enclaive x utimaco®

SOLUTION BRIEF

Enhanced Data Protection and Compliance in the Cloud

with enclaive Virtual HSM and Utimaco SecurityServer

enclaive x utimaco®

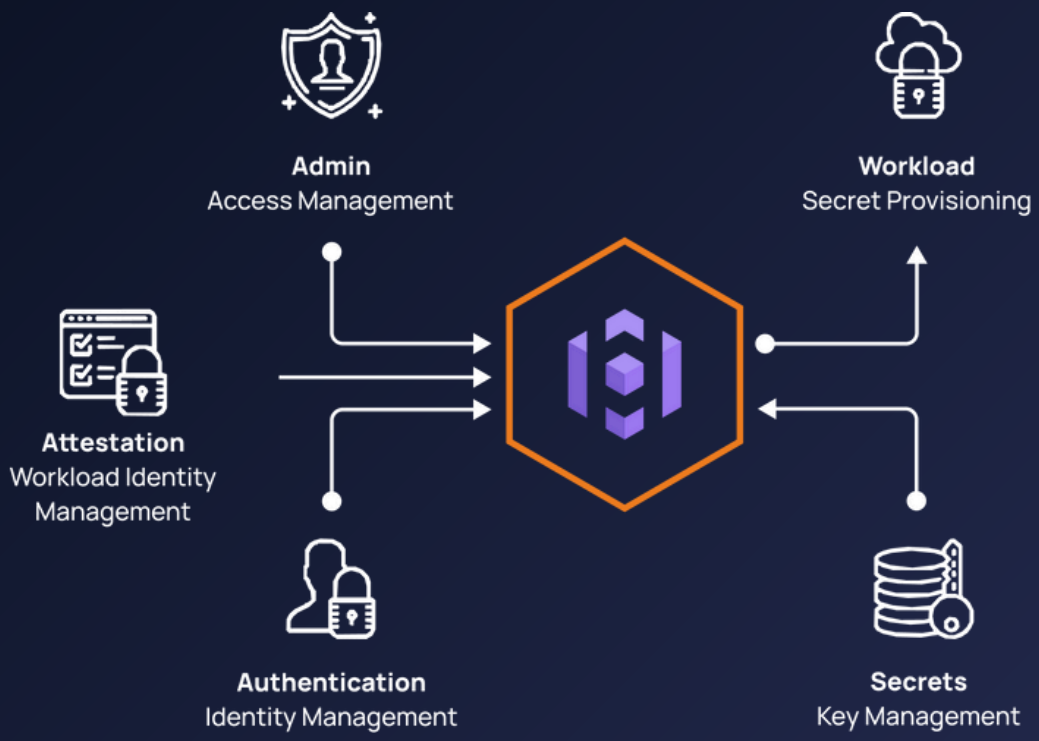
Introduction

Organizations operating in the Cloud today face increasing pressure to shield their business, protect sensitive data, comply with stringent regulations, and secure their modern, distributed application environments.
Managing and granting access to secrets, encryption keys, and sensitive configurations across diverse infrastructure presents significant challenges.

This solution brief outlines how the integration of enclaive Virtual HSM and Utimaco SecurityServer, acting as the root of trust, provides a **robust and comprehensive cloud-ready approach to data protection**.
This synergy enables organizations to **achieve enhanced security in the Cloud**, **meet stringent compliance requirements**, and **streamline their security operations**, particularly for highly regulated, data and business sovereign applications.

enclaive x utimaco®

The Challenge:



Secrets Sprawl

Sensitive credentials (passwords, API keys, tokens, kubeconfigs) are often scattered across various systems, configuration files, and even code, creating security vulnerabilities and making management difficult.

Key Management Complexity in Regulated Environments

Managing the lifecycle of encryption keys under strict regulatory scrutiny demands high-entropy randomness and secure key generation, storage, and usage.

enclaive x utimaco®

The Challenge:

Compliance Requirements

Regulations like GDPR, HIPAA, PCI DSS, and industry-specific mandates necessitate strong roots of trust for cryptographic operations and key management.

Distributed Environments

Modern applications deployed across hybrid, private, and multi-cloud environments require consistent and centralized security controls anchored by a reliable root of trust.

Manual Processes

Relying on manual processes for key generation, distribution, and secret unsealing is error-prone, inefficient, and hinders agility, especially in regulated sectors.

enclaive x utimaco®

The Solution:

Secure Secrets and Key Management with enclaive vHSM and Utimaco SecurityServer (Root of Trust)

This integrated solution leverages enclaive vHSM for centralized secrets management and Utimaco SecurityServer as the foundational root of trust, providing high-entropy randomness and secure unsealing capabilities.

enclaive x utimaco®

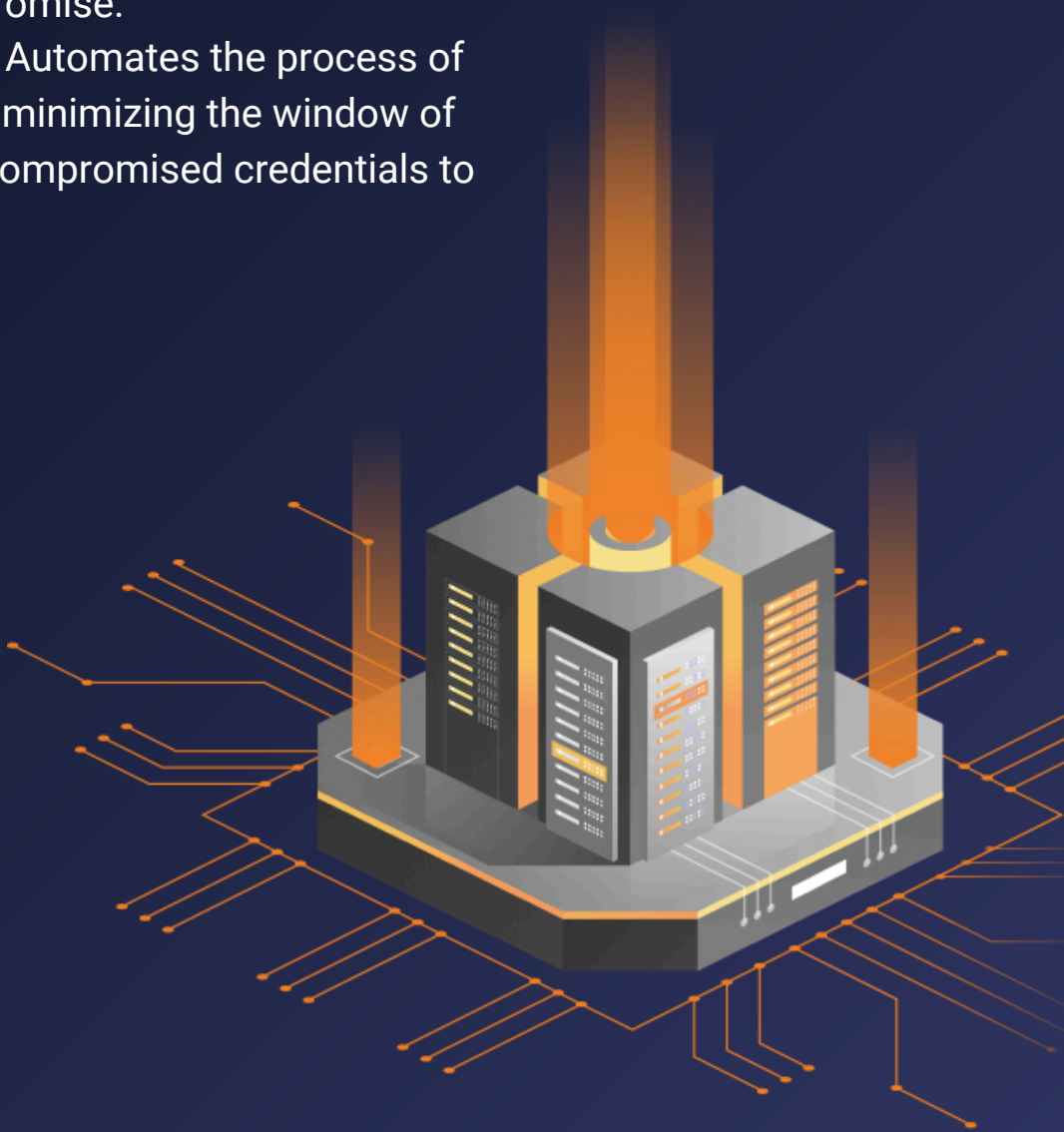
enclaive vHSM

enclaive vHSM is a secrets management platform that provides a secure and centralized location to store, access, and audit secrets across dynamic infrastructure, leveraging secure:

- **Centralized Secrets Management:** Securely stores and manages all types of secrets, including API keys, passwords, certificates, and encryption keys within secure enclaves.
- **Secure Enclave Technology:** Leverages confidential execution environments to encrypt the vHSM at rest, in transit and most notably in use, reducing the attack surface and protecting against cloud compromise.
- **Integration with External Roots of Trust:** Designed to integrate with trusted hardware like Utimaco SecurityServer for critical security functions.
- **Cloud-Readiness:** Securely provision Virtual Machines, Kubernetes clusters, databases and AI pipelines on any cloud infrastructure with secrets, configs, SSH keys and TLS certs.
- **High Availability, Resilience and Elasticity:** Utilizes redundant setups in clusters to maintain uninterrupted availability, eliminate single points of failure, and support both horizontal and vertical scaling to adapt to changing workloads.
- **Identity-Based Access Control:** Enforces granular access policies based on application identity and roles, ensuring only authorized entities can access specific secrets.
- **Workload Identity Management:** Enforce granular access policies thanks to remote attestation of enclaved workloads.

enclaive x utimaco®

- **Audit Logging:** Comprehensive audit logs track all access to secrets and configuration changes, facilitating compliance and security investigations.
- **Signing/Encryption as a Service:** Provides a consistent way for applications to sign/verify and encrypt/decrypt data and code without directly managing keys.
- **Cryptographic Acceleration:** Offloads computationally intensive cryptographic operations, improving performance and scalability outside of the HSM.
- **Dynamic Secrets Generation:** Generates short-lived, on-demand secrets for applications and services, reducing the risk of static credential compromise.
- **Secret Rotation:** Automates the process of rotating secrets, minimizing the window of opportunity for compromised credentials to be exploited.



enclaive x utimaco®

Utimaco SecurityServer (Root of Trust):

Utimaco SecurityServer is a high-performance, tamper-proof Hardware Security Module (HSM) that serves as the foundational root of trust for cryptographic operations and key management. Key capabilities relevant to this integration include:

- **Secure Key Generation and Storage:** Generates and securely stores cryptographic keys within a hardened hardware environment, protected against physical and logical attacks.
- **Compliance with Security Standards:** Meets stringent security standards and certifications, such as FIPS 140-2 Level 3, ensuring regulatory compliance.
- **Tamper Evidence and Response:** Detects and responds to physical tampering attempts, safeguarding the integrity of cryptographic keys and the root of trust.
- **High Availability and Resilience:** Offers redundant configurations to ensure continuous availability and prevent single points of failure.
- **Role-Based Access Control:** Restricts access to HSM functionalities and keys based on defined roles and responsibilities.
- **Secure Secret Unsealing:** Acts as a trusted authority to securely unseal critical secrets, such as the master keys used by enclaive vHSM, ensuring that these sensitive keys are protected and accessible only under authorized conditions.
- **High-Entropy Random Number Generation:** Provides a reliable and auditable source of high-quality randomness crucial for generating strong cryptographic keys, meeting the stringent requirements of highly regulated applications.

enclaive x utimaco®

The Integration: Establishing a Secure Foundation

Integrating enclaive vHSM with Utimaco SecurityServer as the root of trust provides the following critical benefits:

Hardware-Backed Root of Trust:

Utimaco SecurityServer provides a physically secure and highly auditable foundation for critical cryptographic operations, including high-entropy random number generation and secure key storage.

Enhanced Key Security for Regulated Applications:

Leveraging the Utimaco HSM's high-entropy RNG ensures the generation of strong and unpredictable cryptographic keys required by highly regulated industries.

Secure and Auditable Secret Unsealing:

Utimaco SecurityServer acts as the trusted authority to unseal enclaive vHSM's master keys, ensuring a secure and auditable process for accessing the secrets management platform.

Multi-Layered Security:

Combining the software-level security of secure enclaves within enclaive vHSM with the hardware-level security and root of trust provided by the Utimaco HSM creates a robust defense-in-depth strategy.

enclaive x utimaco®

Simplified Management with Strong Security:

enclaive vHSM provides a centralized interface for managing secrets, while relying on the Utimaco HSM for foundational security functions like randomness and unsealing.

Increased Trust and Assurance:

Utilizing a certified HSM as the root of trust provides the highest level of assurance in the security and integrity of cryptographic operations and key management.

Compliance Alignment:

The combined solution directly addresses stringent compliance requirements related to key management, randomness, and the establishment of a strong root of trust.

enclaive x utimaco®

Key Use Cases:

Move IT Securely into the Cloud: While software applications can be migrated to the cloud, physical HSMs cannot. By integrating enclaive vHSM with the Utimaco Security Server as the root of trust in the cloud, organizations can extend their on-premises security standards to the cloud environment, ensuring seamless, compliant, and secure key management.

Bring Your Own Vault: Organizations can maintain full control of their secrets and keys, ensuring data sovereignty and compliance with data residency requirements.

Multi-Cloud and Hybrid Environments: Secure data across diverse environments with centralized key management.

Meeting Stringent Compliance Requirements: Satisfying specific regulatory requirements (GDPR, PCI-DSS, HIPAA) for strong roots of trust, high-entropy randomness, and secure key Management.

Transparent Data-in-Use Encrypted Databases: Go beyond at rest encryption and meet NIS2 and DORA data-in-use encryption requirements.

enclaive x utimaco®

Benefits of the Integrated Solution:

Scalability and Flexibility:

Support for multiple cloud environments and hybrid infrastructures.

Stronger Security Posture:

Multi-layered defense combining software enclavation and hardware security.

Increased Trust and Assurance:

Leveraging a certified HSM as the foundation.

Reduced Risk:

Leveraging a certified HSM as the foundation.

HSM Root of Trust:

Hardware-backed security for critical cryptographic functions, backed by high-entropy randomness generation and hardware-graded unsealing.

Improved Compliance:

Direct alignment with stringent regulatory requirements.

Centralized Management:

Minimizing the risk of key compromise and unauthorized access.

Conclusion:

The unique integration of **enclaive vHSM** with **Utimaco SecurityServer** as the root of trust provides a **robust and compliant solution** for organizations with demanding security requirements, particularly in highly regulated environments.
By leveraging the Utimaco HSM's high-entropy randomness and secure unsealing capabilities, coupled with enclaive vHSM's centralized secrets management and secure enclaves, organizations can establish **a truly secure foundation for protecting their most sensitive data** and meeting **stringent regulatory obligations** in cloud applications.

Ready to learn more about how enclaive vHSM and Utimaco SecurityServer (as the root of trust) can enhance your organization's security and compliance posture?

Contact us today for a personalized consultation.

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