enclaive

Solution Brief

Cloud Sovereignty in Hyperscaler Environments

Confidential Computing as a secure foundation for high-performance cloud networks

Executive Summary

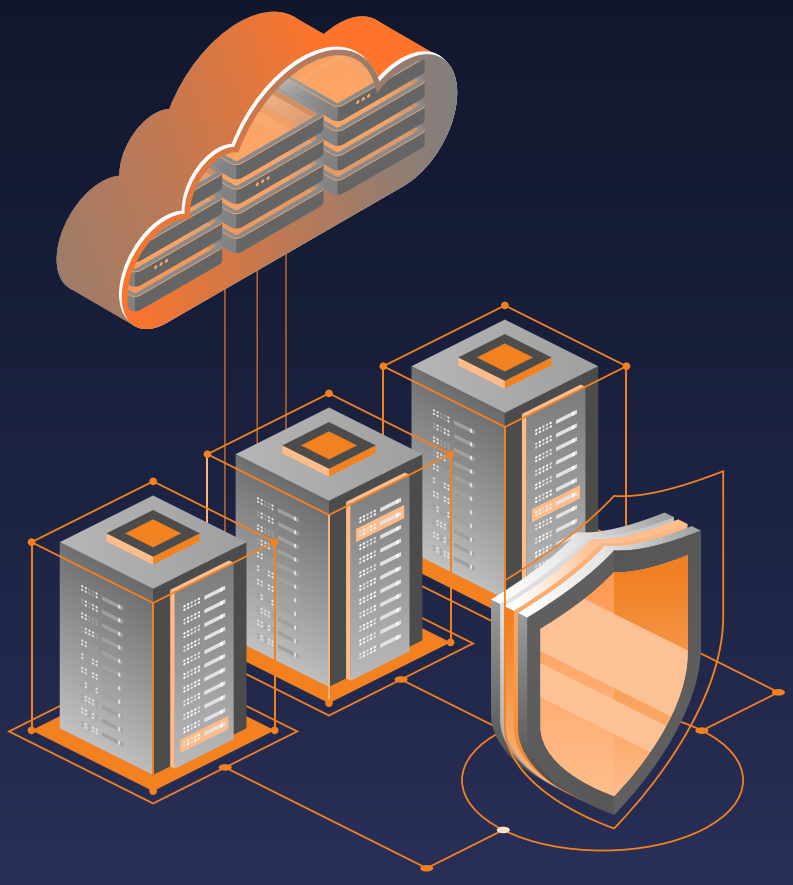
German and European organisations face a strategic dilemma: to drive digital transformation, they depend on the computing power of U.S. hyperscalers — yet doing so risks compliance violations and the loss of data sovereignty.

enclaive's Confidential Computing resolves this conflict. The technology protects data even during processing, enabling organisations to use cloud environments securely without having to trust in the provider — as they can neither view nor access the data.

How enclaive's holistic approach secures cloud environments:

- The **eMCP** (enclaive Multi-Cloud Platform) enables a resilient multi-cloud architecture across several providers.
- With **Vault**, users retain full control of cryptographic, post-quantum-secure keys through independent key management (Hold Your Own Key).
- **Nitride** ensures verifiable integrity of confidential workloads and the underlying infrastructure.

Together, these solutions form the foundation for secure, high-performance, and compliance-ready cloud adoption — paving the way for genuine digital sovereignty within hyperscaler environments.



Introduction

Digital services that are both high-performance and highly secure have become a top priority across Germany and Europe. Public institutions, healthcare providers, and the financial sector manage vast volumes of sensitive data and complex applications that depend on scalable, highly available cloud infrastructures.

U.S. hyperscalers deliver the capabilities required for such workloads: cutting-edge cloud-native services, high-performance computing, advanced AI models, and extensive ecosystems. This technological maturity currently surpasses that of European alternatives by far. For many organisations, these U.S.-based services are therefore essential to accelerate new projects, launch innovative offerings, and drive digital transformation. Yet combining this technological advantage with strict European compliance and sovereignty requirements remains a central challenge.

Challenges

Using U.S.-based cloud services comes with substantial risks and challenges:

- **Compromised Data Sovereignty:** U.S. laws such as the CLOUD Act and FISA 702 allow U.S. authorities to demand access to data from American providers. This also affects data from European organisations stored in the EU.
- **Vendor Lock-in:** Dependence on a single provider limits flexibility and complicates exit strategies.
- **Infrastructure and Kill-Switch Risks:** The hardware foundation of hyperscalers could, in theory, be manipulated for data exfiltration — or services could be shut down or wiped remotely, for instance during political conflicts, abruptly disabling critical systems.
- **Regulation and Proof of Compliance:** Stringent frameworks like GDPR or DORA require high security levels for data storage, transfer, and processing abroad — yet most hyperscaler infrastructures lack the technical evidence of data confidentiality.

Given these risks, hyperscalers are often deemed unsuitable for sensitive workloads. Yet abstaining from them would significantly slow digitalisation and limit cloud innovation. What's needed is a technical foundation that guarantees absolute confidentiality and sovereignty across any cloud environment.

The Solution: enclaive Confidential Computing

Confidential Computing closes one of the last major security gaps in the cloud — the protection of data in use. Traditional encryption methods safeguard data at rest and in transit, but leave it exposed during processing. Confidential Computing moves sensitive workloads into hardware-based, isolated Trusted Execution Environments (TEEs) — also known as enclaves — thereby securing data in all three dimensions and preventing unauthorised access, even from administrators or cloud providers.

Why enclaive?

Based in Berlin and subject to German and European jurisdiction, enclaive offers a comprehensive portfolio of Confidential Computing solutions tailored to the needs of highly regulated industries — designed for seamless operation within hyperscaler infrastructures. The idea is simple: with enclaive, you no longer have to trust your cloud provider.

Our solutions establish a robust foundation for the secure use of hyperscalers:

EMCP

The eMCP (enclaive Multi-Cloud Platform) is a secure, multi-tenant platform for managing confidential databases, virtual machines (enclaive Buckypaper), and Kubernetes clusters (enclaive Dyneemes) across U.S. and European clouds. The redundant multi-cloud architecture ensures high flexibility and resilience while eliminating vendor lock-in and kill-switch risks.

Vault

Independent key management built on a virtual Hardware Security Module (vHSM), enabling Bring and Hold Your Own Key (BYOK/ HYOK) to ensure that only the organisations themselves can decrypt their enclaves — even within hyperscaler environments.

Nitride

Nitride assigns unique identities and permissions to workloads, ensuring that only verified workloads and authorised users can access enclaves. Through cryptographic attestation, Nitride provides verifiable proof — essential for audits and compliance — that workloads run confidentially and the hardware remains unaltered.

Your benefits with enclaive

3D Encryption
Data is protected across all three dimensions (at rest, in transit, and in use) within confidential, isolated execution environments. Only authorised users gain access, creating a perfect complement to Zero-Trust architectures.

Effortless Integration
Our enclaves can be deployed without code modifications and integrate seamlessly into existing infrastructures, delivering maximum security with minimal implementation effort.

Post-Quantum Security
Quantum computers will soon threaten conventional encryption. enclaive already implements a post-quantum strategy, safeguarding data against future quantum attacks and mitigating “store now, decrypt later” risks.

Confidential AI
Our GenAI Firewall Garnet protects sensitive data used in AI interactions through pre-filtering and pseudonymisation — enabling organisations to securely use AI tools without compromising confidentiality, compliance or data sovereignty .

Minimal Performance Overhead
Our encryption adds only about 3% computational overhead, ensuring robust security while maintaining workload performance.

Data Protection & Compliance
enclaive meets the strict requirements of GDPR, DORA, IT-Grundschutz, ISO 27001, TISAX, and other major frameworks — helping organisations achieve seamless and verifiable compliance.

Use Cases

- **Confidential Processing of Large Data Volumes:** Organisations can now process and operate their wide variety of data and applications in cloud environments that are both high-performance and highly secure.
- **Cloud Sovereignty:** With Bring and Hold Your Own Key (BYOK/HYOK), users retain full control of encryption keys and data — regardless of cloud provider or location.
- **Meeting Strict Compliance Requirements:** Confidential Computing provides the technical foundation to meet regulatory mandates such as GDPR, NIS2, or industry-specific frameworks — supported by attestation for verifiable compliance.
- **Secure Data Spaces and Collaboration:** For multi-party data ecosystems, enclaive's end-to-end 3D encryption establishes the necessary trust without compromising data sovereignty.
- **Multi-Cloud Strategies without Vendor Lock-in:** Workloads can be securely distributed across multiple cloud providers. This enables full flexibility and availability without the risk of being dependent on one single provider.
- **Secure Migration of Critical Workloads:** Confidential applications can be moved to hyperscaler environments without code modifications. The data remains protected throughout the process.

Conclusion

enclaive's Confidential Computing technology bridges the gap between the computing power of hyperscalers and the stringent privacy and sovereignty requirements of European and German organisations. Through comprehensive 3D encryption, sovereign key management, and verifiable data integrity via attestation, enclaive establishes a new level of absolute cloud confidentiality. Organisations can now leverage U.S. hyperscaler performance without relinquishing control of their data — empowering them to drive cloud transformation securely, sovereignly, and in full compliance.

Embrace the Cloud with Confidence

Contact us for a personal consultation and experience the security of our enclaves firsthand.

Get a free demo:
https://www.enclaive.io/get-a-free-demo-with-enclaive

Or send us an email at
contact@enclaive.io