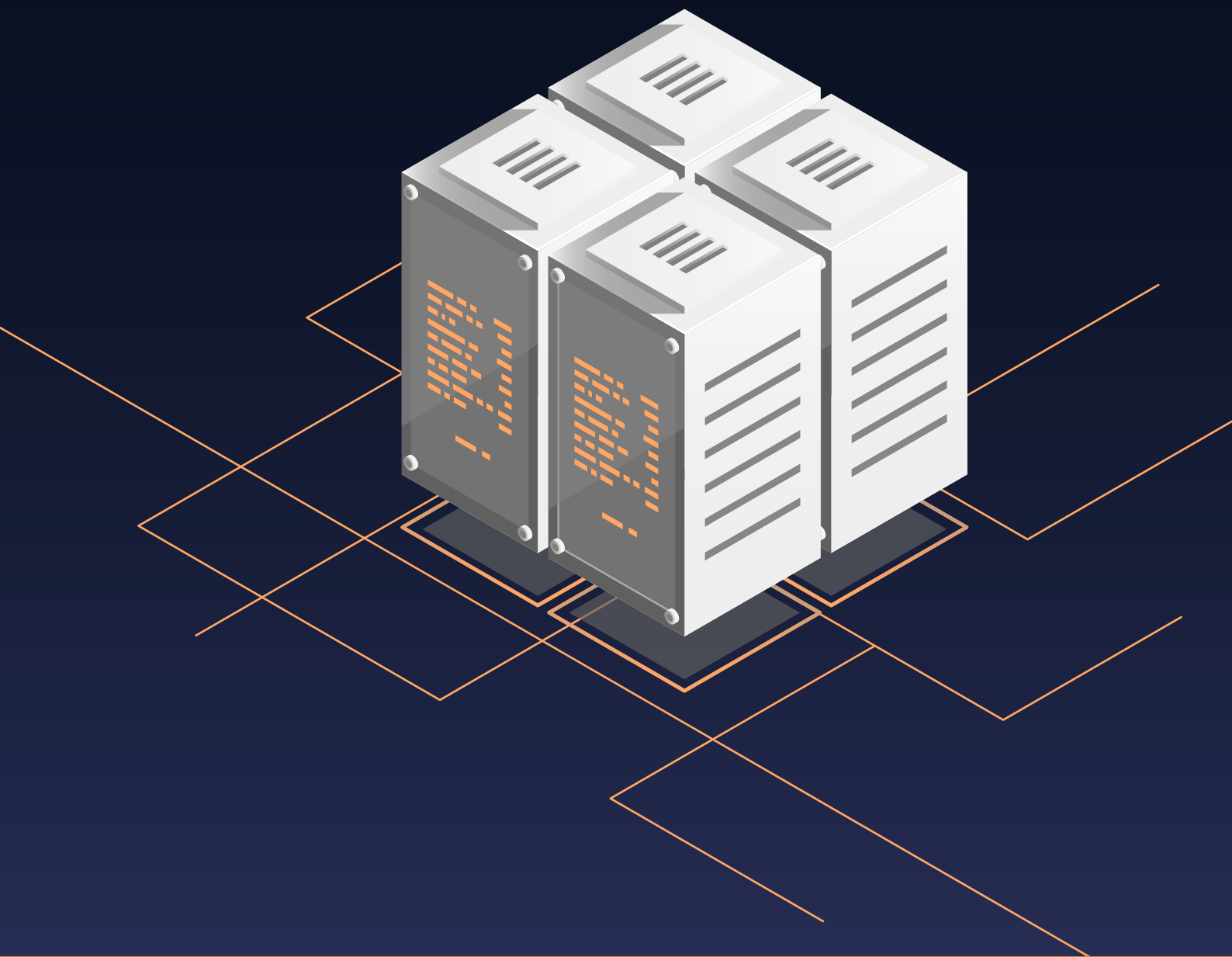
enclaive

Solution Brief

Cloud-Souveränität in Hyperscaler-Umgebungen

Confidential Computing als sicheres Fundament für performante Cloud-Netzwerke



Executive Summary

Deutsche und europäische Organisationen stehen vor einem strategischen Dilemma: Um ihre digitale Transformation voranzutreiben, sind sie auf die Rechenleistung der US-Hyperscaler angewiesen – riskieren dabei jedoch Compliance-Verstöße und den Verlust ihrer Datenhoheit.

Confidential Computing von **enclaive** löst diesen Zielkonflikt. Die Technologie schützt Daten auch während der Verarbeitung und macht es möglich, Cloud-Umgebungen sicher zu nutzen, ohne dem Cloud-Provider vertrauen zu müssen – denn dieser hat weder Einsicht noch Zugriff auf die Daten.

enclaive setzt mit seinen Lösungen dabei auf einen ganzheitlichen Ansatz, um Cloud-Umgebungen abzusichern:

- Die **eMCP** (enclaive Multi-Cloud Platform) ermöglicht eine ausfallsichere Multi-Cloud-Architektur über mehrere Cloud-Anbieter hinweg.
- Mit **Vault** behalten Anwender dank unabhängigem Key Management (Hold Your Own Key) die volle Kontrolle über kryptografische, Post-Quanten-sichere Schlüssel.
- **Nitride** gewährleistet die nachweisbare Integrität vertraulicher Workloads und der zugrundeliegenden Infrastruktur.

Gemeinsam schaffen diese Lösungen das Fundament für eine sichere, performante und Compliance-konforme Cloud-Nutzung – und damit für echte digitale Souveränität in Hyperscaler-Umgebungen.

Einleitung

Digitale Services gleichermaßen performant und hochsicher bereitzustellen, hat in Deutschland und Europa gerade höchste Priorität. Öffentliche Einrichtungen, das Gesundheitswesen oder der Finanzsektor verwalten eine Vielzahl hochsensibler Daten und komplexer Anwendungen, die skalierbare, hochverfügbare Cloud-Umgebungen erfordern.

US-Hyperscaler bieten genau diese Leistungsfähigkeit: Sie liefern modernste Cloud-native Services, High-Performance-Computing, fortschrittliche KI-Modelle und ein umfangreiches Ökosystem. Damit sind sie europäischen Anbietern aktuell weit überlegen. Für viele Unternehmen und Organisationen sind diese Dienste daher unverzichtbar, um neue Projekte und Services oder ihre digitale Transformation erfolgreich voranzutreiben.

Herausforderungen

Die Nutzung von US-basierten Cloud-Services ist allerdings mit hohen Risiken und Herausforderungen verbunden:

- **Gefährdete Datenhoheit:** US-Gesetze wie der CLOUD Act oder FISA 702 erlauben es US-Behörden, Daten amerikanischer Provider anzufordern. Dies betrifft auch in der EU gespeicherte Daten europäischer Organisationen.
- **Vendor Lock-in:** Abhängigkeiten von einzelnen Anbietern schränken die Flexibilität ein und erschweren Exit-Strategien.
- **Infrastruktur und Kill-Switch:** Das Hardware-Fundament der Hyperscaler könnte gezielt zum Abfließen von Daten manipuliert werden. Oder das Abschalten der Server oder Löschen von Daten, etwa im Zuge politischer Verwerfungen, könnte kritische Systeme abrupt lahmlegen.
- **Regelwerke und Nachweispflicht:** Strenge Vorschriften wie DSGVO oder DORA verlangen hohe Sicherheitsniveaus für Cloud-Umgebungen, gerade beim Übertragen, Speichern und Verarbeiten von Daten im Ausland. In der Regel fehlt hier der technische Beweis für die Vertraulichkeit der Daten.

Mit Blick auf diese Risiken sind Hyperscaler für viele Unternehmen und Einrichtungen keine Option. Ein Verzicht würde die Digitalisierung jedoch faktisch ausbremsen und bestehende Cloud-basierte Workloads stark einschränken. Daher braucht es eine Brückentechnologie, die absolute Vertraulichkeit und Souveränität in jeder Cloud-Umgebung bietet.

Die Lösung:
Confidential Computing von enclaive

Confidential Computing schließt eine der letzten großen Sicherheitslücken in der Cloud – den Schutz von Data in Use. Klassische Verschlüsselungstechniken konnten Daten bisher nur im Ruhezustand (Data at Rest) und während der Übertragung (Data in Transit) absichern, während Informationen bei der Verarbeitung bislang ungeschützt blieben. Confidential Computing verlagert sensible Workloads in hardwarebasierte, isolierte „Trusted Execution Environments“ (TEEs) – auch Enklaven genannt – und schützt Daten so in allen drei Dimensionen vor nicht-autorisierten Zugriffen, auch von Seiten der Administratoren oder Cloud-Provider.

Warum enclaive?

enclaive unterliegt als Berliner Unternehmen der deutschen Gerichtsbarkeit und bietet ein breites Confidential-Computing-Portfolio – speziell zugeschnitten auf die Anforderungen streng regulierter Branchen und geeignet für den Einsatz auf der Hyperscaler-Infrastruktur. Das Grundprinzip ist einfach: Mit enclaive müssen Sie Ihrem Cloud-Anbieter nicht mehr blind vertrauen.

Unsere Lösungen schaffen ein robustes Fundament für die sichere Nutzung von Hyperscalern:

EMCP

Die eMCP ist eine sichere, mandantenfähige Plattform, in der sich Datenbanken, virtuelle Maschinen (enclaive Buckypaper) und Kubernetes (enclaive Dyneemes) über US-Hyperscaler und europäische Cloud-Anbieter hinweg verwalten, betreiben und skalieren lassen. Die redundante Multi-Cloud-Architektur bietet ein hohes Maß an Flexibilität und verhindert Vendor-Lockin- und Kill-Switch-Szenarien.

Vault

Anwender müssen jederzeit die Kontrolle über ihre Schlüssel haben (Bring and Hold Your Own Key), um sicherzustellen, dass nur sie die Enklaven entschlüsseln können. Technologisch aufsetzend auf einem virtuellen Hardware-Security-Modul (vHSM) bietet enclaive mit Vault genau dieses eigenständige Key Management – auch in Hyperscaler-Umgebungen.

Nitride

Workloads erhalten mit Nitride eindeutige Identitäten und Berechtigungen, sodass nur autorisierte Nutzer und geprüfte Workloads Zugriff auf die Enklaven haben. Über die kryptografischen Zertifikate (Attestation) wird zudem sichergestellt, dass diese nur mit vertrauenswürdigen Komponenten booten. Nitride ermöglicht so den technischen Nachweis – etwa für Audits oder Compliance-Vorgaben –, dass Workloads vertraulich laufen und die Hardware nicht manipuliert wurde.

Ihre Vorteile mit enclaive

3D-Verschlüsselung
Daten sind in allen drei Dimensionen (at rest, in transit und in use) in vertraulichen, isolierten Ausführungsumgebungen verschlüsselt. Nur autorisierte User haben Zugriff – die perfekte Ergänzung für Zero-Trust-Architekturen.

Einfache Integration
Unsere Enklaven sind ohne Codeänderungen einsetzbar und fügen sich nahtlos in bestehende Infrastrukturen ein. So erreichen Sie ein Höchstmaß an Sicherheit bei minimalem Implementierungsaufwand.

Post-Quanten-Sicherheit
Quantencomputer stellen eine Bedrohung für derzeit übliche Verschlüsselungen dar. enclaive verfolgt bereits jetzt eine Post-Quanten-Strategie, damit die Verschlüsselung auch Quantencomputern standhält und die zunehmenden „Store now, decrypt later"-Angriffe wirkungslos sind.

Confidential AI
Unsere GenAI-Firewall Garnet schützt sensible Datenbestände bei der KI-Nutzung durch Vorfilterung und Pseudonymisierung. So können Unternehmen und Organisationen Daten analysieren, Entscheidungen beschleunigen und Innovationen vorantreiben, ohne Risiken bei Vertraulichkeit oder Datenhoheit einzugehen.

Minimaler Computing-Overhead
Unsere Verschlüsselung erhöht den Rechenaufwand nur um etwa 3 Prozent. Sie müssen sich also nicht zwischen der Sicherheit und der stabilen Performance Ihrer Workloads entscheiden.

Datenschutz & Compliance
enclaive erfüllt die strengen Anforderungen von DSGVO, DORA, IT-Grundschutz, ISO 27001, TISAX und vielen mehr – und hilft Organisationen so dabei, lückenlose Compliance sicherzustellen.

Use Cases

- **Vertrauliche Verarbeitung großer Datenmengen:** Unternehmen und öffentliche Einrichtungen können ihre Vielzahl unterschiedlicher Daten und Anwendungen nun in ebenso performanten wie hochsicheren Cloud-Umgebungen verarbeiten und betreiben.
- **Souveränität in der Cloud:** Durch Bring and Hold Your Own Key (BYOK/HYOK) bleiben die Schlüssel und damit die Kontrolle über die Daten vollständig beim Anwender, unabhängig von Cloud-Anbieter oder Standort.
- **Erfüllen strenger Datenschutz- und Compliance-Anforderungen:** Confidential Computing bietet die technische Grundlage, um regulatorische Vorgaben wie DSGVO, NIS2 oder branchenspezifische Compliance-Anforderungen sicher und dank Attestation nachweisbar zu erfüllen.
- **Sichere Datenräume und Kollaboration:** In Netzwerken, in denen mehrere Akteure sensible Informationen austauschen, schafft die durchgängige 3D-Verschlüsselung das nötige Vertrauen, ohne die jeweilige Datenhoheit zu kompromittieren.
- **Multi-Cloud-Strategien ohne Vendor Lock-in:** Workloads lassen sich sicher über mehrere Cloud-Anbieter verteilen. Dies ermöglicht volle Flexibilität und Ausfallsicherheit ohne die Gefahr der Anbieterabhängigkeit.
- **Sichere Cloud-Migration kritischer Workloads:** Vertrauliche Anwendungen können ohne Code-Anpassungen in Hyperscaler-Clouds verschoben werden. Die Daten bleiben dabei durchgängig geschützt.

Fazit

Confidential Computing von enclaive schlägt die technologische Brücke zwischen der Rechenleistung der Hyperscaler und den hohen Datenschutz- und Souveränitäts-Anforderungen europäischer und deutscher Organisationen. Durch die 3D-Verschlüsselung sensibler Daten, ein souveränes Schlüsselmanagement und nachweisbare Datenintegrität (Attestation) entsteht ein neues Level von absoluter Vertraulichkeit in der Cloud. So können Organisationen die großen US-Cloud-Anbieter nutzen, ohne die Kontrolle über ihre Daten zu gefährden – und damit ihre Cloud-Transformation sicher, souverän und Compliance-konform gestalten.

Starten Sie jetzt souverän in die Cloud

Kontaktieren Sie uns für eine persönliche Beratung und überzeugen Sie sich selbst von der Sicherheit unserer Enklaven.

Hier geht's zur kostenlosen Demo:
https://www.enclaive.io/de/get-a-free-demo-with-enclaive

Oder schreiben Sie uns eine Mail an
contact@enclaive.io