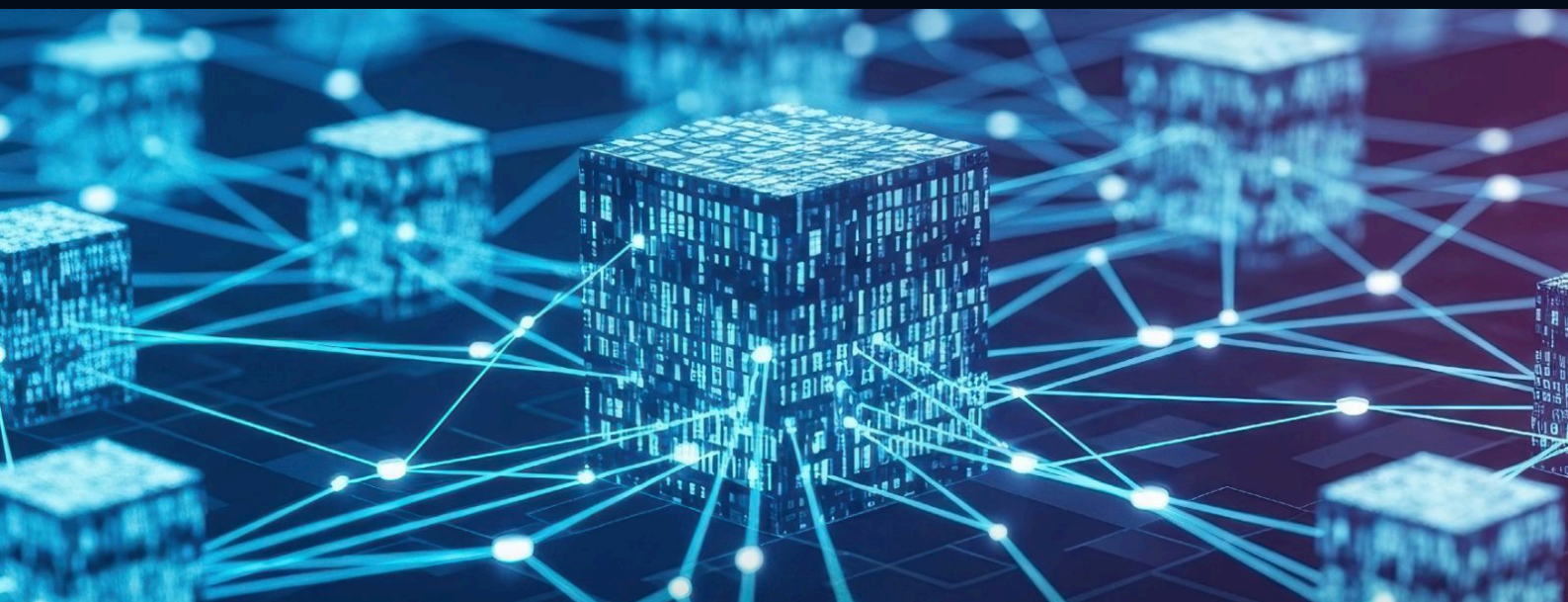
MAKING THE CLOUD THE SAFEST PLACE

enclaive

SOLUTION BRIEF

enclaive Managed Kubernetes

Managed Confidential Containers as Your USP



Executive Summary

Managed Kubernetes is a key growth driver in the portfolios of many Managed Service Providers – yet it is increasingly becoming a commodity. At the same time, companies are migrating more sensitive workloads to container platforms, frequently hitting the limits of traditional security and trust models. Particularly in regulated industries, the question arises: how can companies benefit from Kubernetes as a managed service without granting the hosting partner unrestricted access to data, code, and keys?

enclaive Dyneemes answers this with a fundamentally new approach. By utilizing Confidential Computing, Kubernetes workloads are executed in hardware-isolated enclaves, protecting them even from privileged Kubernetes administrators, hypervisors, and cloud operators. Security is no longer an organisational promise; it is technically enforced and verifiable.

For you as an MSP, enclaive Dyneemes offers the opportunity to enhance your Managed Kubernetes offering with an additional layer of security and trust – without dedicated hardware, without separate clusters, and without compromising scalability or cost-effectiveness. Most importantly, you can do this without changing your Kubernetes distribution, partnerships, or Service Level Agreements. Your customers retain full sovereignty over their data and keys at all times, while you, as the service provider, remain responsible for platform operations, availability, and lifecycle management.

Thus, Confidential Kubernetes is rapidly becoming a strategic differentiator. It enables MSPs to unlock attractive new customer segments, increase margins through premium services, and position themselves as providers of sovereign, future-proof cloud and container platforms.

2–3%

Only 2–3% additional overhead for 3D Encryption

~50%

CAGR for the confidential computing market over the next 5 to 10 years

10 Strategic Technology Trends 2026

Gartner lists Confidential Computing as one of the 10 Strategic Technology Trends 2026

Recommended by official bodies

BSI C5 · gematik · DORA §9

Security and Trust as Growth Inhibitors

Kubernetes has established itself as the standard platform for modern application development. Consequently, more companies are choosing to outsource the operation, scaling, and maintenance of their DevOps environments to specialised Managed Service Providers (MSPs). Therefore, the growth potential for you as a service provider in this sector is high, but so is the level of competition: Managed Kubernetes is increasingly becoming a commodity.

Simultaneously, your customers are migrating sensitive workloads to Kubernetes environments – ranging from personal data and intellectual property to AI models and business-critical processes. It is precisely in these scenarios that traditional Managed Kubernetes approaches reach their limits.

Anyone deciding to obtain their Kubernetes environment via a managed service today implicitly accepts that the operator could – at least theoretically – access their nodes, containers, storage, and secrets, even if organisational policies forbid it.

For many customers, this model is unacceptable for several reasons:

- There is no technical separation between the provider‘s administrative role and the customer‘s sensitive workloads
- Data is not reliably protected from third-party access during processing (“in use”)
- In regulated industries, such solutions often fail to meet compliance requirements
- Depending on the model, customers become dependent on hyperscalers and must rely entirely on their proprietary security models

> **So more and more companies begin to ask: How can we use Kubernetes as a managed service without having to trust the provider with our data, code, and keys?**
>
> Traditional security models, however, do not provide a convincing answer to this.

YOUR OPPORTUNITY AS AN MSP

Redefine Managed Kubernetes!

This increasing demand creates a strategic opportunity for you. By offering Managed Kubernetes services with end-to-end provable confidentiality and reliable protection of “Data in Use,” you can clearly differentiate yourself from the competition and capture high-margin customer segments.

The technical foundation for this is Confidential Computing, which protects sensitive workloads even from privileged Kubernetes admins, hypervisors, and cloud operators. The protection of assets is no longer just “assured”; it is technically enforced and documented in an auditable manner.

THE SOLUTION

enclaive Dyneemes

With **Dyneemes**, enclaive offers a platform for Confidential Kubernetes specifically developed for managed service scenarios. Dyneemes extends existing Kubernetes environments with an additional security layer that executes container workloads in hardware-isolated enclaves.

Dyneemes is based on enclaive's market-leading Confidential Computing technology, which isolates sensitive data during processing in protected enclaves ("vaults"), ensuring that only authorised applications can access them. Each enclave forms its own trust domain, the integrity of which is cryptographically provable via Secure Boot and Remote Attestation (powered by enclaive Nitride). Keys and functions are only released after successful validation. In this model, trust is not assumed, it is proven – forming a cornerstone for modern Zero Trust architectures and compliance audits.

This architecture makes the definitive difference in delivering Confidential Kubernetes: while you as the MSP continue to operate the Kubernetes platform, you no longer have access ("kubectl exec") to your customers' protected workloads, data, or keys. This makes Managed Kubernetes viable for highly sensitive and regulated use cases for the first time.

Confidential Computing: Next-Gen Encryption and a New Revenue Stream for Service Providers

Traditional encryption protects data at rest and in transit, but not during processing. Confidential Computing closes this gap by encrypting sensitive workloads within hardware-based, isolated Trusted Execution Environments (TEEs) – also known as enclaves. This ensures that data remains protected "in use," inaccessible even to privileged insiders, cloud providers, or service providers.

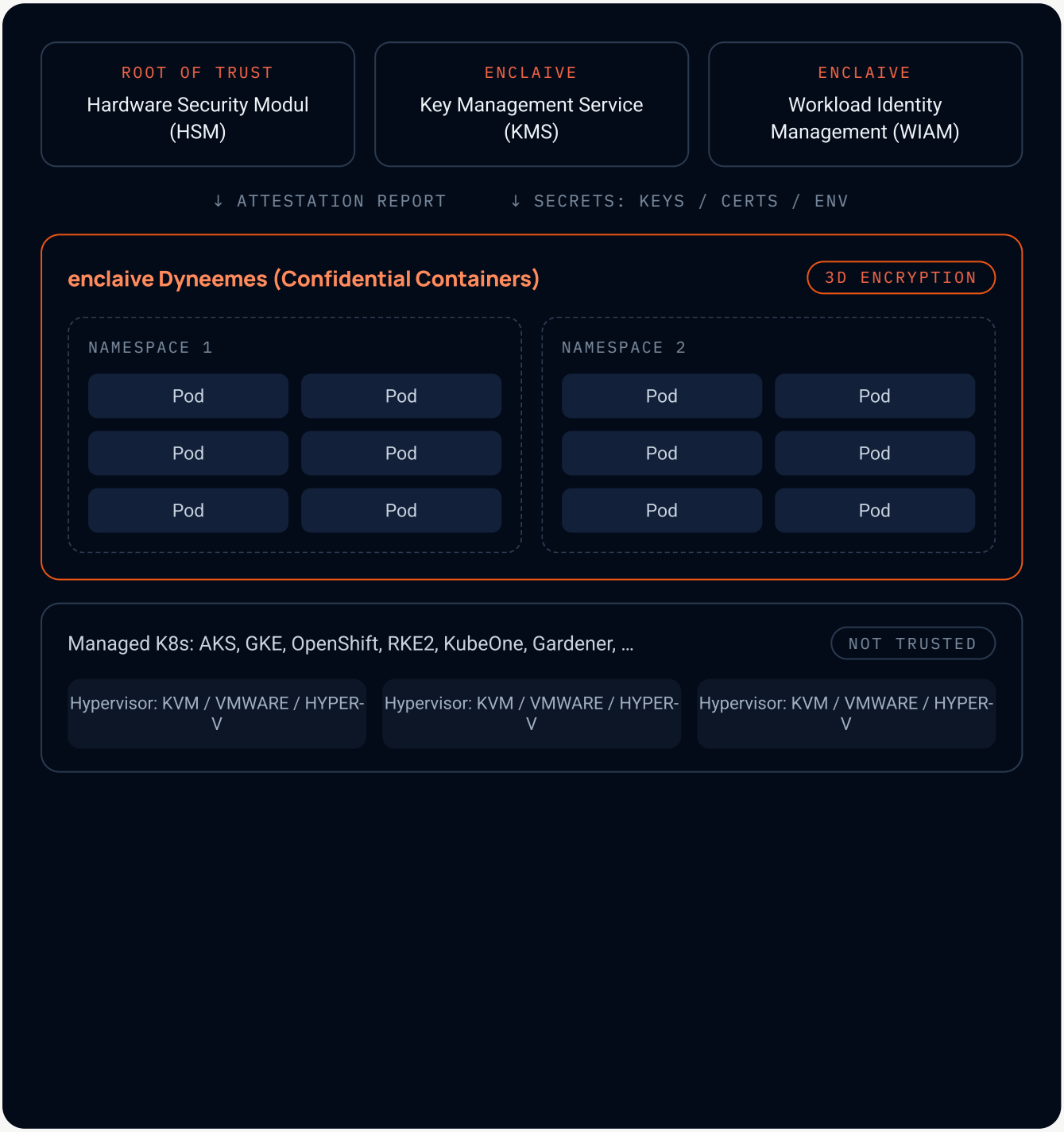
As one of the fastest-growing segments in the security market, Confidential Computing is particularly lucrative for service providers: the CAGR for the next 5–10 years is estimated at approximately 50%. Gartner predicts that by 2029, 75% of all public cloud workloads will be protected "in use." Furthermore, the technology is explicitly recommended by the BSI (German Federal Office for Information Security) in its current C5 catalog for sensitive cloud workloads. The performance overhead for Confidential Computing is typically in the low single digits, making it negligible for most operations.

`Technical Requirements: Intel TDX / AMD SEV-SNP and Linux 6.11.`

How enclaive Dyneemes Works

The technical foundation of Dyneemes is enclaive Buckypaper, our Confidential VM that serves as a protected runtime environment. Dyneemes allows you to provision and orchestrate dedicated Kubernetes pods within this Confidential VM, completely isolated from the provider's environment.

Since Dyneemes is compatible with all major Kubernetes distributions and requires only a minimal performance overhead of 2 to 8 percent, implementing the Confidential Kubernetes environment is quick and easy.



Why This Architecture – and None Other?

Isolated Pods Instead of Isolated Nodes

Unlike other Confidential Computing solutions, Dyneemes does not rely on isolating entire Kubernetes nodes. Instead, it focuses on isolated pods within a Confidential VM, providing several advantages:

- Maximum security with full kernel and hardware isolation at the pod level
- Resource efficiency and better utilisation of underlying hardware
- Multi-tenancy platform instead of single-tenant “islands”
- A dedicated kernel per pod reduces attack surface
- Seamless Integration via CRI for maximum future-proofing, including quantum-safe encryption
- A economically viable business model for MSPs

Confidential VM vs. Traditional Node Hardening

Using enclaive Buckypaper as a Confidential VM establishes a definitive security perimeter that is independent of the underlying cloud or virtualisation stack. Even root access to the host or hypervisor provides no insight into the protected workloads.

Independent Key Management (enclaive Vault)

Keys and secrets remain entirely under the customer‘s control. While you provide the platform, you never have access to cryptographic material. This Hold-Your-Own-Key (HYOK) principle is vital for sovereignty, Zero Trust, and compliance.

Host Protection From Container Escalation

Confidential Containers isolate workloads via hardware and encrypt their memory in RAM. This prevents compromised containers from attacking the host kernel or accessing other containers – ideal for MSPs operating multi-tenant environments.

Hybrid Operations and Seamless Migration

Existing Kubernetes or container clusters can run in parallel with Confidential Containers. Workloads can be migrated incrementally or individually at runtime without interrupting existing services – perfect for MSPs supporting flexible hybrid scenarios.

Confidential Kubernetes as a Managed Service

As a cloud-native, Kubernetes-compatible, and multi-tenant solution, Dyneemes is ideal for delivery as a standardised managed service.

The MSP manages:

- Operations, scaling, and monitoring of the Kubernetes platform
- Lifecycle management of the Dyneemes environment
- Integration into existing Managed Kubernetes stacks

The Customer retains:

- Control over data, code, and keys
- Verifiable security through Remote Attestation
- Freedom in cloud and platform choice
- A familiar environment (same APIs, CI/CD pipelines, tools, etc.)

How Confidential Kubernetes Drives Your Business

ADDITIONAL REVENUE POTENTIAL

- Premium Managed Kubernetes offerings for regulated industries
- New services centered around compliance, data protection, and sovereignty
- Upgrading existing services, such as Confidential DevOps pipelines

LOW OPERATIONAL EFFORT

- No traditional HSMs or dedicated physical clusters required
- Cloud-native scaling and self-healing capabilities
- Rapid provisioning of new customer environments

STRONG MARKET DIFFERENTIATION

- Protection of “Data in Use” – a clear USP
- A sovereign, European alternative to hyperscaler-only approaches
- No vendor lock-in; no dependency on the cloud provider
- Compatible with existing hyperscalers and CNCF Kubernetes distributions

Added Value for Customers

Zero Trust Towards the Provider

No implicit trust in the MSP or cloud provider required

Confidential Container Workloads

Protection of data, code, and models even during active processing

Audit and Compliance Readiness

Cryptographically provable workload integrity

New Use Cases

Secure and compliant integration of AI/ML workloads, processing sensitive data in shared environments, or secure multi-party collaboration

CONCLUSION

Managed Kubernetes With Built-in Trust

With Managed Confidential Kubernetes based on enclaive Dyneemes, you can quickly and easily transform existing Kubernetes environments into a modern platform for highly sensitive workloads. This solution satisfies even the most strictly regulated industries without sacrificing scalability or profitability.

As an MSP, you gain a powerful, innovative tool to clearly differentiate yourself in the crowded Managed Kubernetes market, reach new customer groups, and enforce trust technically rather than only promising it organisationally.

Confidential Computing thus becomes your strategic service enabler.

PREISE & DISCOUNT STAFFELN

Partner Pricing

vHSM Preis und Discount Staffel

vHSM Tenant = 600,- € monatl.

Staffel A · 1 – 9	5 %
Staffel B · 10 – 19	15 %
Staffel C · 20 – 49	25 %
Staffel D · 50 – 99	35 %

Buckypaper Preis und Discount Staffel

vCPUs = 20,- € monatl.

Staffel A · 1 – 99	5 %
Staffel B · 100 – 249	15 %
Staffel C · 250 – 499	25 %
Staffel D · 500 – 999	35 %
Staffel E · ≥ 1000	40 %

Dyneemes Preis und Discount Staffel

Control Plane 100,- € · sc-camel-v-c-p-us = 30,- € monatl.

Staffel A · 1 – 99	5 %
Staffel B · 100 – 249	15 %
Staffel C · 250 – 499	25 %
Staffel D · 500 – 999	35 %
Staffel E · ≥ 1000	40 %

M(S)SP BEISPIEL PACKAGE BUCKYPAPER (VHSM ALS VM)

vHSM 5 Tenant + 250 sc-camel-v-c-p-us = 6.600 € / Monat

M(S)SP BEISPIEL PACKAGE DYNEEMES (VHSM ALS K8S)

vHSM 5 Tenant + CP + 250 sc-camel-v-c-p-us = 8.575 € / Monat

NEXT STEPS

Start Your Confidential Kubernetes Business Now!

Expand your Managed Kubernetes portfolio with a new level of security and position yourself as a provider of trusted cloud and container services.

HOW ENCLAIVE SUPPORTS YOU

- Continuous development of Dyneemes
- Workshops and training courses
- Setup of lab/test environments
- Support for pilot projects
- Co-marketing and co-selling
- Attractive partner and pricing models

CONTACT
sales@enclaive.io

FOR MORE INFORMATION, VISIT
enclaive.io

enclaive