enclaive

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.

virtual HSM

Elevate Your Infrastructure: Unleash Crypto-Agility, Elasticity, and Cloud-Ready Security!

Upgrade your infrastructure without the need for costly hardware investments. Enjoy the benefits of crypto-agility, elasticity, and cloud readiness for secrets and workload identity management.

vHSM seamlessly combines the power of Vault and Nitride to offer an all-in-one security solution.

With Vault's strong credential protection and Nitride's secure Workload Identity and Access Management (WIAM), vHSM ensures the **highest level of security for your secrets**, keys, and machine identities.

Trust in **hardware-rooted identities, automated workload authentication, and access control management**, all within a single, comprehensive package.

enclaive

Current Challenges

Operational Cost

HSMs can increase the cost of cloud-native development projects due to additional maintenance, monitoring, and support requirements. Cloud-native applications are cost-optimized and may not need HSMs, which are expensive. Consider their cost-effectiveness before adopting HSMs for cloud-native development projects.

Latency Issues

Cloud-native applications often use microservices architectures and aim for low-latency interactions. However, physical HSMs can introduce additional latency, which may not be acceptable for some cloud-native use cases.

Scalability

HSMs may lack flexible demand-driven scalability, which is essential for modern cloud-based applications. Adding more physical HSMs does not align with the dynamic needs of modern business applications.

vHSMs deliver the same level of trust and security anchored in hardware with the benefit of shifting functionality into enclaves.

enclaive

Elasticity:

Easily and rapidly scale the resources up or down to meet changing demand. This ensures that the vHSM can adapt to varying needs without the need to over-provisioning.

Scalability:

Horizontal scalability involves adding more vHSM instances to a system to handle increased load and capture trusted domains over multiple, mutually isolated trusted domains/organizations.
Vertical scalability involves increasing the capacity and power of a single machine, typically addressing high-performance needs.

Hardware Trust Anchor:

Choose a hardware anchor such as CPU, TPM, HSM, or Cloud HSM to root trust and ensure the integrity of enclaive's confidential boot and attestation technology.

Easily Pluggable:

Add, update, or remove features with the high pace required today through enclaved virtualization.

enclaive

Benefits

Cost Efficiency

Elasticity helps organizations optimize their spending. You pay for the resources you use, and you don't need to provision for peak loads all the time. This can result in cost savings because you're not maintaining and paying for resources that are underutilized during off-peak periods.

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.

Auto-Scaling

Scalability enables the automatic provisioning and de-provisioning of resources based on real-time demand. When the vHSM experiences increased traffic or workloads, it can automatically add more computing resources (like virtual machines) to handle the load. When the demand decreases, the resources are scaled down to save costs.

Auto-Healing

If a vHSM fails, the vHSM can quickly replace it with a new cluster, maintaining service availability across multiple servers, data centers or cloud service providers. Encrypted storage is redundantly replicated and sealed to each vHSM instance.

Faster Time-to-Market

Easily add new services or features without committing to long-term investments. You can quickly test and deploy new vHSM updates and adjust as simple as replacing a VM.

enclaive

Deployment Options

vHSM standalone

- Deploy any confidential compute-ready system in your IT environment.
- Deploy on IaaS environments that are open to support Confidential Computing.

vHSM in the Cloud

- vHSM can be deployed on the currently supported clouds by enclaive:
  - the Hyperscalers (Azure, AWS, GCP)
  - Selected regional players

SaaS on enclaive Cloud

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

enclaive

Learn more

About enclaive

enclaive 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 enclaive, businesses can confidently build, test, and deploy a wide range of cloud applications, all while **maintaining complete control over their confidential information**. enclaive'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/enclaive

linkedin.com/company/enclaive

https://enclaive.io

youtube.com/@confidentialcompute

CONTACT

contact@enclaive.io
+49 30233292973
Chausseestr. 40, 10115 Berlin, Germany
enclaive.io