
enclaive
Solution Brief
enclaive Multi-Cloud Platform
The Only Platform for Confidential Computing Environments

enclaive

Executive Summary

Enterprises today face a critical challenge: harnessing the scalability and flexibility of the cloud without falling into vendor lock-in or compromising data security. In traditional architectures, data remains unencrypted during processing, which undermines security, confidentiality, and digital sovereignty.

This is where Confidential Computing represents a fundamental paradigm shift. Sensitive assets – such as data, code, and AI models – are isolated within hardware-based enclaves, ensuring that infrastructure providers cannot gain insight into the user's application logic or business data. The enclaive Multi-Cloud Platform (eMCP) makes this highly complex technology accessible to organisations of all sizes for the first time. Secure Confidential Environments can be deployed across multiple cloud providers with just a few clicks, requiring no specialised expertise or time-consuming infrastructure overhauls.

The eMCP is defined by its technology-agnostic approach and radical simplification. As the only platform providing cross-cloud orchestration of Confidential Multi-Cloud resources, it automatically "lifts" containers or VMs into secure enclaves – with zero code changes required. Furthermore, the integrated workload attestation leverages cryptographic proof to provide "out-of-the-box" compliance documentation for all major regulatory frameworks.

This Solution Brief details the features of the eMCP and the specific resources – from Confidential Kubernetes clusters to virtual HSMs – that you can deploy. We explore the specific benefits for roles such as CISOs, Cloud Architects, and Developers, and demonstrate through practical use cases (e.g., Confidential AI) how the eMCP ensures maximum data sovereignty.

enclaive

Gartner lists Confidential Computing as one of the

10 Strategic Technology Trends 2026

Recommended by official bodies (BSI C5, gematik, DORA §9)

~50%

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

Only

2-3%

additional overhead for 3D Encryption

enclaive

Introduction

Organisations and public institutions are increasingly migrating workloads to the cloud to capitalise on attractive scaling and cost advantages. However, storing all data with a single cloud provider creates dependencies and leads to a loss of control over data, code, and AI models.

Furthermore, cloud users face a fundamental security dilemma: conventional security concepts encrypt data "at rest" (in storage) and "in transit" (during transfer), but not "in use" (during processing). Consequently, cloud provider administrators, compromised hypervisors, or hackers with host access could potentially view the data – a significant security gap and a genuine risk to sovereignty and compliance.

The Paradigm Shift: Confidential Computing with eMCP

Confidential Computing closes this gap by shifting trust from the software layer to the hardware layer (chip-level). By utilizing Trusted Execution Environments (TEEs) – secure enclaves directly on the CPU or GPU – workloads and data remain cryptographically isolated even during processing. Neither the cloud provider nor internal or external attackers can access the memory.

In practice, however, Confidential Computing is complex. While many cloud providers offer the necessary hardware, they rely on differing chip technologies. As a result, applications would need modification, operational processes would require redesigning, and specialised knowledge would have to be built – especially in multi-cloud environments. This is exactly where the enclaive Multi-Cloud Platform (eMCP) comes in.

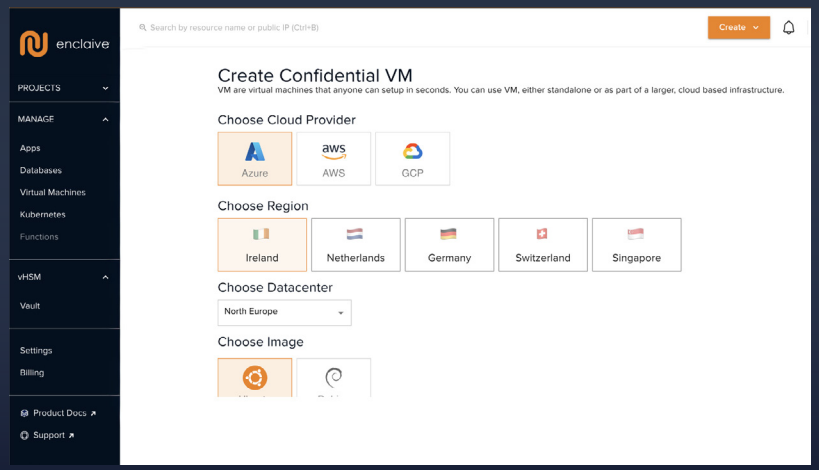
The eMCP is the first platform that empowers companies to generate, orchestrate, and operate fully isolated, hardware-based Confidential Environments across multiple cloud providers. It combines chip-level security, cloud agnosticism, and automated compliance into a unique solution – fully post-quantum secure and "Made in Germany."

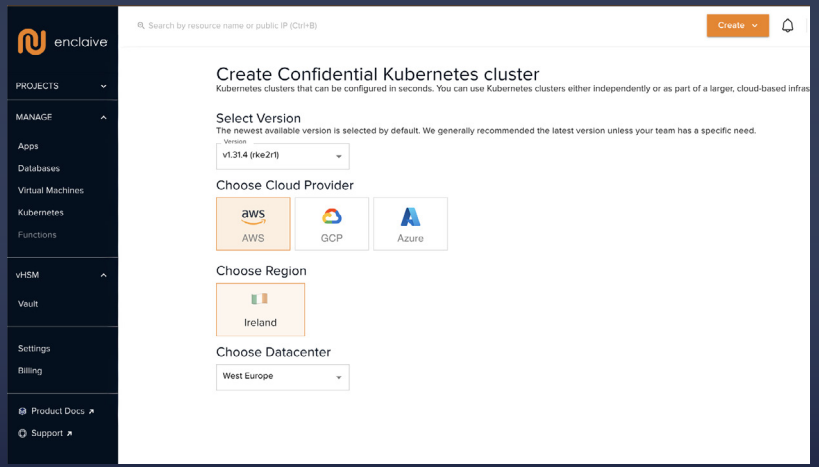
enclaive

The eMCP in Detail

The eMCP is your all-in-one solution to set up and manage confidential execution environments for AI models, databases, applications, and microservices in the multi-cloud with just a few clicks. Using one central dashboard, the platform offers you the following capabilities:

- **Confidential Virtual Machines (Buckypaper):** Run workloads in isolated enclaves. The source code remains untouched while the security architecture is augmented in the background
- **Confidential Kubernetes-Cluster (Dyneemes):** Containerised workloads run in a Zero Trust infrastructure where the control plane, node pools, or individual pods are fully protected
- **Key-Management-as-a-Service (Vault):** Manage keys, identities, and secrets in a protected environment – without dedicated physical HSM infrastructure, but with hardware-level cryptography thanks to enclaives virtual HSM (vHSM)
- **Attestation-as-a-Service (Nitride):** Enclaves can cryptographically prove they are running on trusted hardware, providing technical evidence for audits and compliance
- **Centralised Multi-Cloud Control:** Manage resources, policies, and secrets across different clouds consistently, eliminating provider-specific silos





enclaive

Why Choose eMCP

In the rapidly growing Confidential Computing market, the eMCP sets new standards. Other vendors offer only isolated solutions for specific providers and hardware types or require extensive expertise and code changes for implementation. The eMCP positions itself as a unique solution – not just compared to classic security approaches, but specifically within the Confidential Computing market.

Features only available with eMCP:

Cross-Cloud Orchestration

The eMCP is the only platform providing a unified control plane for Confidential Computing environments across heterogeneous multi-cloud landscapes. Manage everything in one place, regardless of provider or hardware.

Automated Provisioning & Easy Deployment

Thanks to policy-driven deployment and automated attestation, Confidential Environments are set up in seconds and Zero Trust by design. Your workloads become "confidential" in no time.

Technology Agnostic

The eMCP natively utilises available TEE technologies (Intel SGX, AMD SEV-SNP, ARM CCA, NVIDIA Hopper/ Blackwell) and abstracts them into a unified security architecture. You remain independent of hardware vendors and cloud providers.

Out-of-the-box Compliance

The eMCP actively supports you in meeting the strictest regulations (GDPR, NIS2, DORA, TISAX, etc.). Via remote attestation and a practical reporting feature, you can technically prove that your data is protected in a verified hardware enclave at all times.

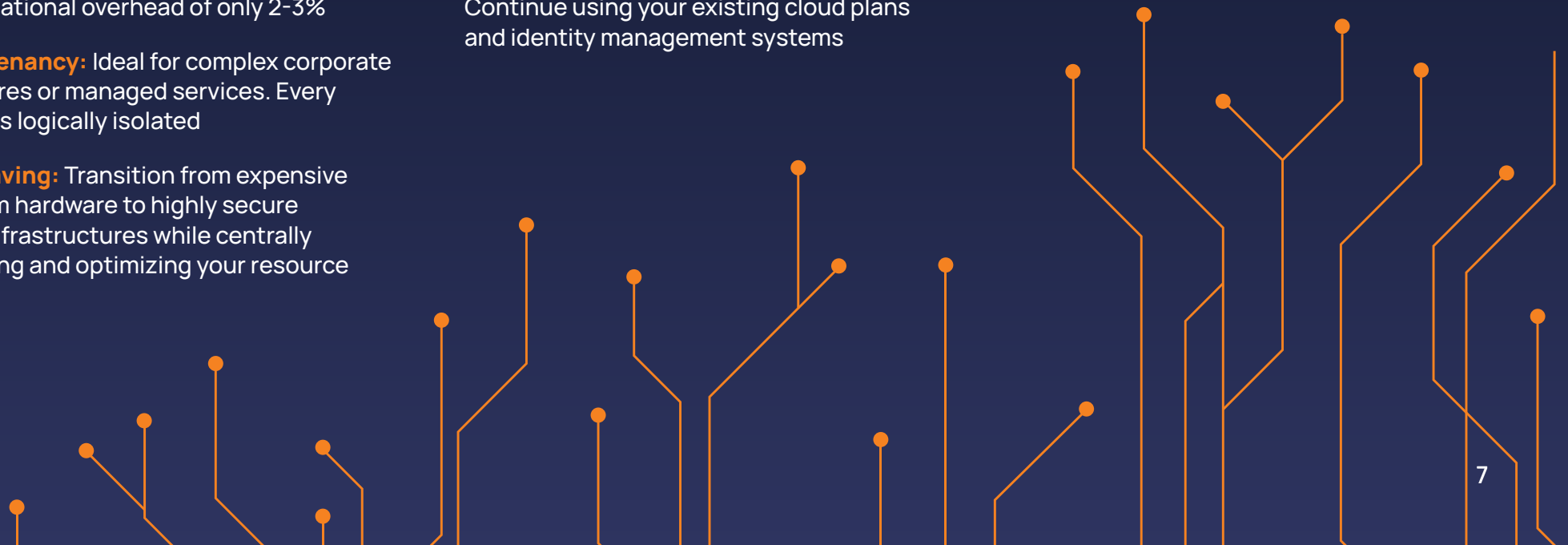
With eMCP, you benefit from a higher level of security and control – while eliminating the complexity of cloud management, implementation and regulatory requirements.

enclaive

Your Key Benefits

Using the eMCP provides tangible technical and economic advantages:

- **Seamless Integration:** Open-source components and standardised APIs (PKCS#11, KMIP, and REST) ensure smooth integration into existing infrastructure and security stacks
- **Zero Code Changes:** Existing applications run unchanged within confidential execution environments
- **Minimal Performance Overhead:** Encryption with enclaive typically incurs a computational overhead of only 2-3%
- **Multi-Tenancy:** Ideal for complex corporate structures or managed services. Every tenant is logically isolated
- **Cost saving:** Transition from expensive on-prem hardware to highly secure cloud infrastructures while centrally managing and optimizing your resource usage
- **Protection in Shared Infrastructure:** Isolation is achieved via enclaves rather than the hypervisor – keeping your data safe from other data center customers and the provider itself
- **Vendor Independence:** Avoid vendor lock-in by managing workloads across private, public, and hybrid cloud environments from different providers
- **Bring Your Own Subscription (BYOS):** Continue using your existing cloud plans and identity management systems
- **Compliance Booster:** The eMCP provides the necessary technical evidence for various regulations, significantly simplifying reporting
- **Post-Quantum Security:** Future-proof your data today. With eMCP and enclaive encryption, implementing your post-quantum transformation is effortless

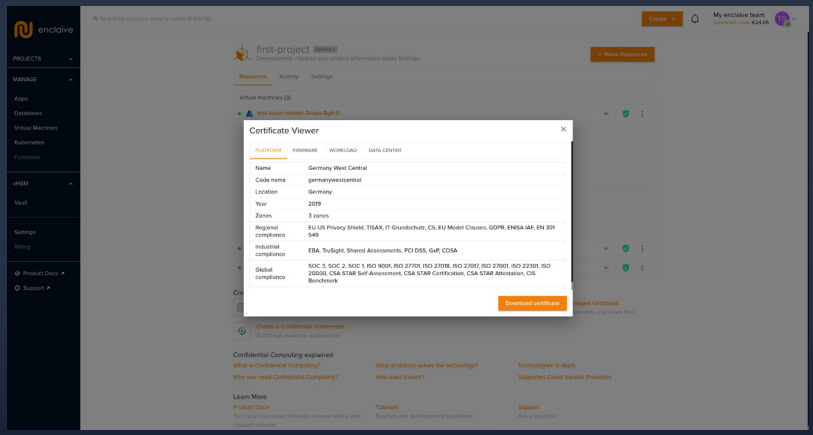


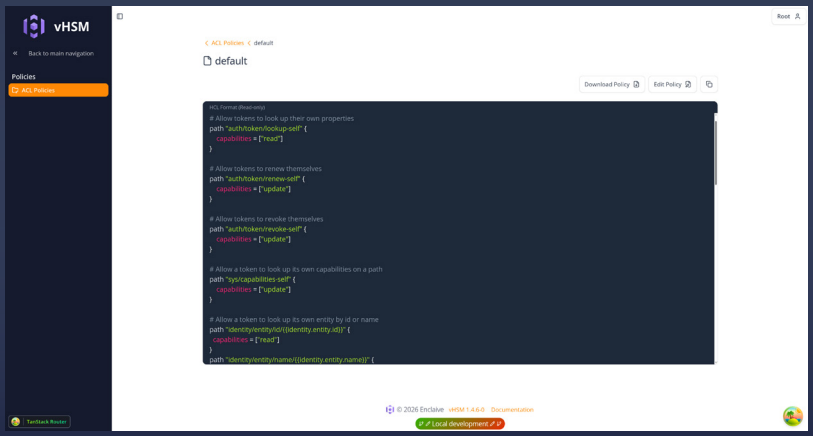
enclaive

Usability

Instead of juggling multiple management consoles and losing oversight, eMCP centralises your operations:

- **Uni ied Control Panel:** Manage your entire cloud resource landscape across providers via a single dashboard
- **Multi-Cloud Resource Provisioning:** Deploy VMs, Kubernetes clusters, and other resources directly with a few clicks
- **Identity & Access Management:** Define permissions and access roles across different clouds in one place
- **Centralised Security Con iguration:** Configure security settings for all confidential computing environments from a single point of control, including firewall and access policies
- **Automated Work lows:** Automate redundant tasks like scaling and resource distribution. Verification of enclave integrity also runs automatically via remote attestation
- **Real-Time Monitoring:** Keep track of resource utilisation, performance, and security through integrated monitoring tools and custom alerts
- **Reporting & Analytics:** Generate detailed reports on resource usage, costs, and performance metrics





enclaive

How eMCP Supports Your Team

The platform bridges the gap between strategic security requirements and operational feasibility, catering to both decision-makers and technical teams.

CISOs

For security officers, the eMCP provides technical safety guarantees rather than contractual assurances – and makes confidentiality verifiable.

- **Risk Mitigation:** Data remains encrypted even if the underlying infrastructure is compromised
- **Verifiable Compliance:** Cryptographic attestation provides tamper-proof audit trails and robust regulatory evidence
- **Strategic Transparency:** A centralised view of all workloads allows for informed decision-making and efficient security governance

Cloud Architects

The eMCP reduces the complexity of distributed multi-cloud architectures and establishes a consistent operational model.

- **Unified Architecture:** One platform instead of fragmented cloud silos
- **Faster Implementation:** Automated attestation and provisioning
- **Multi-Cloud Flexibility:** No security or lock-in risks

Developer

Provide your Devs with security that doesn't slow down the development lifecycle.

- **No TEE Expertise Required:** Existing workloads run without the need for refactoring
- **IP Protection by Design:** Models, data, and business logic remain confidential
- **Simple CI/CD Integration:** Security mechanisms integrate seamlessly into existing processes

enclaive

Use Cases

Confidential Computing delivers value wherever sensitive data is processed, regulatory requirements must be met, or digital sovereignty is paramount.

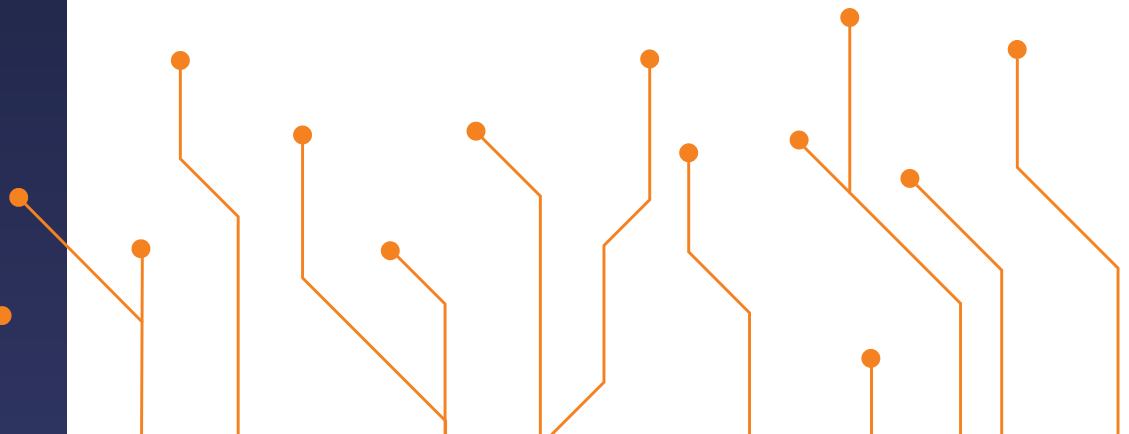
- **Secure Lift-and-Shift Migrations:** Move on-premises workloads to the cloud. Enclaves serve as confidential execution environments – that can be configured to mirror existing setups if needed
- **Regulated Industries:** Process highly sensitive information in the cloud where data must not be compromised under any circumstances (e. g., finance, healthcare, or the public sector)
- **Confidential AI:** Protect AI models, sensitive training data, and inference processes from theft and tampering within secure enclaves. Enable innovation without losing control of your data
- **Confidential Data Spaces:** Create sovereign, trusted data spaces where partners or third parties can exchange or analyse data collectively without any party (or the host) seeing the raw data of others
- **Confidential SaaS:** SaaS providers can use eMCP to guarantee data isolation to their customers – both contractually and technically – providing a powerful competitive advantage

Conclusion

Comprehensive Cloud Protection, Simplified

The requirements for cloud security have fundamentally changed. Databases, applications, and AI workloads must be encrypted even during processing to ensure confidentiality and sovereignty. Confidential Computing delivers this, but new security approaches must not lead to added complexity, higher operational costs, or technological dependencies.

The enclaive Multi-Cloud Platform solves these challenges by combining hardware-based confidentiality with a cloud-agnostic, easy-to-use operational model. It provides a platform that balances security, compliance, performance, and usability. The eMCP is more than just an extension of existing security – it represents a paradigm shift in cloud security and the foundation for a sovereign, future-proof multi-cloud strategy.



enclaive

Secure Your Cloud Workloads with Confidential Computing

The enclaive Multi-Cloud Platform is the answer to the challenges of modern data sovereignty. Protect your sensitive workloads with maximum security without redesigning your entire infrastructure.

- Schedule a demo
- Speak with our experts today
- Try it yourself here
- Find detailed instructions here

Experience how simple Confidential Computing can be – with eMCP, your key to the sovereign multi-cloud.

Contact
sales@enclaive.io

For more information, visit
enclaive.io