HashiCorp Vault

HashiCorp Vault

HashiCorp Vault is a **secrets management tool** designed to securely store, access, and manage sensitive information such as **API keys, passwords, certificates, and encryption keys**. It provides **access control**, **data encryption**, and **dynamic secrets generation** to enhance security in DevOps and cloud environments.

Key Features:

- **Secret Storage** – Securely stores and manages secrets in an encrypted manner.
- **Access Control** – Uses policies and authentication methods (like LDAP, AWS IAM, Kubernetes) to restrict access.
- **Dynamic Secrets** – Generates temporary credentials for databases, cloud platforms, and other services, reducing exposure risks.
- **Data Encryption** – Encrypts data at rest and in transit, offering encryption-as-a-service for applications.
- **Audit Logging** – Tracks all access and changes for compliance and security monitoring.
- **Multi-Cloud & Hybrid Support** – Works with AWS, Azure, GCP, and on-premise environments.

Use Cases:

✅ Protecting **API keys & database credentials**

✅ Managing **TLS certificates & SSH keys**

✅ Securing **cloud infrastructure credentials**

✅ Enforcing **role-based access control (RBAC)**

It is widely used in **DevOps, SRE, and security teams** to manage secrets and enhance infrastructure security. 🚀🔐