enclaive

vHSM

Virtual HSM

Take control of your keys, identities, and workloads —for maximum cloud sovereignty

Protect your sensitive data with our **virtual Hardware Security Module (vHSM)**—flexible, scalable, and without costly hardware installations. Our solution provides secure key management, enables you to meet the highest compliance standards, and integrates seamlessly into your existing IT infrastructure.

Challenges

Hardware Security Modules (HSMs) deliver a higher level of protection than software-based solutions because they are tamper-resistant and physically secured. However, traditional HSMs were never designed for cloud-native environments, which creates growing challenges for modern organizations:

Limited Scalability

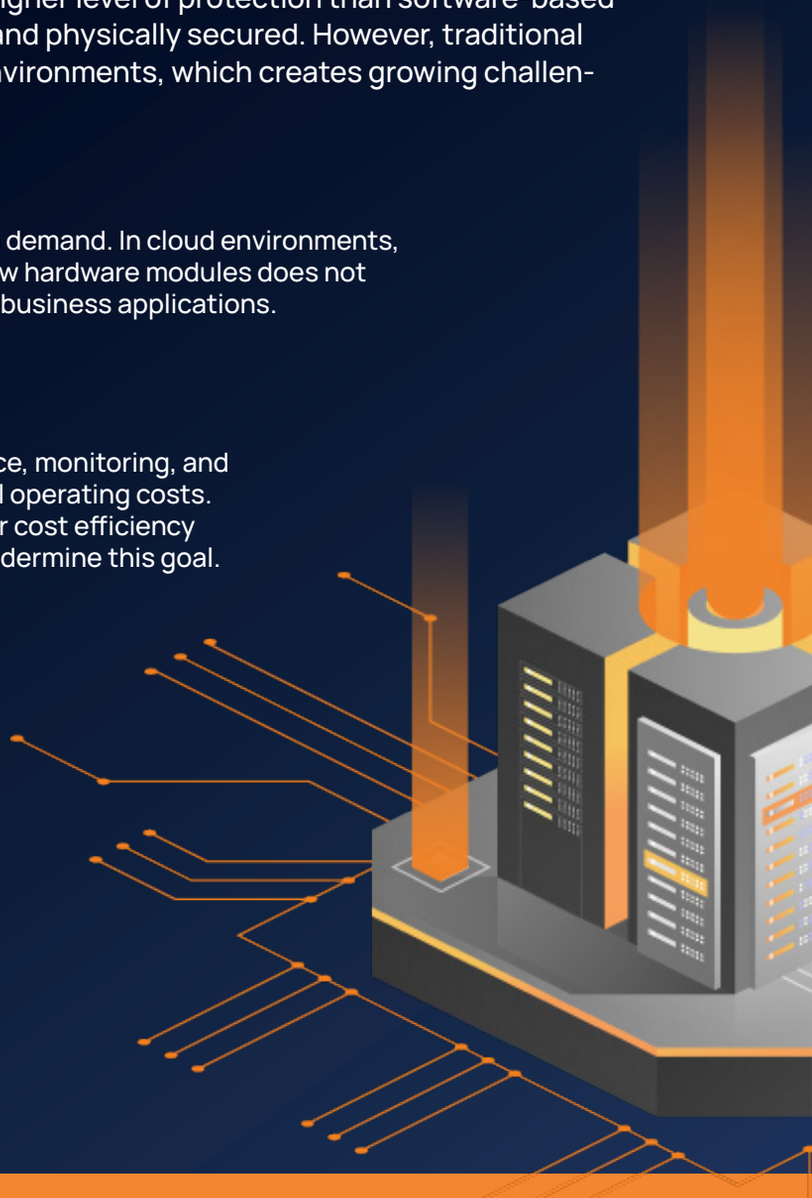
Physical HSMs cannot easily scale on demand. In cloud environments, scalability is essential, and adding new hardware modules does not match the agility required by modern business applications.

High Maintenance Costs

HSMs require continuous maintenance, monitoring, and support, significantly increasing total operating costs. Cloud-native applications are built for cost efficiency —but hardware-based HSMs often undermine this goal.

Latency Constraints

Cloud-native applications depend on low latency and microservices architectures. Physical HSMs can introduce additional delays that are unacceptable for certain real-time or high-performance workloads.



Our Solution

Our vHSM combines the powerful key and identity management of Vault with the robust workload identity management of Nitride—delivering an all-in-one security solution that ensures maximum protection for your data, keys, and machine identities.

Vault

Our cross-cloud key management solution gives you full control (Hold Your Own Key) to secure, manage, and centrally orchestrate cryptographic keys across multiple cloud platforms—ensuring transparency, compliance, and security.

Nitride

Our workload identity and access management solution enables secure authentication and authorization of workloads across platforms. For audits, it provides verifiable proof of the integrity of confidential execution environments.

Elasticity: Quickly and flexibly adjust resources to current demand, avoiding overprovisioning and optimizing cost efficiency.

Modular: Add, update, or remove functions dynamically through enclave virtualization for maximum adaptability.

Hardware Trust Anchor: Establish trust at the hardware level—leveraging CPU, TPM, HSM, or Cloud HSM as the foundation. Validate integrity with enclaive's Confidential Boot and Attestation technologies.

Scalability: Handle higher workloads by deploying additional vHSM instances, extend trusted perimeters across domains and organizations, and increase capacity for high-performance demands.

Sovereignty: Maintain full control over your keys in any cloud environment and verify the integrity of workloads and execution environments at all times.

Why Choose vHSM

- **Automated Scaling:** The vHSM automatically adjusts computational resources based on workload and access demand, reducing costs and improving efficiency.
- **Self-Healing:** If a vHSM instance fails, a new cluster replaces it automatically. Data remains encrypted, redundantly replicated, and continuously available.
- **Cost Efficiency:** Pay only for the resources you actually use.
- **Accelerated Time-to-Market:** Quickly add, test, and deploy new services and features to shorten development cycles and enable rapid innovation.

Learn more:
enclaive.io/virtual-hsm

Mail: contact@enclaive.io
Tel.: +49 302 33 29 29 73
Chausseestr. 40, Berlin, Germany