

Vault

Your Safe for Cross Cloud Secret Management

Streamline operations across diverse cloud platforms with Vault. Centralize key control and bolster data protection for multi-cloud security.

Secure your credentials for secrets, keys and more

Upgrade your organization's data security with Vault, a comprehensive solution for multi-cloud key provisioning and management.

Vault ensures **top-tier protection of your sensitive data**, outperforming traditional encryption methods at every stage - be it at rest, in transit, or at run-time. Plus, enjoy **global compatibility and compliance with privacy export regulations**, including Schrems-II, ensuring seamless international data handling.



About Confidential Computing



Confidential computing represents a breakthrough advancement in data security. It enables environments - whether container, application or VM - to run in a fully encrypted form.

This means that throughout the entire operational cycle, from startup to termination, these environments remain encrypted. Data and program flows are **cryptographically isolated from the rest of the system** thanks to this runtime encryption.

Only the CPU - and no other components or processes - can decrypt this encrypted environment, execute instructions, and then store results in encrypted form again.

Current Challenges



Cost

Cloud-based key management services using traditional HSMs can be expensive and costs can increase with usage and number of keys. Cost management is crucial.



Loss of control

Cloud key management provides convenience, but it may result in a loss of control over cryptographic keys. It is essential to have trust in the security practices of the provider. No system is entirely immune to security risks, and security breaches, insider threats, and vulnerabilities can still occur.



Vendor Lock-In

Many cloud providers offer their own key management services, which can result in vendor lock-in. If you rely heavily on the provider's key management service, switching to another cloud provider or on-premises solution can be complex.

Vault enables your organization to have complete control over your confidential information, no matter where you are.

▶▶ Identity and Access Management

Authentication:

Integrate various authentication methods including username/password and SSO, and instantiate workloads and services using JSON web tokens with cloud platform IAMs such as AWS, Azure, and GCP.

Authorization:

Design fine-grained access control based on roles or groups. Assign users to specific roles and grant privileges to secrets, resources, and workload based on their roles.

▶▶ Key Management

Secrets Store:

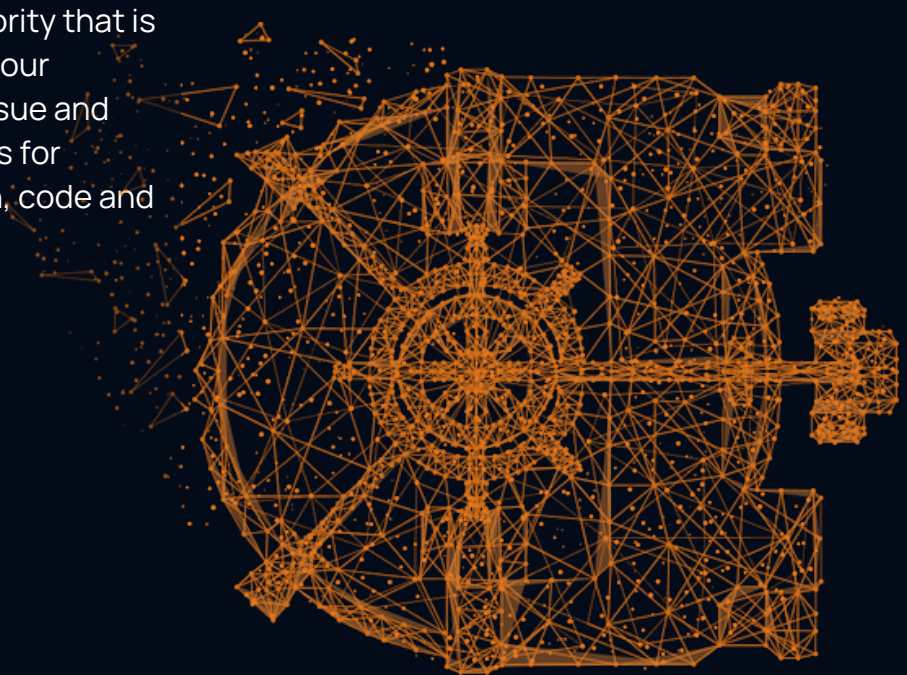
- Safeguard credentials, certificates, and keys from exposure while maintaining a swift development pace.
- Enhance your organization's security posture without compromising efficiency.

Cryptography as a Service:

- Utilize a spectrum of NIST/BSI-standardized cryptographic algorithms, such as PKCS, EC, and PQ.
- Seamlessly integrate encryption, digital signatures, secure key management, and more into your applications and systems.

PKI as a Service:

- Create a Certificate Authority that is specifically designed for your organization. Efficiently issue and manage digital certificates for SSL/TLS, email encryption, code and document signing.



Benefits

▶▶ Elasticity

Efficiently and swiftly adjust resource scaling, allowing it to flexibly accommodate fluctuating demands without the need for excessive resource allocation.

▶▶ Crypto Agile

Manage PKCS, EC, and PQ-ready cryptography in a way that allows for flexibility and adaptability to changing NIST/BSI/NATO cryptographic standards and crypto-analytical breakthroughs.

▶▶ Multi-Cloud Support

Vault can be deployed on-premises or in any cloud of your choice, making it suitable for hybrid, confidential and cross-cloud architectures.

▶▶ Hardware Graded Security

Establish trust in the hardware foundation by selecting either the CPU, TPM, HSM as the anchor and source of randomness.

Deployment Options

Vault standalone

- Flexible deployment option.
- Can be deployed on any hypervisor.
- Can be installed on bare metal infrastructure.
- Allows the user to choose their operating system.

Vault integrated with vHSM

- This is a cloud-ready offering.
- It seamlessly integrates with vHSM (Virtual Hardware Security Module).
- Utilizes encryption functionality from either AMD or Intel.

SaaS on enclave Cloud

- This is a Software-as-a-Service (SaaS) model.
- It's ready-to-use and hosted on enclave's cloud infrastructure.

Learn more

About enclave

enclave enables businesses to securely protect their sensitive data and applications in untrusted cloud environments by leveraging the use of Confidential Computing.

Its comprehensive, multi-cloud operating system allows for **Zero Trust security** by encrypting data in use and shielding applications from both the infrastructure and solution providers.

With enclave, businesses can confidently build, test, and deploy a wide range of cloud applications, all while **maintaining complete control over their confidential information**. enclave's goal is to provide a universal, cloud-independent technology for enclaving sophisticated multi-cloud applications, that can be deployed with confidence and ease.

Contact details



github.com/enclave



[linkedin.com/company/enclave](https://www.linkedin.com/company/enclave)



<https://enclave.io>



[youtube.com/@confidentialcompute](https://www.youtube.com/@confidentialcompute)

CONTACT

contact@enclave.io

+49 30233292973

Chausseestr. 40, 10115 Berlin, Germany



Making the Cloud the safest place for digital businesses