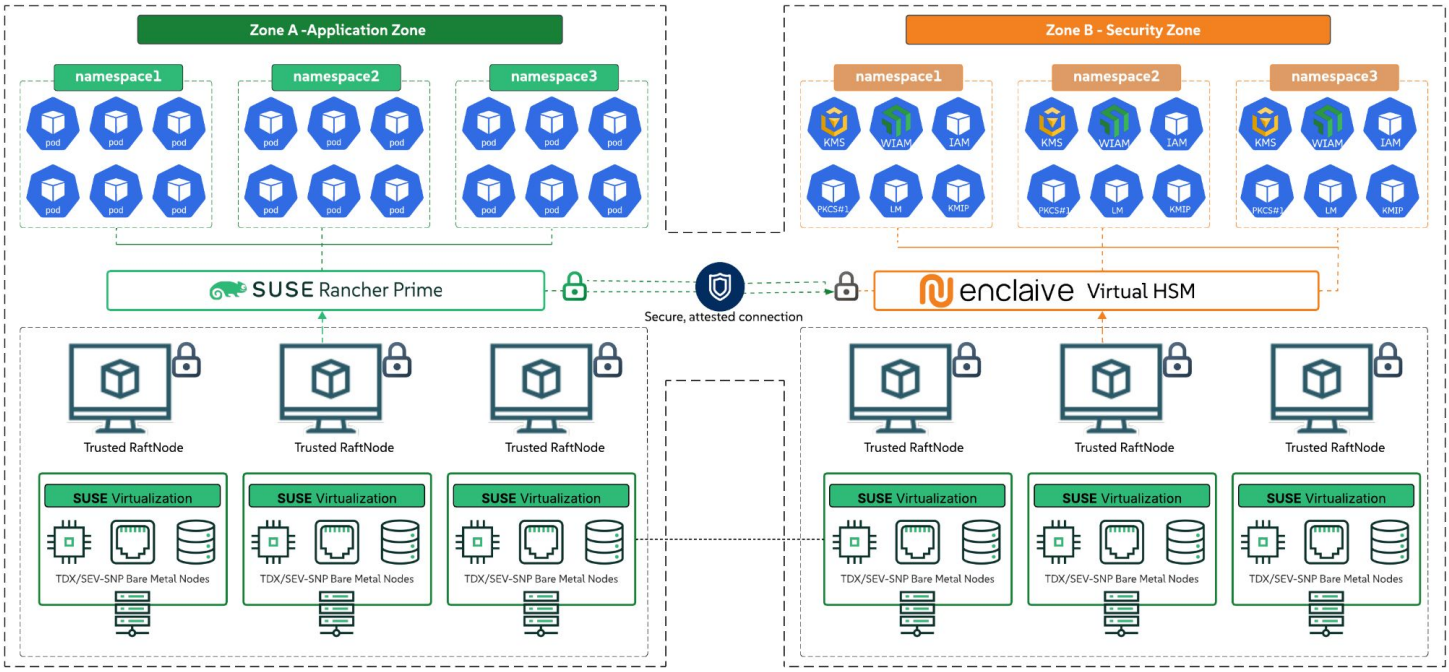
Solution Flyer

SUSE Rancher Prime and enclaive vHSM

Secure the Cloud Crypto Perimeter with Virtual HSM Capabilities

The joint solution from SUSE and enclaive—combining enclaive's Virtual Hardware Security Module (vHSM), powered by Confidential Computing, with SUSE Rancher Prime—delivers verifiable secrets sovereignty and granular security for cloud-native environments. This partnership enables European organizations to adopt the cloud with confidence



Verifiable Control and Digital Sovereignty

Customers maintain complete, exclusive, and verifiable control over their master encryption keys at scale, a cornerstone of digital sovereignty, ensuring alignment with regulatory frameworks like GDPR, DORA, and NIS2.

Seamless Integration and Agility

The vHSM integrates seamlessly into current infrastructure without requiring costly and time-consuming code modifications to existing applications.

Hardware-Grade Key Protection in a Cloud-Native Form

It provides hardware-grade key protection in a scalable, software-defined solution that fits perfectly into sovereign-cloud and multi-cloud architectures.

Zero-Trust Container Security

Leveraging Trusted Execution Environments (TEEs) and Dyneemes, it brings hardware-enforced isolation directly to the Kubernetes pod level, preventing even cluster operators and administrators from accessing or tampering with running workloads.

Open Source and Vendor-Neutral Foundation

The solution is anchored in SUSE's open-source commitment and SUSE Rancher Prime's vendor-neutral platform, avoiding proprietary lock-in and supporting long-term trust

Solution Flyer

SUSE Rancher Prime and enclaive vHSM

Secure the Cloud Crypto Perimeter with Virtual HSM Capabilities

SUSE Rancher Prime

Streamlined Kubernetes management	Simple, consistent hybrid and multi-cluster Kubernetes management with comprehensive features and intuitive UI
Trusted and secure	Centralized security, policy, and user management, secure supply chain, and trusted delivery
Enterprise lifecycle and support	Consistent releases cycles, enterprise lifecycle management, priority support and services
Freedom to choose	Support for any CNCF Kubernetes distribution, on premises, in the cloud, and at the Edge

enclaive vHSM

3D Encryption (at rest, in transit and in use)	TEE-based enclaves protect data even while being processed — inaccessible to cloud providers, admins, and third parties.
Sovereign Key Management (BYOK / HYOK)	Exclusive customer control over master encryption keys at all times — even from the infrastructure provider.
Crypto-Agility and Elastic Scaling	Software-defined HSM that scales on demand. Self-healing redundancy across multi-cloud environments
European Compliance	Built for GDPR, NIS2, DORA, and EUCS — with full audit trails.

Learn more

https://www.suse.com/

SUSE is a global leader in innovative, reliable, secure enterprise-grade open source solutions, relied upon by more than 60% of the Fortune 500 to power mission-critical workloads. We specialize in business-critical Linux, enterprise container management and edge solutions, and collaborate with partners and communities to empower our customers to innovate everywhere – from the data center, to the cloud, to the edge and beyond. SUSE gives customers the agility to tackle innovation challenges today and the freedom to evolve their strategy and solutions tomorrow.

enclaive GmbH is an award-winning deep-tech cybersecurity company headquartered in Berlin, Germany. Founded in 2022 by a team of distinguished academic researchers and seasoned cyber-industry veterans, enclaive specializes in making Confidential Computing practical and accessible for the modern multi-cloud era.

SUSE Software Solutions Germany GmbH
Frankenstraße 146 90461 Nürnberg
Germany
www.suse.com

For more information, contact SUSE at:
+1 800 796 3700 (U.S./Canada)
+49 (0)911-740 53-0 (Worldwide)