enclaive

Solution Brief

enclaive Managed Kubernetes

Managed Confidential Containers als USP

enclaive

Executive Summary

Managed Kubernetes ist ein wichtiger Wachstumstreiber im Portfolio vieler Managed Service Provider – wird aber zunehmend zur austauschbaren Standardleistung. Gleichzeitig verlagern Unternehmen immer mehr sensible Workloads in Container-Plattformen – und stoßen dabei an die Grenzen klassischer Security- und Trust-Modelle. Gerade in regulierten Branchen stellt sich also die Frage, wie Unternehmen von Kubernetes als Managed Service profitieren können, ohne dem Hosting-Partner uneingeschränkten Zugriff auf Daten, Code und Schlüssel zu gewähren.

enclaive Dyneemes beantwortet diese Frage mit einem grundlegend neuen Ansatz: Durch den Einsatz von Confidential Computing werden Kubernetes-Workloads in hardware-isolierten Enklaven ausgeführt und sind auf diese Weise selbst vor privilegierten Kubernetes-Administratoren, Hypervisoren und Cloud-Betreibern geschützt. Sicherheit ist damit kein organisatorisches Versprechen mehr, sondern wird technisch erzwungen und überprüfbar gemacht.

Ihnen als MSP eröffnet enclaive Dyneemes die Möglichkeit, Ihr Managed Kubernetes-Angebot um eine zusätzliche Security- und Vertrauensebene zu erweitern – ohne dedizierte Hardware, ohne separate Cluster und ohne Abstriche bei Skalierbarkeit oder Wirtschaftlichkeit, und ohne ihre Kubernetes-Distribution, Partnerschaft und Service Level Agreements zu wechseln. Ihre Kunden behalten so jederzeit die Hoheit über ihre Daten und Schlüssel, während Sie als Service Provider den Betrieb, die Verfügbarkeit und den Lifecycle der Plattform wie gewohnt verantworten.

Confidential Kubernetes wird so immer mehr zum strategischen Differenzierungsmerkmal: MSPs erschließen sich attraktive neue Kundensegmente, erhöhen Margen durch Premium-Services und positionieren sich als Anbieter souveräner und zukunftssicherer Cloud- und Container-Plattformen.

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

enclaive

Herausforderungen

Kubernetes hat sich als Standardplattform für die moderne Anwendungsentwicklung etabliert – und immer mehr Unternehmen entscheiden sich dafür, den Betrieb, die Skalierung und die Wartung ihrer DevOps-Umgebungen im Rahmen von Managed Kubernetes Services in die Hände spezialisierter Managed Service Provider (MSPs) zu legen. Für Sie als Service Provider ist das Wachstumspotenzial in diesem Bereich also hoch – aber auch der Wettbewerbsdruck steigt: Managed Kubernetes wird zunehmend zur Commodity.

Gleichzeitig verlagern Ihre Kunden immer öfter auch sensible Workloads in Kubernetes-Umgebungen – von personenbezogenen Daten über geistiges Eigentum bis hin zu KI-Modellen und geschäftskritischen Prozessen. Und genau in diesem Szenario stoßen klassische Managed-Kubernetes-Ansätze an ihre Grenzen.

Sicherheit und Vertrauen als Wachstumsbremse

Wer sich heute entschließt, seine Kubernetes-Umgebung künftig im Rahmen von Managed Services zu beziehen, nimmt damit implizit immer auch in Kauf, dass der Betreiber zumindest theoretisch auf seine Nodes, seine Container, seinen Speicher und seine Secrets zugreifen könnte – selbst wenn er es organisatorisch nicht soll.

Für viele Kunden ist ein solches Modell daher in mehr als einer Hinsicht nicht akzeptabel:

- Es gibt keine technische Trennung zwischen der Betreiber-Rolle und den sensiblen Workloads des Kunden
- Daten sind während der Verarbeitung („in use“) nicht zuverlässig vor Zugriffen Dritter geschützt
- Gerade in regulierten Branchen ist eine solche Lösung nicht Compliance-konform
- Je nach Modell und Umgebung begeben sich die Kunden in die Abhängigkeit von Hyperscalern – und müssen sich auf deren Sicherheitsmodelle verlassen

Die zentrale Frage lautet daher immer häufiger: **Wie können wir Kubernetes als Managed Service nutzen, ohne dem Betreiber unsere Daten, unseren Code und unsere Schlüssel anvertrauen zu müssen?** Doch leider geben klassische Sicherheitsmodelle darauf keine überzeugende Antwort.

enclaive

Ihre Chance als MSP: Definieren Sie Managed Kubernetes neu!

Für Sie als MSP ergibt sich daraus eine wertvolle strategische Gelegenheit: Wenn es Ihnen gelingt, Managed Kubernetes Services mit lückenlos nachweisbarer Vertraulichkeit und zuverlässigem Schutz von Data in Use anzubieten, können Sie sich klar vom Wettbewerb absetzen – und so neue, margenstarke Kundensegmente erschließen.

Die technische Grundlage dafür ist Confidential Computing, das sensible Workloads selbst vor privilegierten Kubernetes-Administratoren, Hypervisoren und Cloud-Betreibern schützt. Der Schutz der Assets wird dabei nicht mehr zugesichert, sondern technisch erzwungen und auditierbar dokumentiert.

enclaive

Die Lösung

Mit Dyneemes bietet enclaive eine speziell für Managed-Service-Szenarien entwickelte Plattform für Confidential Kubernetes. Dabei erweitert Dyneemes bestehende Kubernetes-Umgebungen um eine zusätzliche Sicherheitsschicht, die Container-Workloads in hardware-isolierten Enklaven ausführt.

Dyneemes basiert auf der marktführenden Confidential-Computing-Technologie von enclaive, die sensible Daten während der Verarbeitung in geschützten Enklaven („Tresore“) isoliert, sodass ausschließlich autorisierte Anwendungen darauf zugreifen können. Jede Enklave bildet eine eigene Vertrauensdomäne, deren Integrität über Secure Boot und Remote Attestation kryptografisch belegbar ist (enclaive Nitride). Erst nach erfolgreicher Validierung werden Schlüssel und Funktionen freigegeben. Damit wird Vertrauen nicht angenommen, sondern nachweisbar – ein zentraler Baustein für moderne Zero-Trust-Architekturen und Compliance-Audits.

Die Cloud-Computing-Architektur macht auch bei der Bereitstellung von Confidential Kubernetes den entscheidenden Unterschied: Zwar betreiben Sie als MSP auch in diesem Setup weiterhin die Kubernetes-Plattform – Sie erhalten aber keinen Zugriff („kubectl exec“) mehr auf die geschützten Workloads, Daten oder Schlüssel Ihrer Kunden. Damit wird Managed Kubernetes erstmals auch für hochsensible und regulierte Anwendungsfälle praktikabel.

Confidential Computing – neuartige Verschlüsselung und Geschäftsfeld für Service Provider

Klassische Verschlüsselung schützt Daten im Ruhezustand und bei der Übertragung, aber nicht während der Verarbeitung. Confidential Computing schließt diese Lücke, indem sensible Workloads in hardwarebasierten, isolierten Trusted Execution Environments (TEEs) – auch Enklaven genannt – direkt auf der CPU verschlüsselt sind. Daten sind so auch „in use“ geschützt und selbst für privilegierte Insider sowie Cloud- und Service Provider nicht zugänglich.

Als einer der wachstumsstärksten Security-Märkte ist Confidential Computing für Service Provider besonders interessant: Der CAGR für die nächsten 5-10 Jahre liegt bei etwa 50 %. Gartner prognostiziert, dass bis 2029 75 % aller Workloads in der Public Cloud auch „in use“ geschützt sein werden. Die Technologie wird zudem vom BSI im aktuellen C5-Katalog ausdrücklich für sensible Cloud-Workloads empfohlen.

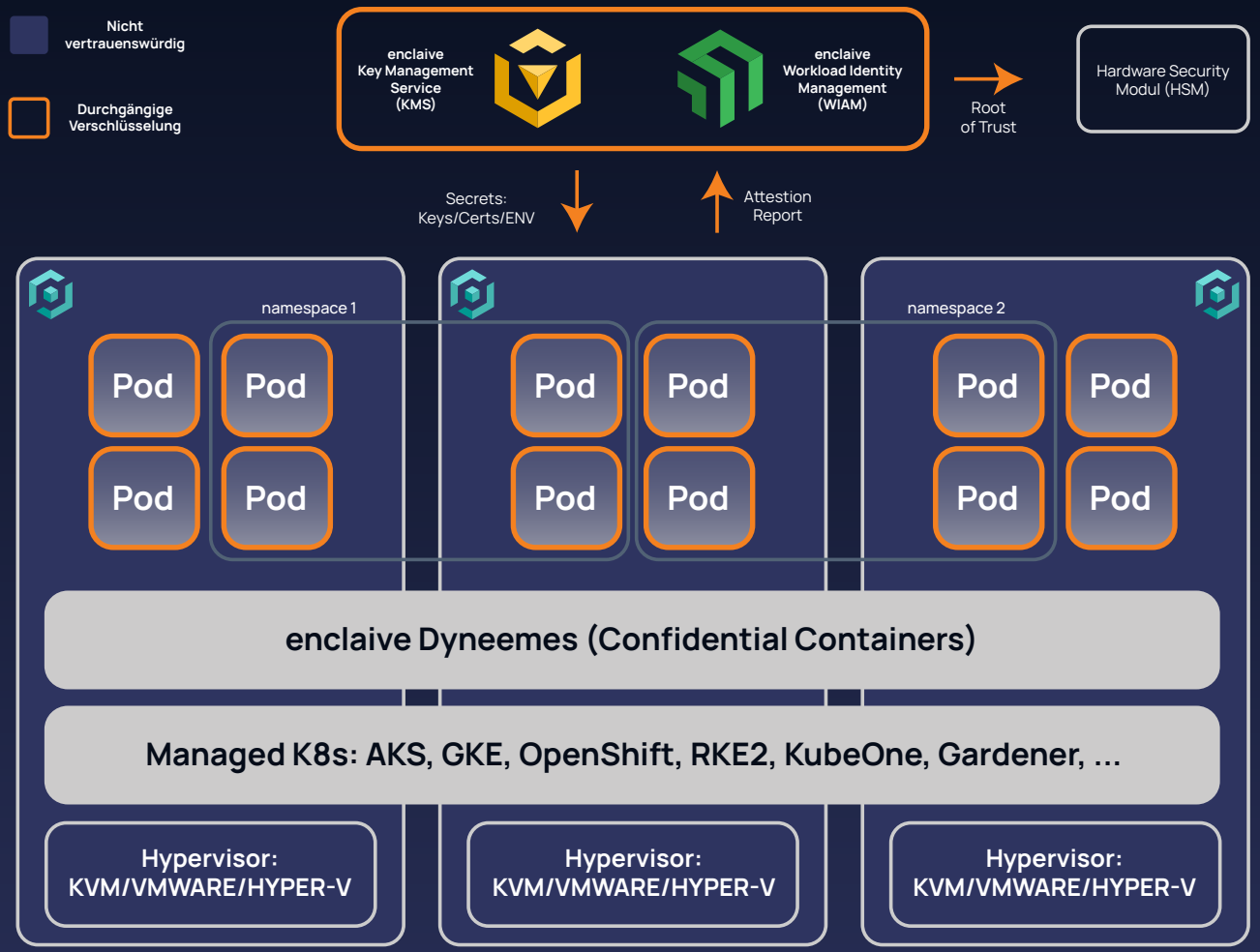
Der zusätzliche Rechenaufwand für Confidential Computing liegt in der Regel im niedrigen einstelligen Prozentbereich, ist also vernachlässigbar. Technische Voraussetzungen: Intel TDX / AMD SEV-SNP und Linux 6.11.

enclaive

So funktioniert enclaive Dyneemes

Die technische Grundlage von Dyneemes ist enclaive Buckypaper, unsere Confidential VM, die Ihnen als geschützte Laufzeitumgebung dient. Dyneemes ermöglicht es Ihnen, innerhalb dieser Confidential VM dedizierte Kubernetes-Pods bereitzustellen und zu orchestrieren, die vollständig von der Umgebung des Betreibers isoliert sind.

Da Dyneemes mit allen gängigen Kubernetes-Distributionen kompatibel ist und nur einen minimalen Performance-Overhead von 2 bis 8 Prozent erfordert, lässt sich die Confidential Kubernetes-Umgebung erfahrungsgemäß einfach und schnell implementieren.



enclaive

Warum diese Architektur – und keine andere?

Isolierte Pods statt isolierter Nodes

Im Gegensatz zu anderen Confidential-Computing-Lösungen setzt Dyneemes nicht auf die Isolation ganzer Kubernetes-Nodes, sondern auf isolierte Pods innerhalb einer Confidential VM, was Ihnen und Ihren Kunden eine Reihe von Vorteilen sichert:

- Höchste Sicherheit durch vollständige Kernel- und Hardware-Isolierung auf Pod-Ebene
- Höhere Ressourceneffizienz und bessere Auslastung
- Mandantenfähige Plattform statt Single-Tenant-Inseln
- Eigener Kernel pro Pod verringert die Angriffsfläche
- Nahtlose Integration via CRI für ein Höchstmaß an Zukunftssicherheit schon jetzt auch schon mit Quanten-sichere Ver schlüsselung
- Wirtschaftlich tragfähiges Modell für MSPs

Confidential VM statt klassischer Node-Härtung

Der Einsatz von enclaive Buckypaper als Confidential VM zieht eine klare Sicherheitsgrenze, die unabhängig ist vom zugrunde liegenden Cloud- oder Virtualisierungsstack. Selbst Root-Zugriffe auf den Host oder den Hypervisor ermöglichen keinen Einblick in die geschützten Workloads.

Eigenes Schlüsselmanagement (enclaive Vault)

Die Schlüssel und Secrets verbleiben vollständig unter Kontrolle Ihrer Kunden. Sie als MSP stellen zwar die Plattform bereit, haben jedoch zu keinem Zeitpunkt Zugriff auf kryptografisches Material. Dieses Hold-Your-Own-Key-Prinzip ist für Souveränität, Zero Trust und Compliance von entscheidender Bedeutung.

Schutz des Hosts vor Container-Eskalationen

Confidential Containers isolieren Workloads hardwaregestützt und verschlüsseln deren Speicher im Arbeitsspeicher. Dadurch wird verhindert, dass kompromittierte Container den Host-Kernel angreifen oder auf andere Container zugreifen können – ideal für Managed Service Provider, die Multi-Tenant-Umgebungen sicher betreiben müssen.

Hybrider Betrieb und nahtlose Migration

Bereits vorhandene Kubernetes- oder Container-Cluster können parallel zu Confidential Containers betrieben werden. Workloads lassen sich schrittweise oder individuell zur Laufzeit migrieren, ohne bestehende Services zu unterbrechen – ideal für Managed Service Provider, die flexible Hybrid-Szenarien unterstützen möchten.

enclaive

Confidential Kubernetes als Managed Service

Als cloud-native, Kubernetes-kompatible und Multi-Tenant-fähige Lösung lässt sich Dyneemes ideal als standardisierter Managed Services bereitstellen.

Sie als MSP übernehmen:

- Betrieb, Skalierung und Monitoring der Kubernetes-Plattform
- Lifecycle-Management der Dyneemes-Umgebung
- Integration in bestehende Managed-Kubernetes-Stacks

Ihre Kunden behalten:

- Kontrolle über Daten, Code und Schlüssel
- Nachweisbare Sicherheit durch Remote Attestation
- Freiheit bei Cloud- und Plattformwahl
- Vertraute Umgebung (gleiche APIs, CI/CD-Pipelines, Tools etc.)

Wie Confidential Kubernetes Ihr Business vorantreibt

Zusätzliche Umsatzpotenziale

- Premium-Managed-Kubernetes-Angebote für regulierte Branchen
- Neue Services rund um Compliance, Datenschutz und Souveränität
- Aufwertung bestehender Services, etwa Confidential DevOps-Pipelines

Geringer Betriebsaufwand

- Keine klassischen HSMs oder dedizierten Cluster nötig
- Cloud-native Skalierung und Self-Healing
- Schnelle Provisionierung neuer Kundenumgebungen

Klare Differenzierung

- Schutz von Data in Use – ein Alleinstellungsmerkmal
- Europäische, souveräne Alternative zu Hyperscaler-Ansätzen
- Kein Vendor-Lock-in, keine Abhängigkeit vom Cloud-Provider
- Kompatibel mit existierenden Hyperscalern und CNCF Kubernetes-Distributionen

enclaive

Mehrwerte für Kunden

Audit- und Compliance-Fähigkeit
Kryptografisch belegbare Integrität der Workloads

Zero Trust gegenüber dem Betreiber
Kein implizites Vertrauen in MSP oder Cloud Provider notwendig

Neue Use Cases
Etwa bei der sicheren und Compliance-konformen Einbindung von KI- und ML-Workloads, bei der Verarbeitung sensibler Daten in Shared-Kubernetes-Umgebungen oder bei der sicheren Kollaboration zwischen mehreren Parteien

Vertrauliche Container-Workloads
Schutz von Daten, Code und Modellen auch während der Verarbeitung

Fazit

Managed Kubernetes mit eingebautem Vertrauen

Mit Managed Confidential Kubernetes auf Basis von enclaive Dyneemes überführen Sie bestehende Kubernetes-Umgebungen einfach und schnell in eine zeitgemäße Plattform für hochsensible Workloads, die selbst in streng regulierten Branchen überzeigt – und das ohne Abstriche bei Skalierbarkeit oder Wirtschaftlichkeit.

Sie als MSP erhalten damit ein leistungsfähiges und innovatives Werkzeug, um sich im umkämpften Managed-Kubernetes-Markt klar zu differenzieren, neue Kundengruppen zu erschließen – und Vertrauen technisch durchzusetzen, statt organisatorisch zu versprechen. Confidential Computing wird damit zum strategischen Service-Enabler.

enclaive

Starten Sie jetzt Ihr Confidential-Kubernetes-Business!

Erweitern Sie Ihr Managed-Kubernetes-Portfolio um eine neue Sicherheitsdimension und positionieren Sie sich als Anbieter vertrauenswürdiger Cloud- und Container-Services.

Wie enclaive Sie unterstützt

- Kontinuierliche Weiterentwicklung von Dyneemes
- Workshops und Schulungen
- Aufbau einer Labor-/Testumgebung
- Unterstützung bei Pilotprojekten
- Co-Marketing und Co-Selling
- Attraktive Partner- und Preismodelle

Kontakt
sales@enclaive.io

Mehr Informationen unter
enclaive.io