enclaive

Solution Brief

enclaive Multi-Cloud Platform

Die einzige Plattform für Confidential Computing Environments

Executive Summary

Unternehmen stehen vor der Herausforderung, die Skalierbarkeit und Flexibilität der Cloud zu nutzen, ohne sich von einem Provider abhängig zu machen oder ihre Datensicherheit zu gefährden. So bleiben Daten in klassischen Architekturen während der Verarbeitung unverschlüsselt, was Sicherheit, Vertraulichkeit und Souveränität beeinträchtigt.

Hier setzt Confidential Computing als technologischer Paradigmenwechsel an: Schützenswerte Assets wie Daten, Code und KI-Modelle sind in hardware-basierten Enklaven isoliert, sodass Infrastruktur-Betreiber keinen Einblick in die Applikations- und Business-Logik des Nutzers erhalten. Die enclaive Multi-Cloud Platform (eMCP) macht diese hochkomplexe Technologie erstmals für Unternehmen jeder Größe einfach nutzbar. Hochsichere Confidential Environments lassen sich über mehrere Cloud-Provider hinweg mit wenigen Klicks einrichten, ohne dass spezielles Knowhow oder zeitaufwendige Infrastruktur-Änderungen erforderlich sind.

Die eMCP zeichnet sich durch ihre Technologieoffenheit und radikale Vereinfachung aus. Als einzige Plattform bietet sie eine cloud-übergreifende Orchestrierung von Confidential Multi-Cloud-Ressourcen und „hebt“ Container oder VMs vollautomatisiert in sichere Enklaven – ganz ohne Code-Änderungen. Die integrierte Attestierung der Workloads liefert auf Basis von kryptografischen Nachweisen zudem Compliance-Belege „out of the box“ für sämtliche wichtigen Regelwerke.

In diesem Solution Brief erfahren Sie im Detail, welche Features die eMCP bietet und welche konkreten Ressourcen – von Confidential Kubernetes-Clustern bis hin zu virtuellen HSMs – Sie damit bereitstellen können. Wir beleuchten die spezifischen Vorteile für verschiedene Rollen wie CISOs, Cloud-Architekten und Entwickler und zeigen anhand praxisnaher Use Cases (z. B. Confidential AI), wie Sie mit der eMCP maximale Datensouveränität sicherstellen.

enclaive

Gartner zählt Confidential Computing zu den

Top 10 Strategic Technology Trends 2026

Von offizieller Seite als Technologiebaustein empfohlen (BSI C5, gematik, DORA §9)

~50 %

CAGR für den Confidential-Computing-Markt in den nächsten 5 bis 10 Jahren

Lediglich

2-3 %

zusätzliche Rechenleistung für 3D-Verschlüsselung

Einleitung

Unternehmen und öffentliche Einrichtungen verlagern ihre Workloads zunehmend in die Cloud, um von attraktiven Skalierungs- und Kostenvorteilen zu profitieren. Wer allerdings sämtliche Daten bei einem Cloud-Anbieter speichert, macht sich abhängig und verliert die Kontrolle über Daten, Code und KI-Modelle.

Unternehmen stehen bei der Nutzung von Cloud-Diensten zudem vor einem grundlegenden Sicherheits-Dilemma: Herkömmliche Schutzkonzepte verschlüsseln Daten zwar im Ruhezustand (at rest) und bei der Übertragung (in transit), nicht jedoch bei der Verarbeitung (in use). Die Folge: Administratoren der Cloud-Provider, kompromittierte Hypervisoren oder Hacker mit Host-Zugriff könnten die Daten einsehen – eine gravierende Sicherheitslücke sowie ein echtes Souveränitäts- und Compliance-Risiko.

Der Paradigmenwechsel: Confidential Computing mit der eMCP

Confidential Computing schließt diese Sicherheitslücke. Es verlagert das Vertrauen von der Software- auf die Hardwareebene (Chip-Level). Durch den Einsatz sogenannter Trusted Execution Environments (TEEs) – sicheren Enklaven direkt auf der CPU oder GPU – bleiben Workloads und Daten selbst während der Verarbeitung kryptografisch isoliert. Weder der Cloud-Anbieter noch interne oder externe Angreifer können auf den Arbeitsspeicher zugreifen.

Doch in der Praxis ist Confidential Computing komplex. Viele Cloud-Anbieter bieten zwar die nötigen Hardware-Voraussetzungen für Confidential Computing, setzen jedoch auf unterschiedliche Chip-Technologien. Anwendungen müssten angepasst, Betriebsprozesse neu gedacht und Spezialwissen aufgebaut werden – insbesondere in Multi-Cloud-Umgebungen. Genau hier setzt die enclaive Multi-Cloud Platform (eMCP) an.

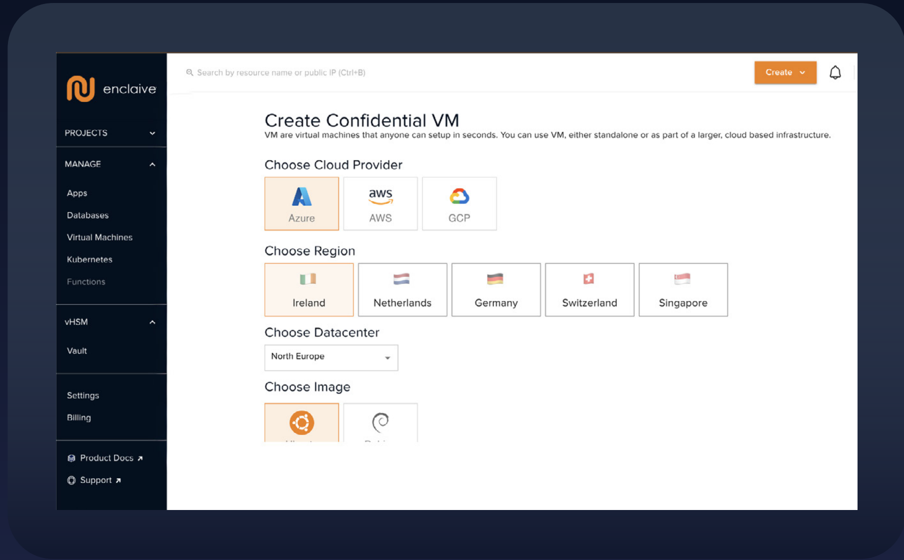
Die eMCP ist die erste Plattform, die Unternehmen dazu befähigt, vollständig isolierte, hardware-basierte Confidential Environments über mehrere Cloud-Anbieter hinweg zu generieren, zu orchestrieren und zu betreiben. Sie verbindet Sicherheit auf Chip-Level, Cloud-Agnostik und automatisierte Compliance zu einer Lösung, die es so bisher nicht gab – und das alles auch Post-Quantum-sicher und Made in Germany.

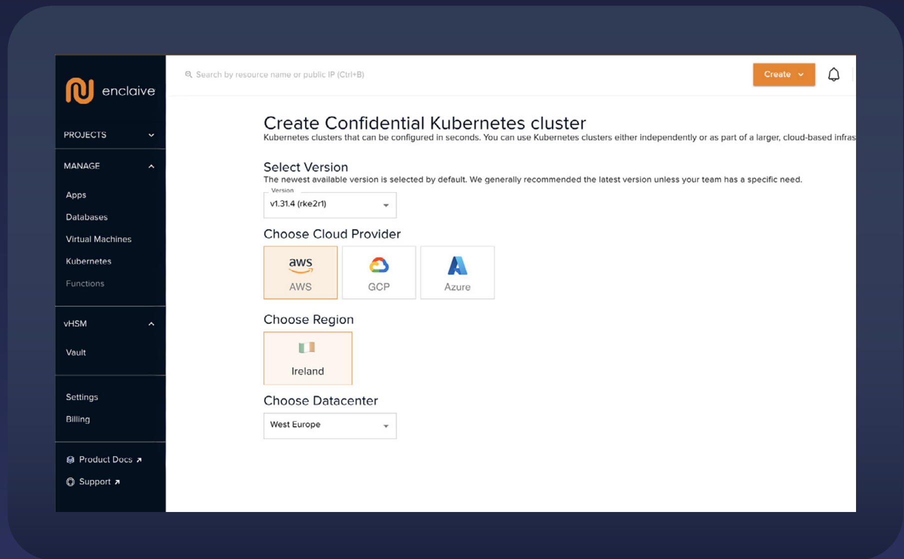
enclaive

Die eMCP im Detail

Die eMCP ist Ihre All-in-One-Lösung, um vertrauliche Ausführungsumgebungen für KI-Modelle, Datenbanken, Anwendungen und Microservices mit wenigen Klicks in der Multi-Cloud einzurichten und zu verwalten. Die Plattform bietet Ihnen über das zentrale Dashboard folgende Einsatzmöglichkeiten:

- **Confidential Virtual Machines (Buckypaper):** Workloads werden in isolierten Enklaven ausgeführt. Der Quellcode bleibt unverändert, die Sicherheitsarchitektur wird im Hintergrund ergänzt.
- **Confidential Kubernetes-Cluster (Dyneemes):** Containerisierte Workloads laufen in einer Zero-Trust-Infrastruktur, bei der sowohl Control Plane als auch Node Pools oder einzelne Pods geschützt sind.
- **Key-Management-as-a-Service (Vault):** Schlüssel, Identitäten und Secrets werden in einer geschützten Umgebung verwaltet – ohne dedizierte physische HSM-Infrastruktur, aber dank enclaives virtuellem HSM (vHSM) mit Kryptografie auf Hardware-Niveau.
- **Attestation-as-a-Service (Nitride):** Enklaven können kryptografisch belegen, dass sie auf vertrauenswürdiger Hardware ausgeführt werden. Das schafft technische Beweisbarkeit für Audits und Compliance.
- **Multi-Cloud zentral steuern:** Ressourcen, Policies und Secrets werden cloudübergreifend verwaltet – konsistent und ohne providerabhängige Insellösungen.





enclaive

Warum Sie auf die eMCP setzen sollten

Im stark wachsenden Markt für Confidential Computing setzt die eMCP neue Standards. Andere Anbieter bieten lediglich isolierte Lösungen für spezifische Cloud-Provider und Hardware-Typen, oder setzen entsprechendes Knowhow und Code-Änderungen bei der Implementierung voraus. Genau hier positioniert sich die eMCP als einzigartige Lösung – nicht nur im Vergleich zu klassischen Sicherheitsansätzen, sondern gerade innerhalb des Confidential-Computing-Marktes.

Was nur die eMCP Ihnen bietet:

Cloud-übergreifende Orchestrierung

Die eMCP ist die einzige Plattform, die eine einheitliche Control Plane für Confidential-Computing-Umgebungen über heterogene Multi-Cloud-Umgebungen hinweg bereitstellt. Sie steuern alles zentral, unabhängig vom Cloud-Anbieter oder der Hardware.

Automatisierte Provisionierung und Easy Deployment

Confidential Environments sind dank policy-gesteuerter Bereitstellung und automatisierter Attestation innerhalb weniger Sekunden eingerichtet – und Zero Trust by Design. Ihre Workloads sind im Handumdrehen „confidential".

Technologieoffenheit

Die eMCP nutzt nativ verfügbare TEE-Technologien (Intel SGX, AMD SEV-SNP, ARM CCA, NVIDIA Hopper/Blackwell) und abstrahiert diese zu einer einheitlichen Sicherheitsarchitektur. Sie bleiben unabhängig vom Hardware-Hersteller und Cloud-Provider und der eingesetzten Hardware-Technologie.

Out-of-the-box Compliance

Die eMCP unterstützt Sie aktiv bei der Erfüllung strengster Regelwerke (DSGVO, NIS2, DORA, TISAX u.v.m.).
Über Remote Attestation samt praktischem Berichts-Feature lässt sich technisch nachweisen, dass Ihre Daten jederzeit in einer verifizierten Hardware-Enklave geschützt sind.

Mit der eMCP gewinnen Sie an Sicherheit und Souveränität – und eliminieren gleichzeitig die Komplexität beim Cloud-Management, der Implementierung und bei regulatorischen Anforderungen.

enclaive

Ihre Vorteile

Die Nutzung der eMCP bietet Ihnen konkrete technische und wirtschaftliche Vorteile:

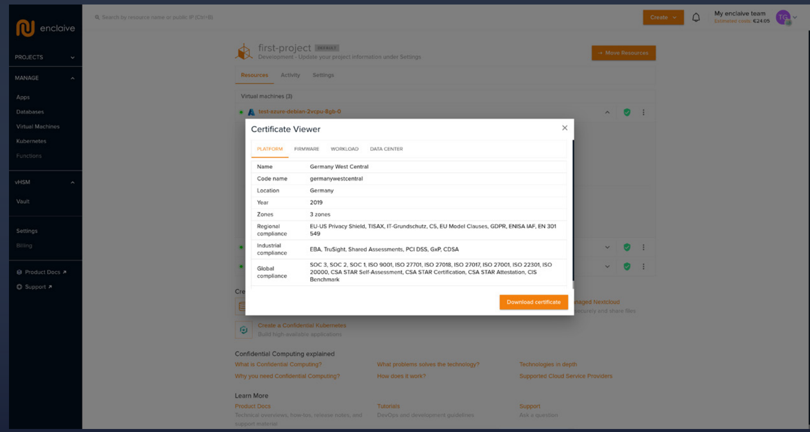
- **Nahtlose Integration:** Open Source und standardisierte APIs (PKCS#11, KMIP und REST) ermöglichen die reibungslose Einbindung in bestehende Infrastruktur- und Security-Stacks.
- **Keine Code-Änderungen:** Bestehende Anwendungen laufen unverändert in vertraulichen Ausführungsumgebungen.
- **Minimaler Performance-Overhead:** Die Verschlüsselung mit enclaive verursacht einen zusätzlichen Rechenaufwand von nur 2-3 %.
- **Multi-Mandantenfähigkeit:** Ideal für komplexe Unternehmensstrukturen oder Managed Services. Jeder Tenant ist logisch isoliert.
- **Kostenersparnis:** Ersetzen Sie teure On-Prem-Hardware durch hochsichere Cloud-Strukturen und steuern Sie Ihre Ressourcennutzung dabei zentral.
- **Schutz in Shared Infrastructure:** Isolation nicht durch den Hypervisor, sondern durch Enklaven – Ihre Daten bleiben selbst vor anderen RZ-Kunden und dem Provider geschützt.
- **Anbieter-Unabhängigkeit:** Vermeiden Sie Vendor Lock-in. Managen Sie Ihre Workloads über private, öffentliche und hybride Cloud-Umgebungen verschiedener Anbieter hinweg.
- **Bring Your Own Subscription (BYOS):** Nutzen Sie Ihre bestehenden Cloud-Tarife und Identitätsmanagementsysteme einfach weiter.
- **Compliance-Booster:** Die eMCP liefert die notwendigen technischen Nachweise für eine Vielzahl an Regelwerken und erleichtert das Reporting erheblich.
- **Post-Quanten-Sicherheit:** Mit der eMCP und Verschlüsselung von enclaive setzen Sie Ihre Post-Quanten-Transformation spielend leicht in die Tat um.

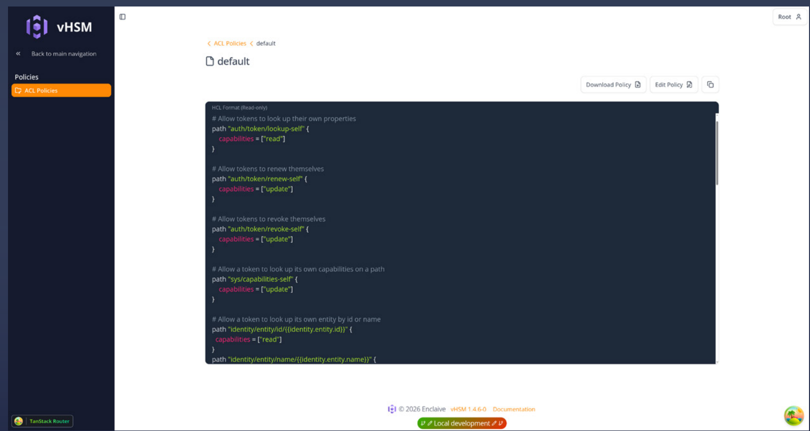
enclaive

Usability

Anstatt mehrere Management-Konsolen verschiedener Provider verwalten zu müssen und den Überblick zu verlieren, zentralisiert eMCP den Betrieb:

- **Zentrales Kontrollpanel:** Sie verwalten Ihre gesamte Cloud-Ressourcen-Landschaft providerübergreifend über ein einziges Dashboard.
- **Bereitstellung von Multi-Cloud-Ressourcen:** Stellen Sie VMs, Kubernetes-Cluster oder andere Ressourcen direkt und mit wenigen Klicks über die eMCP bereit.
- **Benutzer- und Zugriffsmanagement:** Legen Sie Berechtigungen und Zugriffsrollen mit wenigen Klicks über verschiedene Clouds hinweg fest.
- **Sicherheitskonfigurationen:** Konfigurieren Sie Sicherheitseinstellungen für alle Confidential-Computing-Umgebungen zentral an einem Ort, inklusive Firewall- und Zugriffsregeln.
- **Automatisierte Workflows:** Automatisieren Sie redundante Aufgaben wie Skalierung und Ressourcenverteilung. Auch die Verifizierung der Enklaven-Integrität läuft automatisch über den Remote Attestation Service.
- **Echtzeit-Monitoring:** Behalten Sie durch unsere Monitoring-Tools und benutzerdefinierten Warnmeldungen Ihre Ressourcennutzung, Performance und Sicherheit stets im Blick.
- **Berichte und Analysen:** Erstellen Sie detaillierte Berichte zu Ressourcennutzung, Kosten und Leistungsmetriken.





enclaive

Wie die eMCP Sie konkret unterstützt

Die Plattform verbindet strategische Sicherheitsanforderungen mit operativer Umsetzbarkeit und richtet sich damit gleichermaßen an Entscheider wie an technische Umsetzungsteams.

CISOs

Für Sicherheitsverantwortliche bietet die eMCP technische Sicherheitsgarantien statt vertraglicher Zusicherungen – und macht Vertraulichkeit überprüfbar.

- **Risikominimierung:** Selbst bei kompromittierter Infrastruktur bleiben Daten jederzeit verschlüsselt
- **Nachweisbare Compliance:** Kryptografische Attestation ermöglicht revisionssichere Audit-Trails und regulatorisch belastbare Belege
- **Strategische Transparenz:** Zentrale Sicht auf alle Workloads erlaubt fundierte Entscheidungen und effiziente Steuerung der Sicherheitsarchitektur

Cloud Architects

Die eMCP reduziert die Komplexität verteilter Multi-Cloud-Architekturen und schafft ein konsistentes Sicherheits- und Betriebsmodell.

- **Zentrales Architekturmodell:** Einheitliche Plattform statt Cloud-Silos
- **Schnellere Implementierung:** Automatisierte Attestation & Provisionierung
- **Multi-Cloud-Flexibilität:** Keine Sicherheitsbrüche oder Lock-in-Risiken

Entwickler

Bieten Sie Ihren Developern Sicherheit, die Entwicklungsprozesse nicht verlangsamt.

- **Kein TEE-Knowhow erforderlich:** Bestehende Workloads laufen ohne Refactoring
- **IP-Schutz by Design:** Modelle, Daten und Geschäftslogik bleiben vertraulich
- **Einfache Integration in CI/CD:** Sicherheitsmechanismen greifen ohne Prozessänderung

enclaive

Use Cases

Confidential Computing entfaltet seinen Mehrwert überall dort, wo sensible Daten verarbeitet, regulatorische Anforderungen erfüllt oder digitale Souveränität gewährleistet werden muss.

- **Geschützte Lift-and-Shift-Migrationen:** Bringen Sie Ihre On-Premises-Workloads in die Cloud. Enklaven dienen als geschützte Ausführungsumgebungen und lassen sich bei Bedarf wie die bestehende Umgebung konfigurieren.
- **Regulierte Industrien:** Verarbeiten Sie hochsensible Daten in der Cloud, wo Daten unter keinen Umständen kompromittiert werden dürfen – etwa in der Finanzbranche, im Gesundheitswesen oder in der öffentlichen Verwaltung.
- **Confidential AI:** Schützen Sie KI-Modelle, sensible Trainingsdaten und Inferenzprozesse vor Diebstahl und Manipulation in sicheren Enklaven. Sichere Innovation statt Kontrollverlust und Datenabfluss.
- **Confidential Data Spaces:** Schaffen Sie souveräne, vertrauenswürdige Datenräume, in denen Mitarbeiter, Partner oder Dritte Daten austauschen oder gemeinsam auswerten und bearbeiten können, ohne dass eine Partei (oder der Host) die Rohdaten der anderen einsehen kann.
- **Confidential SaaS:** SaaS-Anbieter können die eMCP nutzen, um ihren Endkunden vertraglich und technisch nachweisbare Datenisolation zu garantieren – und sich so von der Konkurrenz abheben.

Fazit

Lückenlose Sicherheit, einfach umgesetzt

Die Anforderungen an Cloud-Sicherheit haben sich grundlegend verändert. Daten(banken), Anwendungen und KI-Workloads müssen auch während der Verarbeitung verschlüsselt sein, um Vertraulichkeit und Souveränität sicherzustellen. Confidential Computing kann dies leisten, doch neue Sicherheitsansätze dürfen nicht zu zusätzlicher Komplexität, höheren Betriebskosten oder technologischen Abhängigkeiten führen.

Die enclaive Multi-Cloud Platform löst diese Herausforderungen, indem sie die hardwarebasierte Vertraulichkeit mit einem cloudübergreifenden, einfach zu bedienenden Betriebsmodell verbindet. Unternehmen erhalten so eine Plattform, die Sicherheit, Compliance, Performance und Usability in Einklang bringt. Die eMCP ist damit nicht nur eine Erweiterung bestehender Sicherheitsarchitekturen – sie steht für einen Paradigmenwechsel in der Cloud-Sicherheit und bildet die Grundlage für eine souveräne, zukunftssichere Multi-Cloud-Strategie.

enclaive

Sichern Sie jetzt Ihre Cloud-Workloads mit Confidential Computing

Die enclaive Multi-Cloud Platform ist die Antwort auf die Herausforderungen moderner Datensouveränität. Schützen Sie Ihre sensiblen Workloads mit maximaler Sicherheit und Vertraulichkeit – ohne dabei Ihre Infrastruktur neu denken zu müssen.

- Vereinbaren Sie eine Demo
- Sprechen Sie mit unseren Experten
- Probieren Sie es einfach hier selbst aus
- Eine detaillierte Anleitung finden Sie hier

Erleben Sie, wie einfach Confidential Computing sein kann – mit der eMCP, Ihrem Schlüssel zur souveränen Multi-Cloud.

Kontakt
sales@enclaive.io

Mehr Informationen unter
enclaive.io