorp Vault Enterprise



Thales family of HSM solutions, either Luna Cloud HSM Services on Data Protection on Demand (DPoD) or Luna Network HSM, provide companies the option of maintaining root of trust protection and management of encryption keys across cloud-based, hybrid/multi-cloud, on-premises, or a mixture of deployments. This flexibility makes it easier to deploy a cloud-based, on-premises, or hybrid solution to address ever-changing compliance mandates and budgetary requirements.

HSMs from Thales:

- Luna Cloud HSM Services is a cloud based hardware security module (HSMoD) that offers key management capabilities that can be deployed within minutes with no need for specialized hardware or associated skills
- Luna Network HSMs store, protect and manage sensitive cryptographic keys on-premises in FIPS 140-2 Level 3, tamper-resistant hardware appliances, providing high-assurance key protection within an organization's own IT infrastructure.

Solution Advantages

The integration between Thales HSM solutions and HashiCorp Vault enables key advantages:

Master Key Wrapping: Luna HSM solutions encrypt the Vault master key in a hardware root of trust to provide maximum security and comply with regulatory requirements.

Automated Unseal: Master keys are encrypted and stored by the HSMs, allowing users to automatically unseal Vault, using the key stored within the HSM. This eliminates the need for manual unsealing normally done by providing a pre-set minimum number of unseal keys, thereby improving the security posture.

HashiCorp Vault:

HashiCorp Vault centrally secures, stores, and tightly controls access to tokens, passwords, certificates, and encryption keys for protecting secrets and other sensitive data using a UI, CLI, or HTTP API. Organizations use HashiCorp Vault to solve security challenges as they adopt cloud and DevOps. Core use cases addressed include:

- **Secrets Management:** Centrally store, access, and distribute dynamic secrets such as tokens, passwords, certificates, and encryption keys.
- **Data Encryption:** Keep application data secure with centralized key management and simple APIs for data encryption.

Vault Enterprise communicates with Luna Network HSM or Luna Cloud HSM Services to decrypt the Master Key using PKCS #11 API.

Achieve Regulatory Compliance for your Application Infrastructure

Contact HashiCorp to determine how to protect Vault Enterprise keys in a cloud-based HSM on Demand service or a FIPS-validated on-premises HSM, providing maximum security and compliance for your applications.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing amount of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

About HashiCorp

HashiCorp is the leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. HashiCorp open source tools Vagrant, Packer, Terraform, Vault, Consul, and Nomad are downloaded tens of millions of times each year and are broadly adopted by the Global 2000. Enterprise versions of these products enhance the open source tools with features that promote collaboration, operations, governance, and multi-data center functionality. The company is headquartered in San Francisco and backed by Mayfield, GGV Capital, Redpoint Ventures, True Ventures, IVP, and Bessemer Venture Partners.

For more information, visit: hashicorp.com, or follow HashiCorp on Twitter @hashicorp.