

Virtuelles HSM

Übernehmen Sie die Kontrolle über Ihre Schlüssel, Identitäten und Workloads – für maximale Cloud-Souveränität

Schützen Sie Ihre sensible Daten zuverlässig mit unserem virtuellen Hardware Security Modul (vHSM) – flexibel, skalierbar und ohne teure Hardware-Installationen. Unsere Lösung ermöglicht Ihnen ein sicheres Schlüsselmanagement, hilft Ihnen dabei, höchste Compliance-Anforderungen zu erfüllen, und lässt sich nahtlos in Ihre IT-Infrastruktur integrieren.

Herausforderungen

HSMs (Hardware Security Modules) bieten ein höheres Sicherheitsniveau im Vergleich zu softwarebasierten Lösungen, da sie manipulationssicher und physisch geschützt sind. Allerdings sind HSMs nicht für die Cloud oder Cloud-native Anwendungen ausgelegt, was moderne Unternehmen vor immer größere Herausforderungen stellt:



Einschränkung bei der Skalierung

HSMs weisen Einschränkungen in Bezug auf flexible, bedarfsorientierte Skalierbarkeit auf. In Cloud-Umgebungen ist Skalierbarkeit eine grundlegende Anforderung, und das Hinzufügen weiterer physischer HSMs passt nicht zu der Dynamik, die moderne Geschäftsanwendungen erfordern.



Kostspielige HSM-Wartung

HSMs erfordern kontinuierliche Wartung, Überwachung und Unterstützung, was die Gesamtbetriebskosten erheblich erhöht. Cloud-native Anwendungen sind darauf ausgelegt, Kosten zu optimieren. Die hohen Kosten für HSMs passen möglicherweise nicht zu den Kosteneffizienzielen der Cloud-nativen Entwicklung.



Niedrige Latenz

Cloud-native Anwendungen setzen oft auf niedrige Latenzzeiten und Microservices-Architekturen. Der Einsatz physischer HSMs kann zusätzliche Latenzen verursachen, die für bestimmte Cloud-native Anwendungsfälle nicht akzeptabel sind.

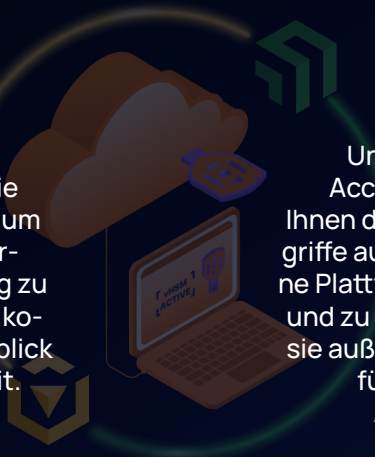


Unsere Lösung

Unser vHSM vereint das leistungsstarke Key & Identity-Management von **Vault** mit dem zuverlässigen Workforce Identity Management von **Nitride** in einer All-in-One-Sicherheitslösung – und gewährleistet so ein Höchstmaß an Sicherheit für Ihre Daten, Schlüssel und Maschinenidentitäten.



Unsere Cross-Cloud Key-Management-Lösung gibt Ihnen die volle Kontrolle (Hold Your Own Key), um kryptografische Schlüssel über verschiedene Cloud-Plattformen hinweg zu sichern, zu verwalten und zentral zu koordinieren. So behalten Sie den Überblick und sorgen für maximale Sicherheit.



Unsere Workload-Identity-and-Access-Management-Lösung gibt Ihnen die Werkzeuge an die Hand, um Zugriffe auf Ihre Workloads über verschiedene Plattformen hinweg sicher zu verwalten und zu authentifizieren. Für Audits bietet sie außerdem den technischen Nachweis für die Integrität vertraulicher Ausführungsumgebungen.

Elastizität: Passen Sie Ressourcen schnell und flexibel an den aktuellen Bedarf an und vermeiden Sie so eine Überprovisionierung von Kapazitäten.

Modular: Ergänzen, aktualisieren oder entfernen Sie Funktionen schnell und flexibel durch Enklaven-Virtualisierung.

Hardware Trust Anchor: Verankern Sie das Vertrauen in der Hardware aufsetzend auf CPU, TPM, HSM oder Cloud-HSM als Grundlage. Prüfen Sie die Integrität mit der Confidential Boot- und Attestation-Technologie von enclave.

Skalierbarkeit: Bewältigen Sie höhere Auslastungen durch zusätzliche vHSM-Instanzen, erweitern Sie vertrauenswürdige Bereiche über mehrere Domains oder Organisationen und steigern Sie Kapazität und Leistung für High-Performance-Anforderungen.

Souveränität: Behalten Sie in jeder Cloud die volle Kontrolle über Ihre Schlüssel und überprüfen Sie die Integrität Ihrer Workloads und Ausführungsumgebungen.

Warum Sie auf vHSM setzen sollten

- **Automatisierte Skalierung:** Das vHSM passt Rechenressourcen automatisch an steigende oder sinkende Workloads und Zugriffe an, spart unnötige Kosten und erhöht die Effizienz.
- **Self-Healing:** Fällt ein vHSM aus, ersetzt ein neues Cluster die Instanz automatisch. Daten bleiben verschlüsselt, redundant repliziert und jederzeit verfügbar.
- **Kosteneffizienz:** Bezahlen Sie nur für die Ressourcen, die Sie tatsächlich nutzen.
- **Verkürzte Time-to-Market:** Neue Services und Funktionen lassen sich schnell hinzufügen, testen und bereitstellen. So einfach wie das Austauschen einer virtuellen Maschine.