enclaive

WHITEPAPER

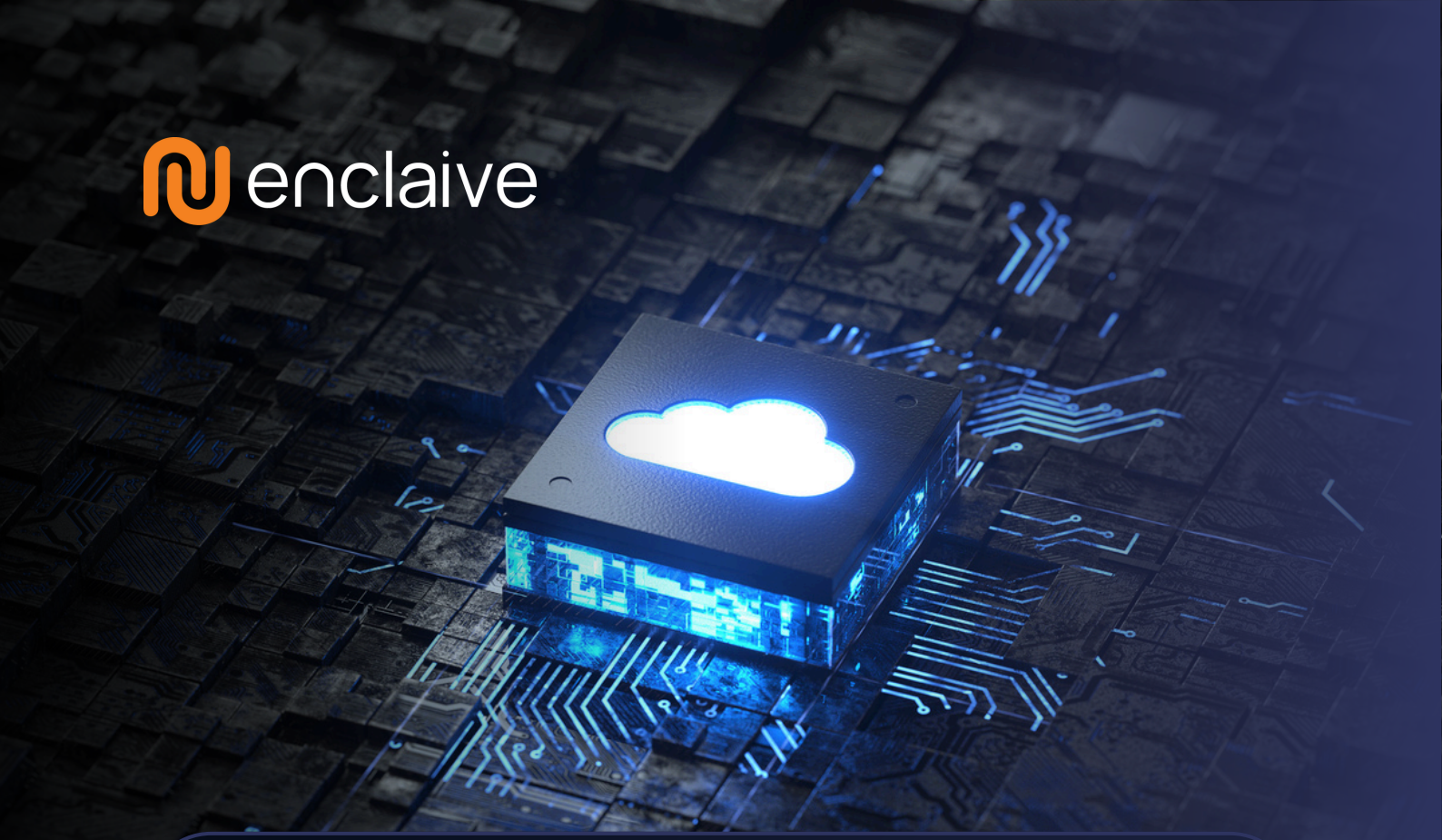
enclaive's Multi-Cloud Platform (eMCP):

Enhancing Cloud Security and Management

enclaive

You will read about:

enclaive



Introduction

The shift to cloud computing has revolutionized IT infrastructure, bringing **flexibility, scalability,** and **cost efficiency**.
However, managing and securing resources across multiple cloud environments presents significant challenges.

Furthermore, many organizations, particularly those dealing with sensitive data, hesitate to migrate to the cloud due to security concerns.
enclaive's Multi-Cloud Platform (eMCP) addresses these issues by offering a comprehensive solution for secure, **confidential and efficient multi-cloud management**.

This whitepaper explores the structure, benefits, and technical implications of eMCP, providing **business leaders and IT professionals** with a clear understanding of its value.

enclaive

What is eMCP?

enclaive's Multi-Cloud Platform (eMCP) is a **state-of-the-art solution** designed to streamline the access, and provisioning, and management of confidential cloud resources within your overall IT environment.

This platform leverages confidential computing technologies using 3D encryption to **ensure data integrity and privacy**, even in multi-tenant and shared environments. Data and applications stay completely secure at rest, in transit and even during processing.

Managed Service:

eMCP is a fully managed service, alleviating the operational, administrative, and security burdens typically associated with deploying and maintaining confidential computing environments.
By offloading these complex tasks to eMCP, businesses can focus on optimizing the development and management of their cloud applications, enhancing productivity and innovation.

Seamless Integration:

eMCP integrates effortlessly with existing IT infrastructures, allowing businesses to retain full control over their data and applications without necessitating significant changes to their current workflows. This ensures a smooth transition to a secure cloud environment.

enclaive

Challenges Solved by eMCP

Data Security:

Traditional cloud models raise concerns about data visibility and unauthorized access. eMCP employs hardware-based 3D encryption and Trusted Execution Environments (TEEs) to protect data in transit, at rest, and in use.

Vendor Lock-In:

Organizations often face difficulties switching providers due to dependency on specific technologies. eMCP mitigates this risk by supporting a variety of cloud environments, offering flexibility and avoiding vendor lock-in.

Cost Management:

Managing cloud costs can be unpredictable. eMCP provides tools for monitoring and controlling expenses, ensuring cost-efficiency.

Compliance:

Meeting regulatory requirements is challenging in a multi-tenant cloud environment. eMCP ensures compliance with regulations such as GDPR and HIPAA by providing robust encryption and access control mechanisms.

enclaive

Structure of eMCP

enclaive's Multi-Cloud Platform (eMCP) is built to enhance security, scalability, and flexibility for cloud management. Here's how it's structured:

- Integration:
  - eMCP seamlessly integrates with different cloud services, which means you don't need to overhaul your current systems. This integration simplifies the deployment and management processes, allowing businesses to continue using their existing tools and workflows.
- Security:
  - Security is at the core of eMCP. The platform uses Trusted Execution Environments (TEEs) to ensure data is encrypted and secure during processing. This prevents unauthorized access and protects data in use, at rest, and in transit.
- Scalability:
  - eMCP is designed to scale effortlessly. Whether you need to expand your operations or handle fluctuating demands, eMCP can adjust your infrastructure without extensive reconfiguration, making it easy to grow your business.
- Flexibility:
  - eMCP supports a wide range of IT environments. It can be deployed as a private, on-premises solution or as a platform-as-a-service (PaaS). This flexibility allows businesses to choose the deployment method that best suits their needs.

enclaive

Benefits of eMCP

Enhanced Security:

eMCP uses advanced encryption methods and secure enclaves to protect sensitive information from breaches and unauthorized access. This ensures that data remains confidential and secure at all times.

Operational Efficiency:

Managing multiple cloud environments can be complex and costly. eMCP simplifies this by providing a unified platform that reduces the complexity and operational costs associated with multi-cloud management. Businesses can focus on their core operations rather than the intricacies of cloud management.

Cost Savings:

eMCP's cost management tools enable businesses to monitor and control their cloud spending effectively. This ensures that companies only pay for the resources they use, leading to significant cost savings.

Regulatory Compliance:

eMCP helps businesses meet stringent regulatory requirements, such as GDPR and HIPAA, by providing robust encryption and access control mechanisms. This reduces the risk of legal issues and financial penalties.

Trust and Transparency:

eMCP offers verifiable proof of data integrity and confidentiality. This builds trust between businesses and their cloud providers, ensuring transparency and accountability in how data is managed and secured.

enclaive

Technical Requirements

The technical requirements for implementing eMCP are crucial for understanding the necessary infrastructure and software modifications. These requirements ensure that eMCP operates efficiently and securely across various cloud environment.

Hardware Requirements:

eMCP leverages confidential computing technologies that require specific hardware capabilities:

1. Intel Trusted Domain Extensions (TDX): Requires Intel Xeon Series 5 or related processors, such as Saphire Rapids and Emerald Rapids.
2. AMD Secure Encrypted Virtualization (SEV): Compatible with AMD EPYC 2 (SEV ES), EPYC 3 (SEV SNP), or later processors (Rome, Milan).
3. ARM Confidential Compute Architecture (CCA): Needs ARM Cortex A9 or newer processors.

These processors come with built-in cryptographic coprocessors on the System on Chip (SoC), enabling secure data encryption and processing.

enclaive

Software Requirements:

Implementing eMCP necessitates specific software capabilities, particularly for guest and host operating systems, including the hypervisor:

1. Kernel and Hypervisor Patches:
   - The host kernel, hypervisor, guest UEFI, and guest kernel need patches to support the new security features of CPUs (i.e., SEV, TDX, CCA). Major Linux distributions like SUSE Enterprise, Red Hat Enterprise, and Ubuntu Canonical have partially implemented these patches.
2. KVM/QEMU:
   - Patches for supporting security processors are being discussed in the Linux kernel working group. enclaive provides all necessary patches for SEV and TDX for major Linux distributions and ready-to-use VM images (.iso, .ovf).
3. VMWare:
   - In vSphere 7.0 Update 1 and later, SEV-ES can be activated on supported AMD CPUs and guest operating systems. VMWare plans to release updates to support SEV SNP and TDX in Q4/2024.

enclaive

What are the components of eMCP?

eMCP offers a range of products designed to enhance security and simplify multi-cloud management. These products provide comprehensive solutions for various cloud-related challenges:

Confidential Virtual Machines (cVMs):

- Data Encryption: cVMs employ 3D encryption to protect data in transit, at rest, and in use.
- Secure Boot: The Confidential Boot process ensures that only trusted code is executed.
- Attestation: Verifies the integrity of the virtual machine and its components using enclaive's vHSM (virtual Hardware Security Module).

Confidential Kubernetes:

- Zero-Trust Infrastructure: Ensures data confidentiality throughout the lifecycle of containerized workloads.
- Seamless Integration: Works with existing Kubernetes environments without significant changes.

Virtual Hardware Security Module (vHSM):

- Vault: Manages secrets, including database passwords, disk encryption keys, and TLS certificates. It provides identity access management and key management features.
- Nitride: Attests cVMs and issues access tokens, ensuring only authorized entities can access secrets stored in Vault.

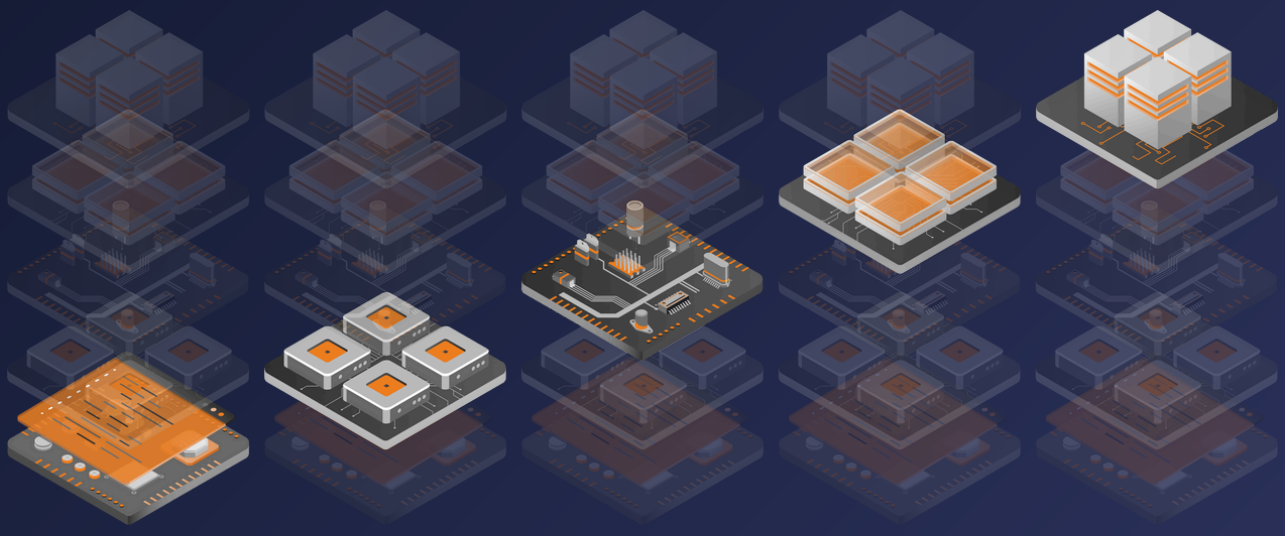
enclaive

Confidential Databases:

- Encryption: Keeps data encrypted at rest, in transit, and in use.
- Compatibility: Works with various database management systems without requiring code modifications.

Managed Solutions:

- Pre-Configured Applications: Offers a portfolio of confidential applications managed by enclaive, saving time and resources for businesses.
- Customizable Environments: Allows businesses to create and manage their own confidential applications and environments.



enclaive

Technical Perks

- Confidential Computing:
  - eMCP leverages TEEs to ensure that data remains encrypted during processing. This is critical for maintaining data privacy and integrity in a multi-cloud environment.

- Performance:
  - Despite the added security measures, eMCP is designed to minimize performance overhead. Tests have shown only a 2% increase in CPU cycles, making it a viable option for performance-sensitive applications.

- Compatibility:
  - eMCP is compatible with various cloud providers and IT environments. This compatibility ensures that businesses can integrate eMCP with their existing systems without significant modifications.

- Hardware Requirements:
  - eMCP requires CPUs with built-in cryptographic capabilities, such as Intel SGX, AMD SEV, or ARM CCA. These technologies are widely available in modern data center hardware.

- Software Requirements:
  - The platform supports major Linux distributions and requires patches to the host kernel, hypervisor, guest UEFI, and guest kernel to enable the necessary security features.

enclaive

Conclusion

enclaive's Multi-Cloud Platform (eMCP) is a powerful solution for businesses seeking to **enhance** their **cloud security and management capabilities**.

By addressing key challenges such as data security, vendor lock-in, and cost management, eMCP provides a **robust, flexible, and compliant platform for all you confidential computing resources**.
Seamless integration and minimal performance impact make it an **ideal choice for organizations looking to secure their cloud environments** without compromising efficiency.

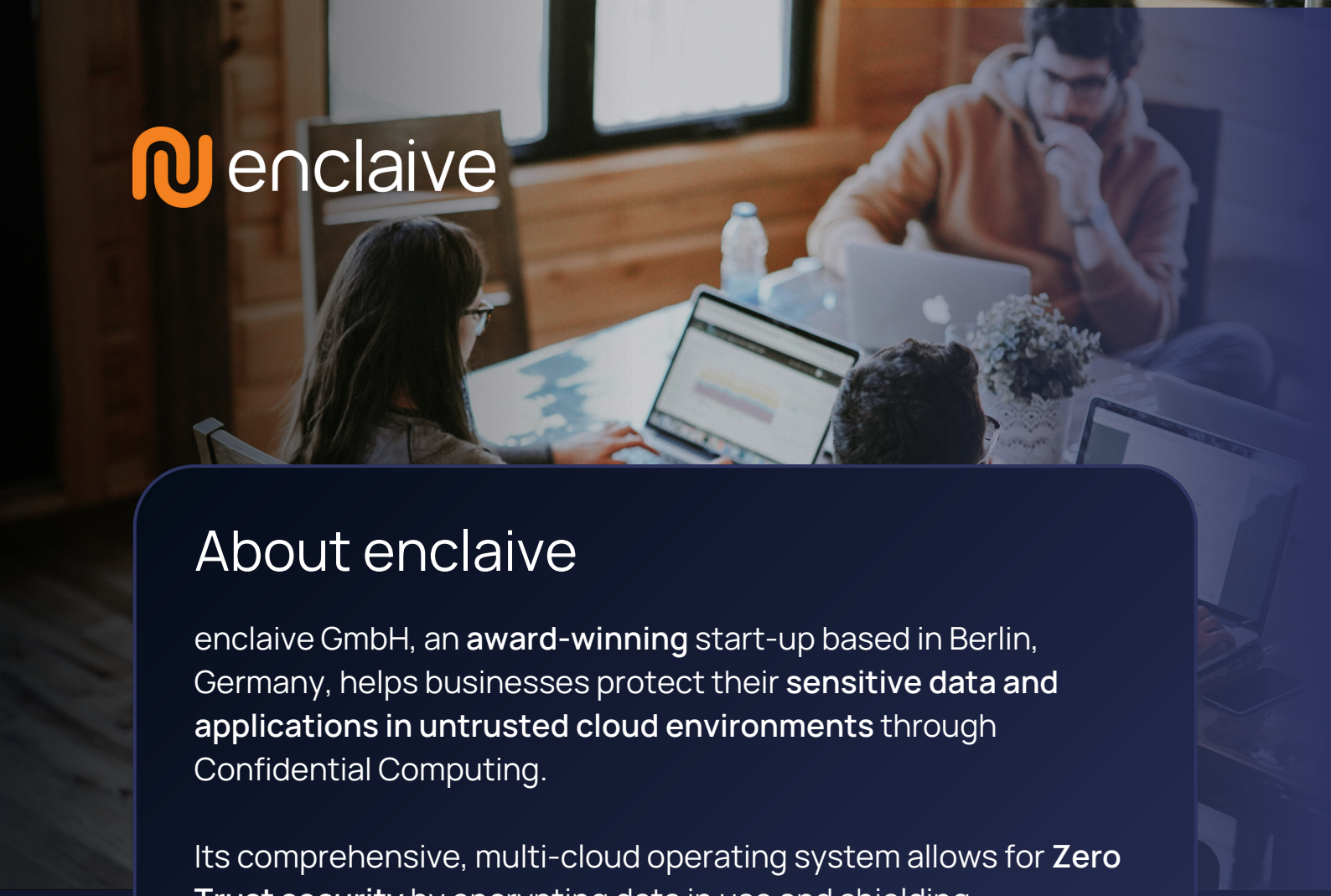
For more information on how eMCP can benefit your organization, explore our documentation linked below.

Further Reading

For a deeper understanding of confidential computing and its benefits, refer to the following resources:

- Confidential Computing 101
- enclaive Multi-Cloud Platform Documentation
- enclaive Multi-Cloud Platform: Get a free demo

For personalized advice and deployment options, contact enclaive at contact@enclaive.io.



About enclaive

enclaive GmbH, an **award-winning** start-up based in Berlin, Germany, helps businesses protect their **sensitive data and applications in untrusted cloud environments** through Confidential Computing.

Its comprehensive, multi-cloud operating system allows for **Zero Trust security** by encrypting data in use and shielding applications from both the infrastructure and solution providers.

With enclaive, businesses can confidently **build, test, and deploy a wide range of cloud applications**, all while maintaining **complete control over their confidential information**.

enclaive's goal is to provide **a universal, cloud-independent technology** for enclaving sophisticated multi- cloud applications, that can be deployed with confidence and ease.

Contact details

github.com/enclaive

linkedin.com/company/enclaive

youtube.com/@confidentialcompute

contact@enclaive.io

+49 302 33 29 29 73

Chausseestr. 40, Berlin, Germany