Vault

Disk Encryption and Key Management with Vault Enterprise

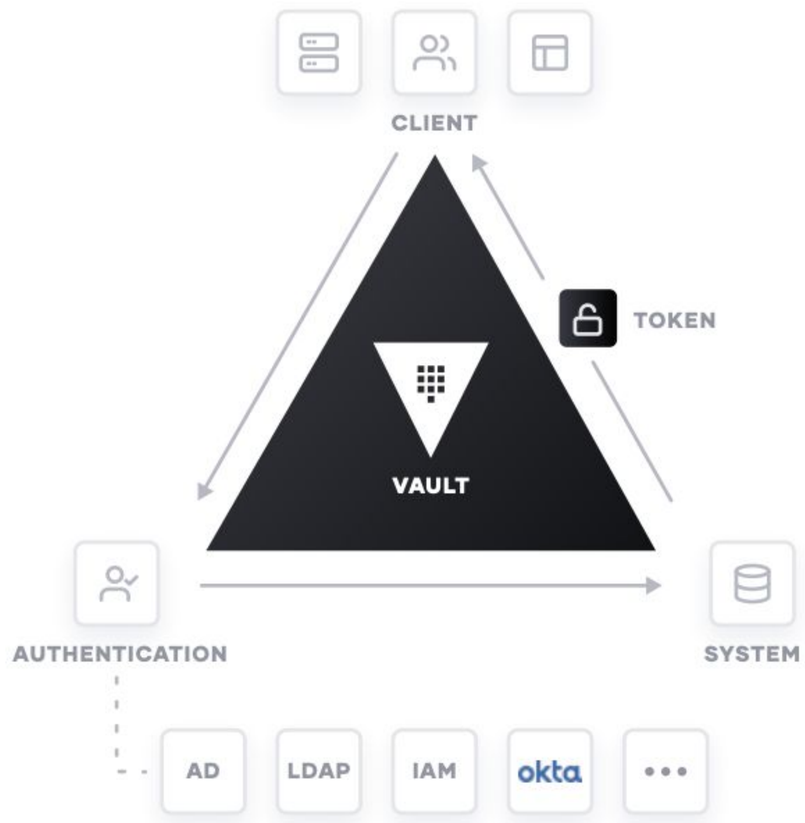
Part of the Advanced Data Protection Module

HashiCorp Vault

Vault allows you to secure, store and tightly control access to tokens, passwords, certificates, encryption keys, and other sensitive data using a UI, CLI, or HTTP API.

You can increase productivity, control costs by reducing systems, licenses and overhead by centrally managing all secrets operations. Vault can also assist with reducing the risk of a breach by eliminating static, hard-coded credentials by centralizing secrets.

- **Identity Brokering** for authentication and access to different clouds, policy enforcement, and easy automation.
- **Single Workflow** that integrates with existing infrastructure, reduces costs, and provides a unified audit trail.
- **Open & Extensible** strong open source community, large partner ecosystem, and full featured multi-cloud secrets engines.

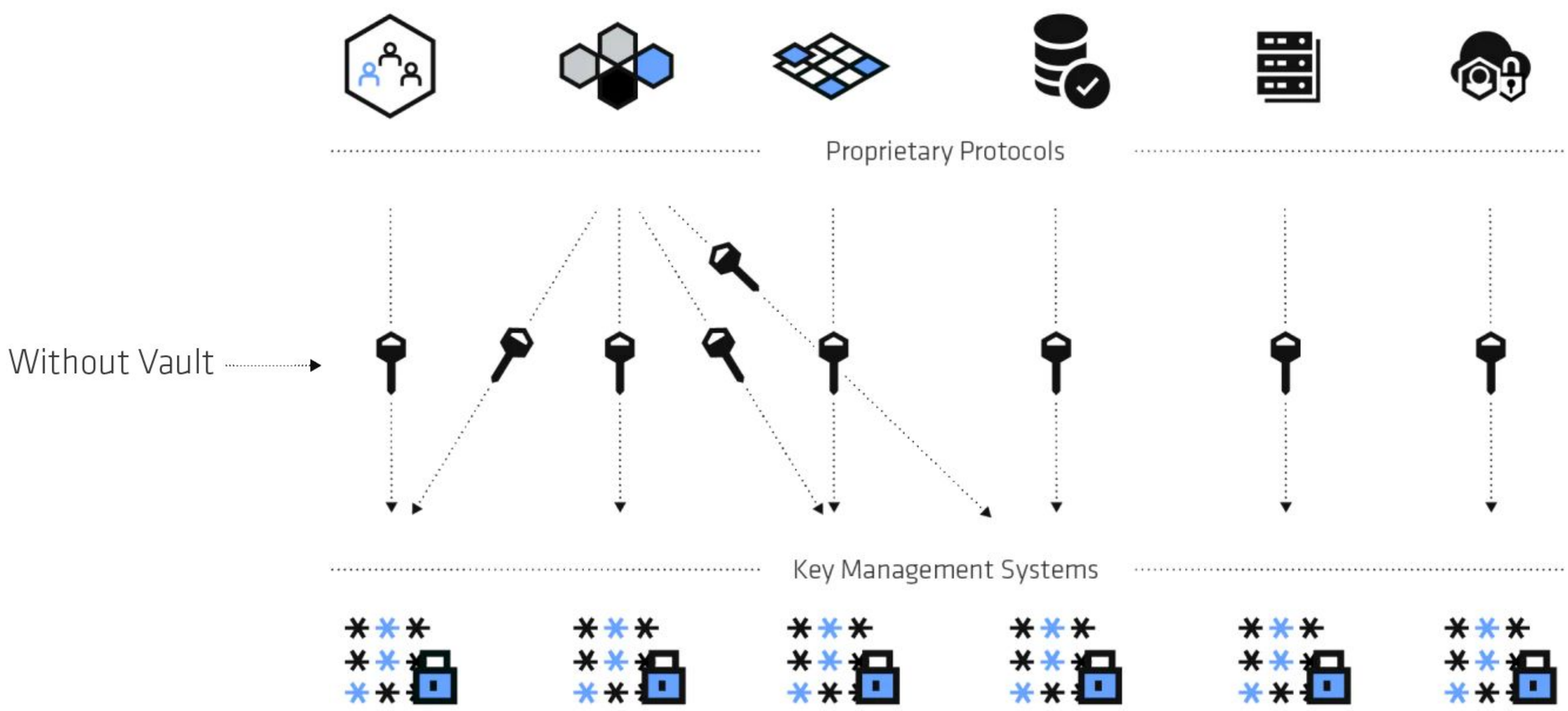


Disk Encryption and External Key Management with KMIP is here!

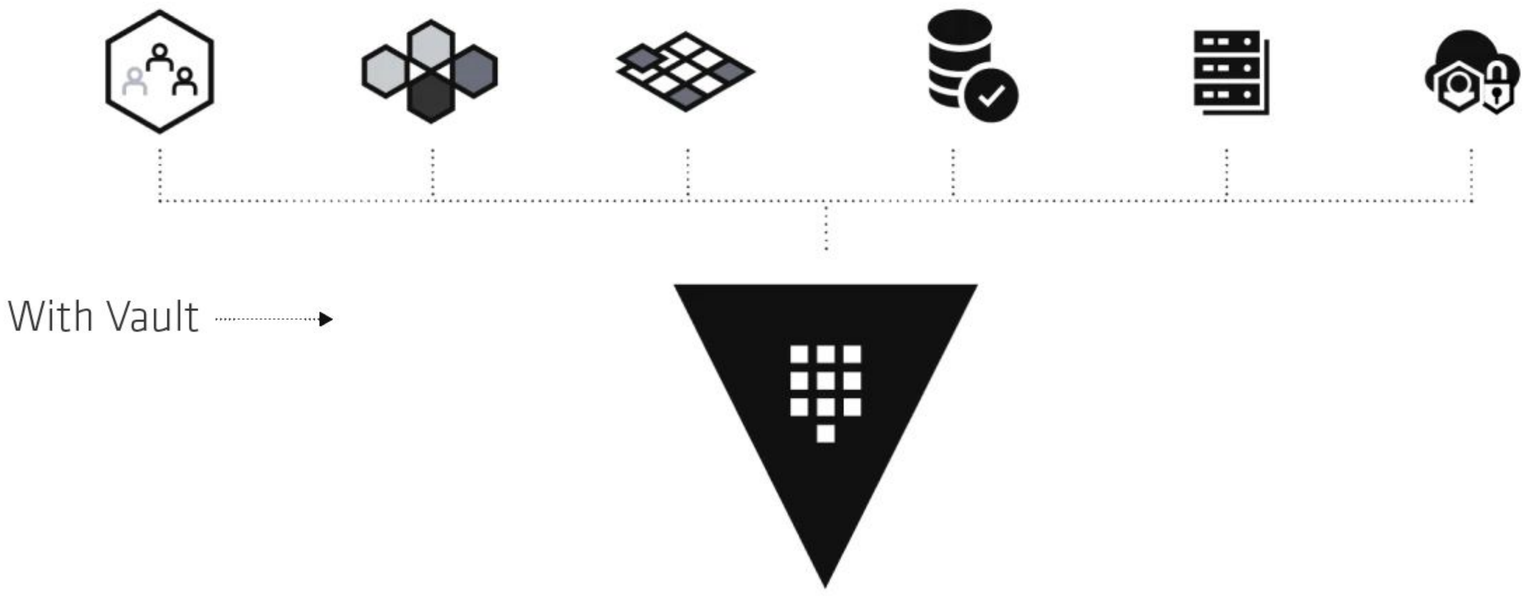
Vault Enterprise has introduced a new way for customers to secure workloads and protect data across traditional systems, clouds, and infrastructure. With the introduction of Vault KMIP in the latest release of Vault Enterprise, users can directly integrate and automate centralizing and protecting secrets and securing cryptographic workloads for enterprise on-premise and cloud infrastructure.

What is External Key Management with Vault

Traditional key management environments and applications use different/unique means to communicate. The added complexity and infrastructure costs, operational costs, and employee costs make running different systems cumbersome and complex. KMIP was developed to bridge the gap that existed across these different traditional systems. This creates an additional layer of complexity, which is how to bring traditional systems and cloud-based security into the same conversation.



Certain services and applications within organizations need to perform cryptographic operations, such as data encryption for storage at rest. These services do not necessarily want to implement the logic around managing these cryptographic keys, and thus seek to delegate the task of key management to external providers. Vault enables KMIP operations to be run through a dedicated, secure protocol to managing and executing Vault operations. With Vault Enterprise and the Advanced Data Protection module, customers can directly integrate Vault Enterprise with their secure workloads and enterprise workflows to cryptographic operations, such as, transparent database encryption, full disk encryption, virtual machine, and volume disk encryption etc, into one, easy-to-use workflow and API.



How Does It Work

Challenge

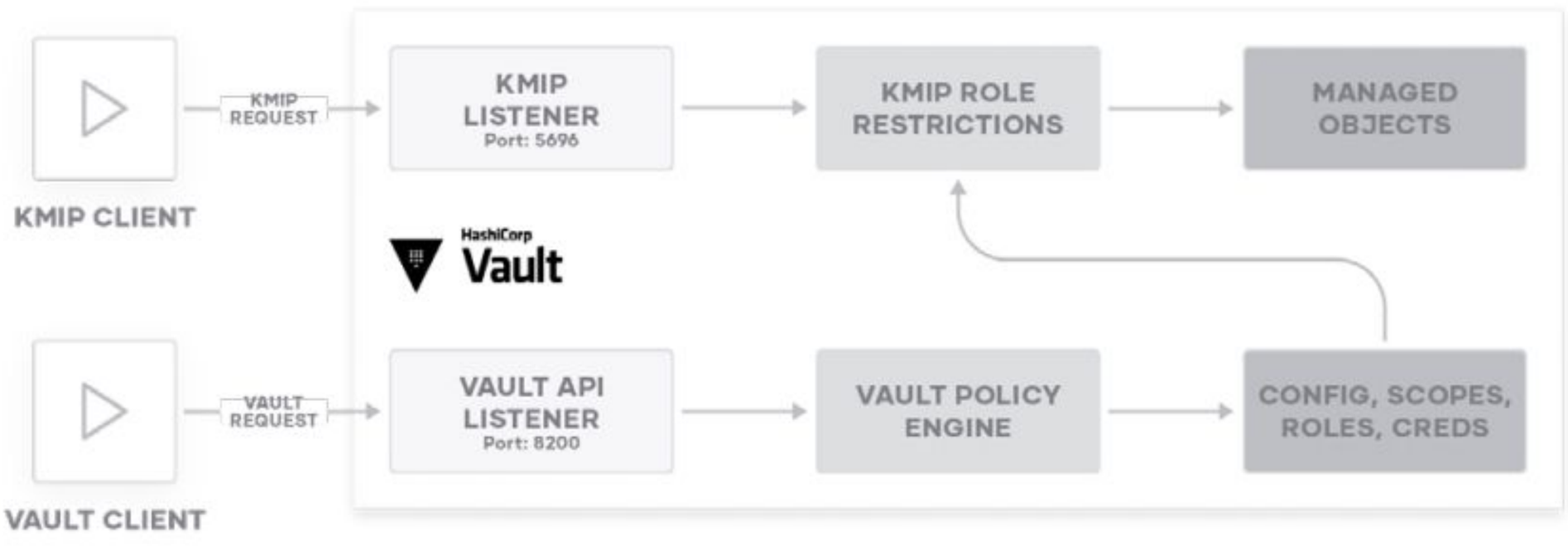
Organizations store sensitive, personal and valuable data, which must be protected. Leakage of such data can lead to financial loss, reputational damage, legal ramifications and more. There are often requirements to comply with data protection standards and regulations like the PCI DSS, GDPR, HIPAA, etc.

The OASIS Key Management Interoperability Protocol (KMIP) standard is a widely adopted protocol for handling cryptographic workloads and secrets management for enterprise infrastructure such as databases, network storage, and virtual/physical servers.

When an organization has services and applications that need to perform cryptographic operations (e.g. transparent database encryption, full disk encryption, etc), it often delegates the key management task to an external provider via KMIP protocol. As a result, your organization may have existing services or applications that implement KMIP or use wrapper clients with libraries/drivers that implement KMIP. This makes it difficult for an organization to adopt the Vault API in place of KMIP.

Solution

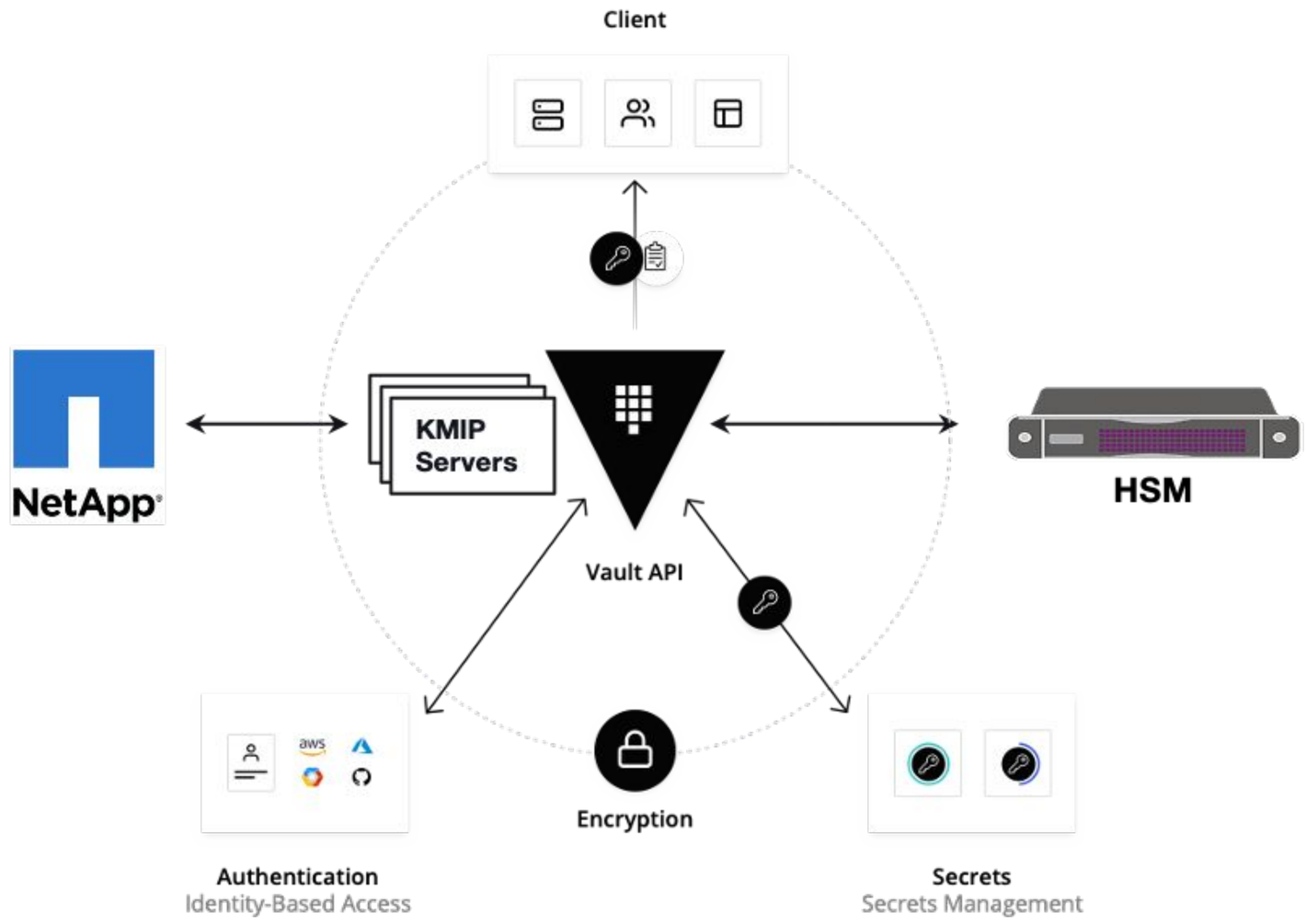
Vault Enterprise v1.2 introduced the KMIP secrets engine which allows Vault to act as a KMIP server for clients that retrieve cryptographic keys for encrypting data via KMIP protocol.



Vault's KMIP secrets engine manages its own listener to service KMIP requests which operate on KMIP managed objects. Vault policies do not come into play during these KMIP requests. The KMIP secrets engine determines the set of KMIP operations the clients are allowed to perform based on the roles that are applied to a TLS client certificate.

This enables existing systems to continue using the KMIP APIs instead of Vault APIs.

Disk Encryption and Key Management with Vault and NetApp



Securing NetApp Data with HashiCorp Vault

NetApp Encryption

NetApp offers state of the art secure data management, file-shares, backup, recovery, replication and disaster recovery solutions to a large number of enterprises all around the globe. The NetApp ONTAP system, which is one of the most popular storage operating systems in the world, offers FIPS compliant encryption technology that also supports the OASIS KMIP protocol.

NetApp Storage Encryption (NSE) is NetApp's implementation of Full Disk Encryption while NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE) are software-based, data-at-rest encryption solutions, available in NetApp ONTAP based systems. Although NetApp does offer an onboard key manager, most enterprises must use an external key manager for compliance reasons as the keys must be stored outside of the storage system.

Vault as an External Key Manager for NetApp

HashiCorp Vault is the de-facto standard for managing secrets in multi-cloud and hybrid enterprise environments. It is a simple, modern, scalable and highly automatable solution for management of all kinds of sensitive and secret data including passwords, keys, certificates, and encryption keys. One of the latest enterprise capabilities of Vault is a KMIP Secrets Engine which is the best solution for external key manager requirements for enterprise storage systems like NetApp ONTAP. Moreover, Vault can be integrated with an HSM for master key wrapping and auto unsealing.

For more on disk encryption and external key management with Vault and NetApp, download the **Securing NetApp Data White Paper**

Disk Encryption with Vault and VMware

Securing VMware Data with HashiCorp Vault

VMware Encryption

VMware Encryption was introduced with version 6.5 of VMware vSphere and allows integration with different types of Key Management Servers (KMS) for managing encryption keys. The process flow includes the KMS, the vCenter Server, and the ESXi host.

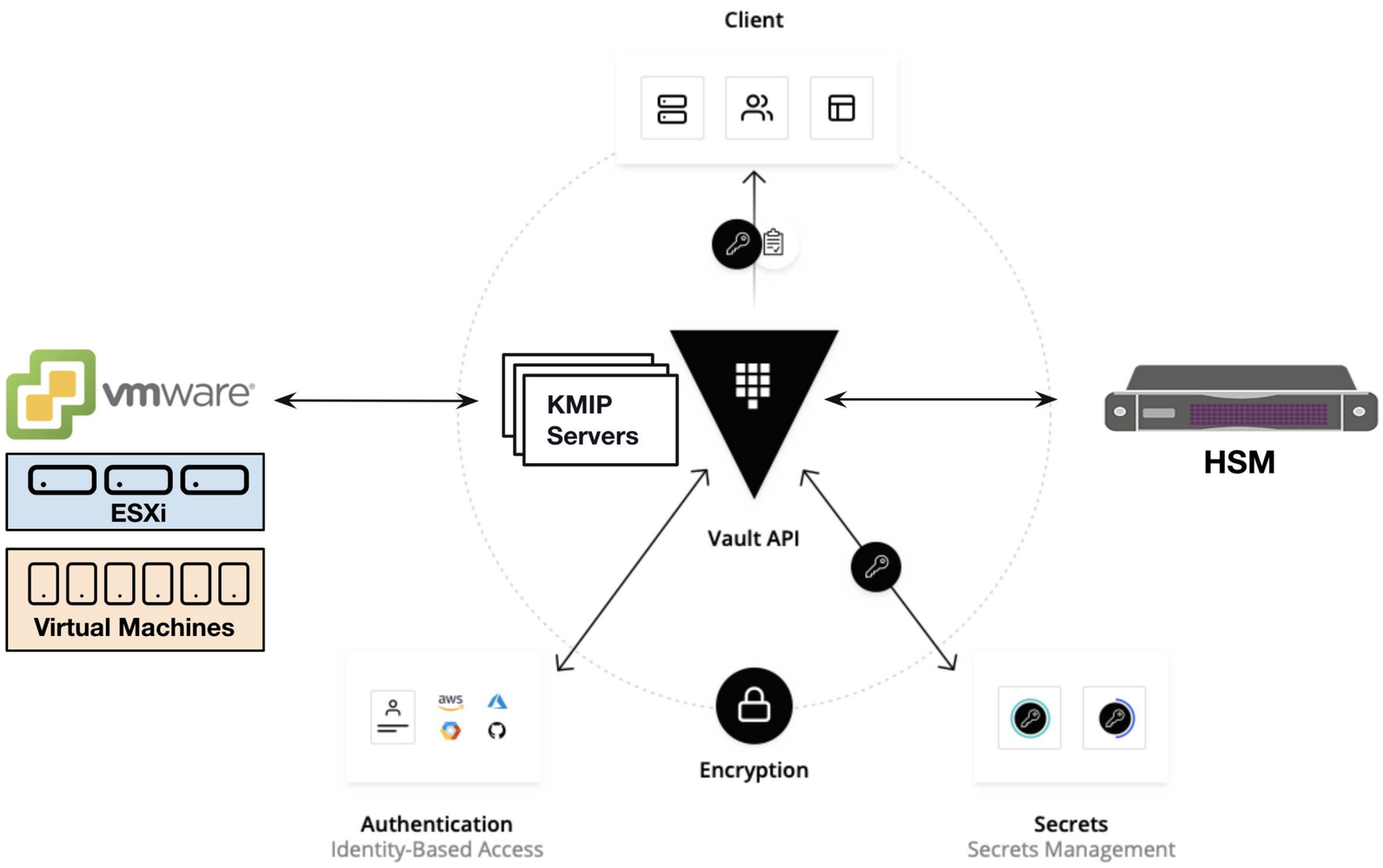
During the encryption process, different components interact as follows:

1. When the user performs an encryption task, for example, creating an encrypted virtual machine, vCenter Server requests a new key from the default KMS. This key is used as the Key Encryption Key (KEK).
2. vCenter Server stores the key ID and passes the key to the ESXi host. If the ESXi host is part of a cluster, vCenter Server sends the KEK to each host in the cluster. The key itself is not stored on the vCenter Server system. Only the key ID is known.
3. The ESXi host generates internal Data Encryption Keys (DEKs) for the virtual machine and its disks. It keeps the internal keys in memory only, and uses the KEKs to encrypt internal keys. Unencrypted internal keys are never stored on disk. Only encrypted data is stored. Because the KEKs come from the KMS, the host continues to use the same KEKs.
4. The ESXi host encrypts the virtual machine with the encrypted internal key. Any hosts that have the KEK and that can access the encrypted key file can perform operations on the encrypted virtual machine or disk.

What is encrypted	Details
Virtual machine files	Most virtual machine files, in particular, guest data that are not stored in the VMDK file, are encrypted. This set of files includes but is not limited to the NVRAM, VSWP, and VMSN files. The key that vCenter Server retrieves from the KMS unlocks an encrypted bundle in the VMX file that contains internal keys and other secrets. When you use the vSphere Client to create an encrypted virtual machine, you can encrypt and decrypt virtual disks separate from virtual machine files. All virtual disks are encrypted by default. For other encryption tasks, such as encrypting an existing virtual machine, you can encrypt and decrypt virtual disks separate from virtual machine files.
Virtual disk files	Data in an encrypted virtual disk (VMDK) file is never written in cleartext to storage or physical disk, and is never transmitted over the network in cleartext. The VMDK descriptor file is mostly cleartext, but contains a key ID for the KEK and the internal key (DEK) in the encrypted bundle. You can use the vSphere API to perform either a shallow recrypt operation with a new KEK or deep recrypt operation with a new internal key.
Core dumps	Core dumps on an ESXi host that has encryption mode enabled are always encrypted.

For more on disk encryption with Vault and VMware, download the **Securing VMware Data White Paper**

External Key Management with Vault and VMware



HashiCorp Vault as a KMS for VMware

- **Workflows, not Technologies:** Request secrets for any system through one consistent, audited, and secured workflow.
- **Secure Multi-tenancy:** Isolate different tenant environments for security and compliance. Different teams and departments can work independently of each other and have access to only their own keys and systems.
- **HSM Support:** Vault supports integration with any HSM that supports PKCS #11. Most hardware-based KMIP Servers only support specific HSMs.
- **Flexibility:** Most key managers are hardware devices and difficult to procure, manage and maintain. Vault gives you more flexibility as it is distributed as a binary and can be deployed across multiple platforms.
- **Cost and Efficiency:** One deployment of Vault can create multiple independent KMIP servers. Save time and cost as you don't need to buy and manage hardware devices for each department.
- **Management:** Vault is easy to manage and use, as it offers Web UI, CLI, and HTTP API interfaces.
- **High Availability:** Built-in High Availability using Consul as the storage back-end. Using Consul also provides automated registration, tagging, and health checks for Vault services within Consul.
- **Multi-datacenter replication:** Built-in multi-datacenter replication for horizontal scalability and disaster recovery use-cases.
- **Audit Logging:** With Vault's audit log, monitoring secret access across multiple environments and clouds is easy and automated.
- **Future-proof:** Vault comes power packed with multiple integrations like AWS, Azure, GCP, Kubernetes, Databases, and more to provide a central service for secret and certificate management, cryptographic and advanced data protection needs.

For more on key management with Vault and VMware, download the **Securing VMware Data White Paper**