enclaive

CONFIDENTIAL COMPUTING MADE SIMPLE

Run any workload on the safest cloud ecosystem

Get Started >

CONFIDENTIAL COMPUTING
CONSORTIUM

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

enclaive shields your business in 3D with encryption in transit, at rest, and most notably in use!

- Confidential Computing is a new security paradigm, allowing to run applications in an enclave – a fully memory and persistent storage encrypted, trusted execution environment (meTEE).

- Enables the execution of ANY application in a vault/black/box/safe
  - **No change to code**
  - **No change to DevOps**
  - **No change to infrastructure**
  - **No performance penalty (+2% CPU cycles)**

- Enables more customers and reduces internal costs
  - **Move IT to the cloud and become financially agile through CAPEX-to-OPEX shift**
  - **Reduce internal IT workload with IaaS/SaaS/PaaS in contrast to expensive self-hosted services**
  - **Protect business IPs (e.g. code, data, docs) in environments managed by third parties (e.g. external devs, cloud service provider, customer's infrastructure)**
  - **Shield IT from bad actors, vulnerabilities, weak isolation of virtualization and save on security expenses**
  - **Avoid fines and liability lawsuits for data leaks/GDPR violations**
  - **Untap business cases and industry segments that have been avoiding cloud/SaaS, or where regulations put a high burden (e.g. CRITIS, finance, insurance, public, defense)**

{ Mission }

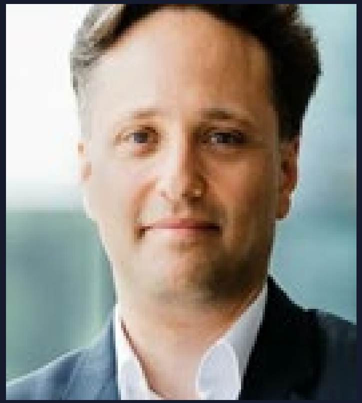
WELCOME TO ENCLAIVE

We help customers to protect data, application and business logic by providing digital safes – so called enclaves – around any workload anywhere.

{About us}

OUR Team_

Founded in 2022, enclaive is backed by experts with +100 years experience of building cutting-edge cybersecurity technologies, products and companies.



Ammar Alkazar

Ex-CIO Saarland

Dr. Rainer Baumgart

Ex-CEO Secunet AG

Dr. Sebastian Gajek

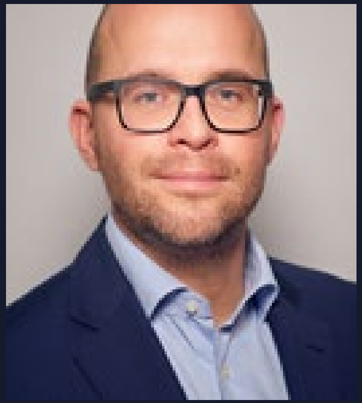
Founder & CTO

Andreas Wahlbrodt

Founder & CEO

Prof. Dr. Norbert Pohlmann

Chair of Teletrust
Advisor to ENISA

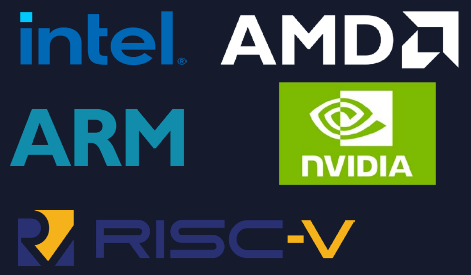


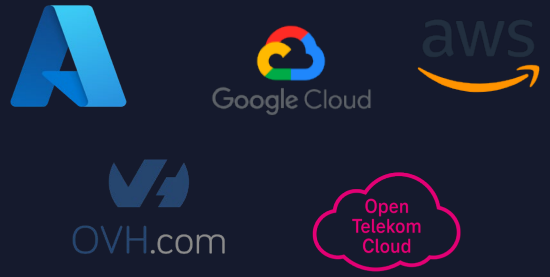
Marian Rachow

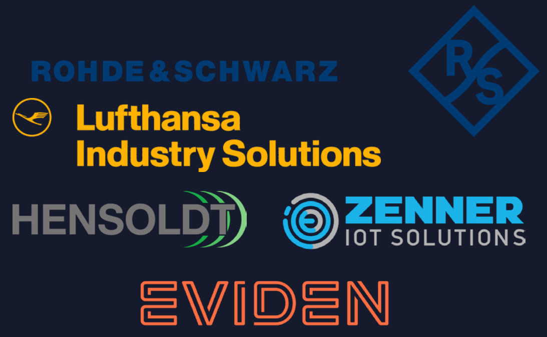
CEO Rohde & Schwarz Cybersecurity

{Partners and clients trusting us}

Strong Partnerships, available almost everywhere for Clients across Industries_







Technology Partners

Supported on leading technology today and enroute to support the leading technology platform

Infrastructure Partners

Build to run where you desire from the hyperscalers to local providers or your private Data Centre

Customers that trust us

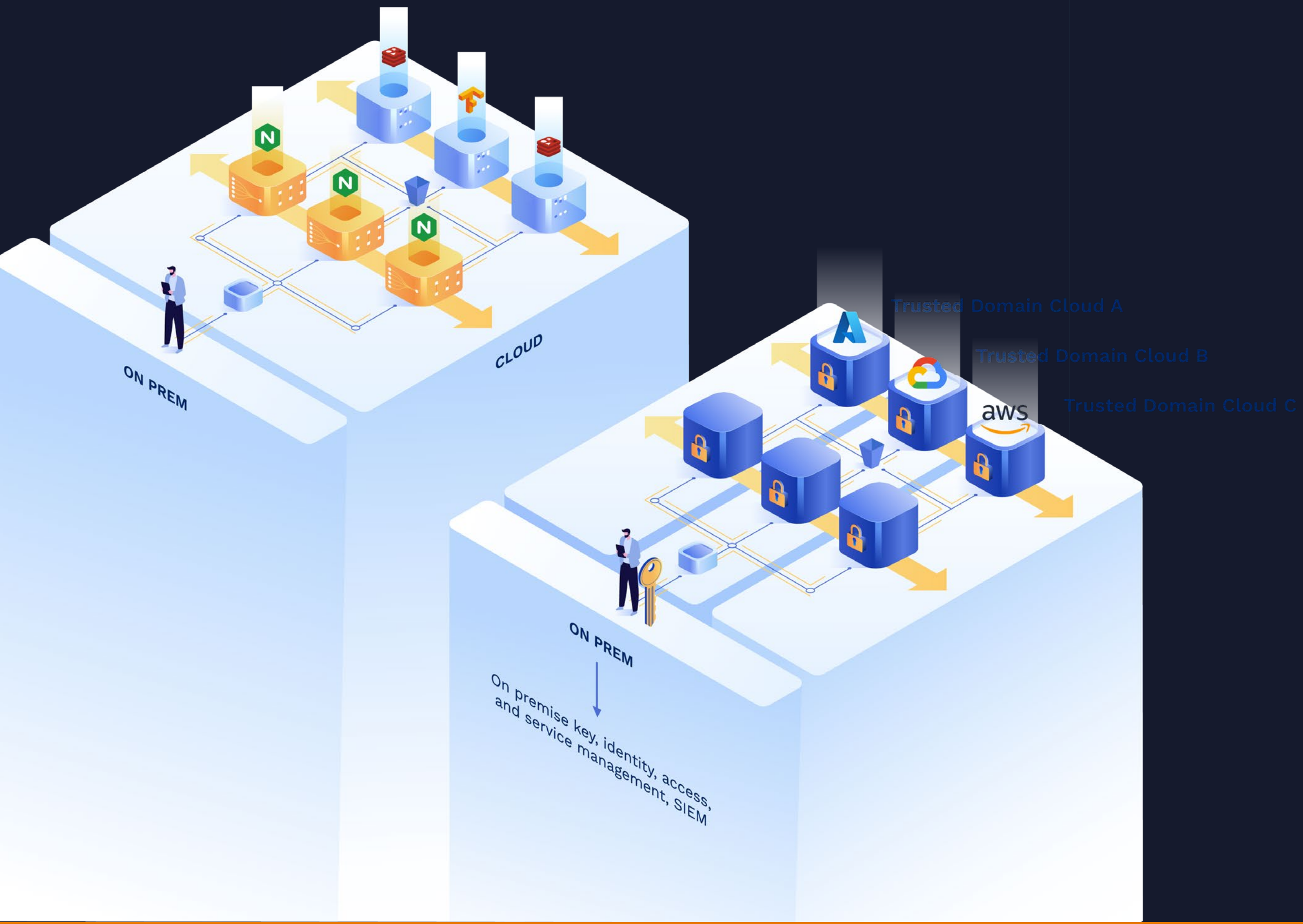
Embraced by innovative clients across industries for a wide variety of use cases

Product EMCP

Platform to run any workload on the safest cloud ecosystem

{Product}

OUR Multi Cloud Platform_



// Hardware Rooted

Trust based on hardware security element

// Software Enclaved

Workload is 3D encrypted:

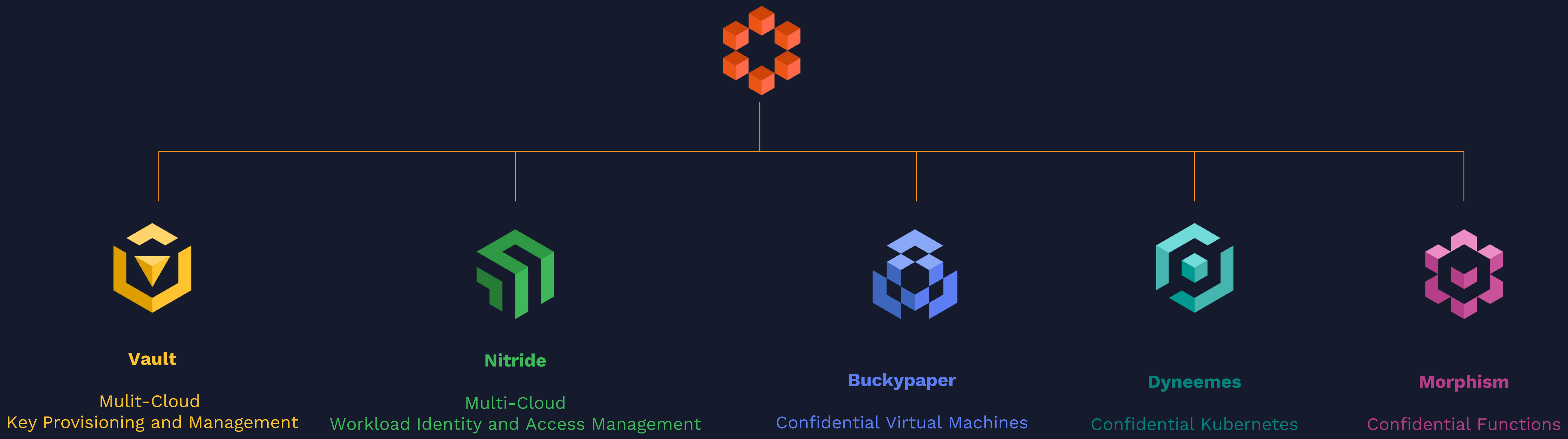
in transit, at rest **AND** in use

// Confidential Cloud

Private, hybrid and public cloud

enclaive Multi-Cloud Platform

Manage, deploy and monitor confidential workload in the mulit-cloud



Vault

Mulit-Cloud
Key Provisioning and Management

Nitride

Multi-Cloud
Workload Identity and Access Management

Buckypaper

Confidential Virtual Machines

Dyneemes

Confidential Kubernetes

Morphism

Confidential Functions

{Use Case}

Spawn in less than 10s Buckypaper_

1. Choose the CSP

Select among Azure, GCP, AWS and other cloud providers

2. Choose the Sizing

Select compute resource and Operating System

Product Vault

Secure your credentials for secrets, keys and more (vHSM)

{Overview}

OUR Vault_

// Hardware Rooted

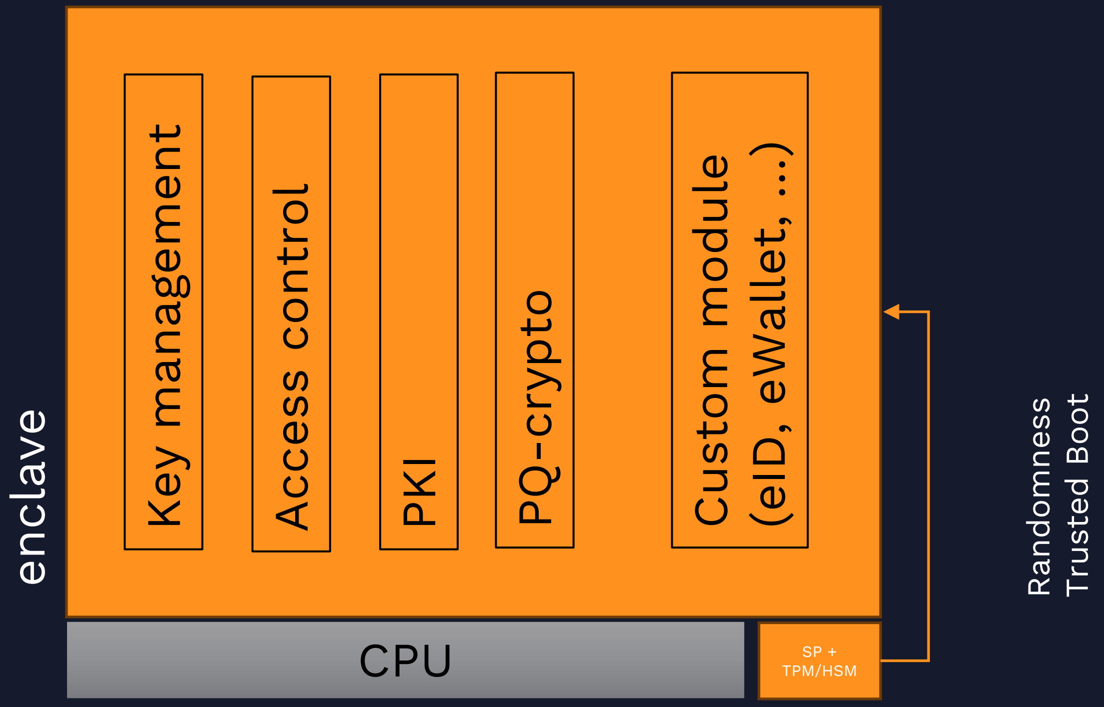
Trust based on hardware element (SP, TPM or HSM)

// Software Enclaved

Services are run-time memory encrypted

// Sealed

Persistent storage is sealed by HW to run only in ENCLAVE



No Vendor Lock

open-source software

Trust Anchor

SP, TPM or HSM

Crypto Agile

change crypto rapidly
(key lengths, PQ/isogeny)

High Performance

up to 192 cores, 8 TB RAM

High Availability

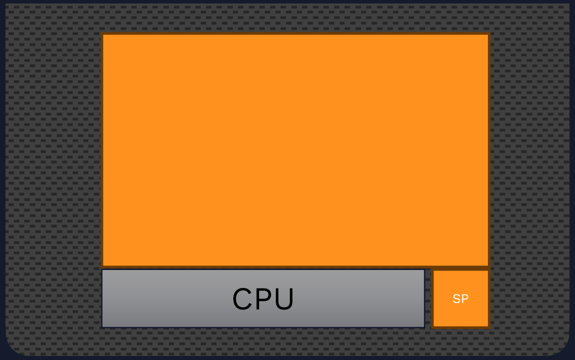
Cluster for fault-tolerant applications

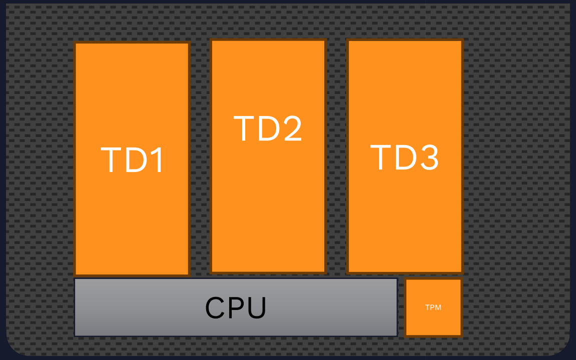
High Scalability

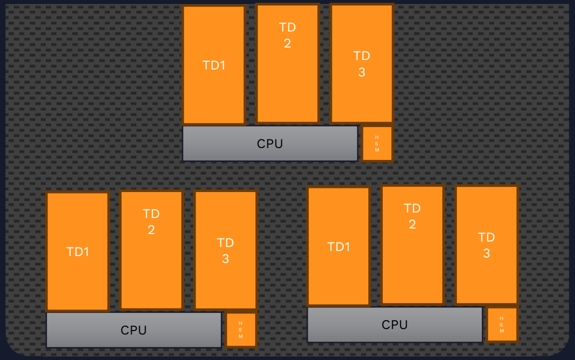
sizable to meet the right demand & costs

{Sizing}

Vault can be configured to meet any demand _







// Single Use

entry-size product replacing a commodity HSM

// Trusted Domains

share resources among different departments/ organizations

// Cluster

achieve high-availability with redundant clusters

{ Comparison }

HSM vs Vault_

6 reasons to choose Vault_

1. Budget-friendly as underlying HW is a commodity
2. Customizable as an overlying SW is an enclave
3. Reduced maintenance
4. Future-ready (eID, eWallet, Blockchain)
5. Cloud-ready (manage VM, K8s keys, and secrets)
6. Scales dynamically when you need it

Product Nitride

Workload Identity and Access Management (WIAM)

{Overview}

OUR Nitride_

// Hardware Identity

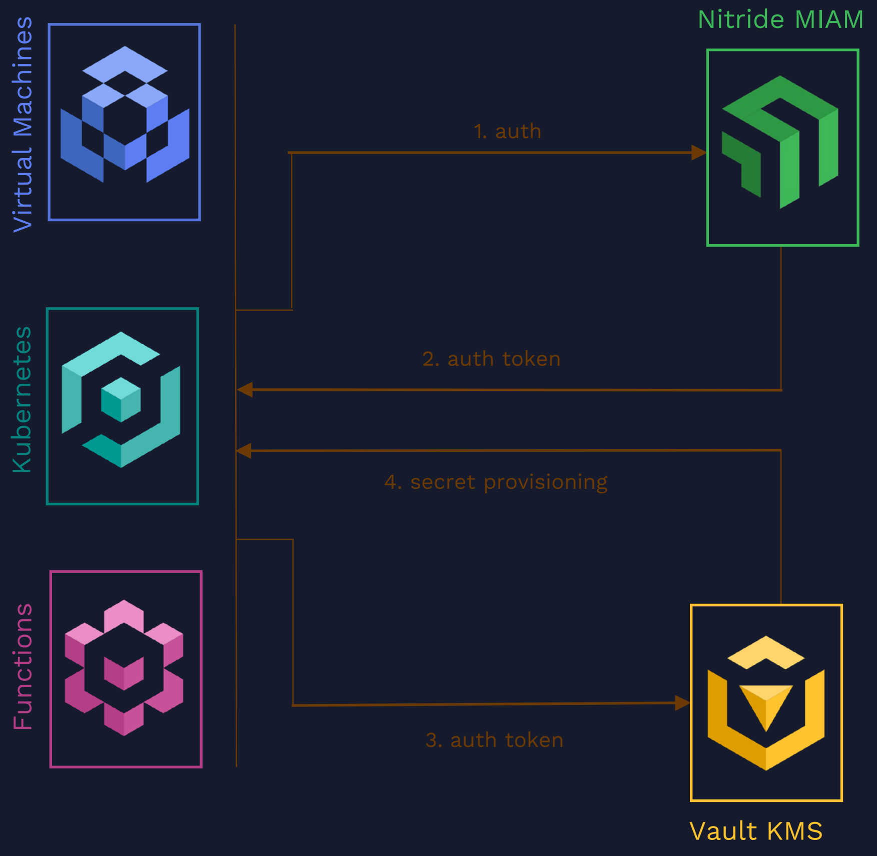
Machines have an identity rooted in the PKI of the CPU vendor

// Verification

Nitride verifies machine root-of-trust (aka attestation)

// Access Control

Nitride manages access to Vault and other services



Attestation

From CPU Vendor to Application

Authorization

Machine-based Access Control

Life Cycle Management

Manage lifetime of attestations and Access

High Performance

Up to 192 cores, 8 TB RAM

Single-Sign On

Issue auth tokens

High Scalability

Dynamically sizable upon demand

{ Comparison }

IAM vs Nitride_

5 reasons to choose Nitride_

1. Automate workload/endpoint/app authentication
2. Automate CSP authentication
3. Automate CSP compliance tracking
4. Define finer-grained access to apps/services
5. Scale dynamically when you need it

Product Buckypaper

Always Encrypting Virtualization without worries

{Overview}

OUR Buckypaper_

// Always encrypted VMs

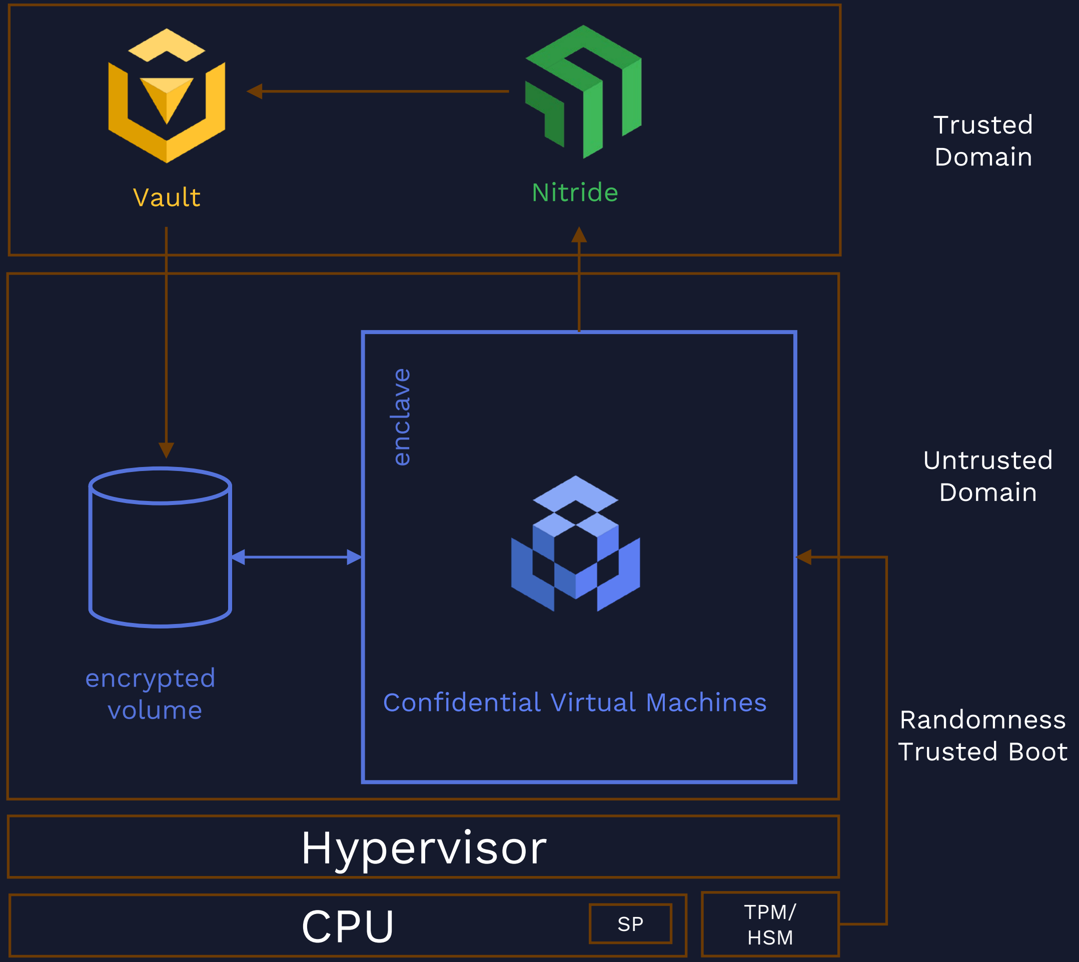
At any time virtualized workload is encrypted, authenticated and integrity protected

// Always encrypted Discs

At any time, persitance is encrypted and bound to VM

// Vertical Isolation

Protection against compromised VMs



Supported Hypervisor

KVM, VMWare, Hyper-V

OS Virtualization

Linux, Windows, legacy 16/32bit software

Life Cycle Management

Compatible with any VM

Run-Time Security

Hardware graded encryption

At Rest Security

Resizable Disc Encryption

Live Migration

Move VMs to any datacenter

{ Comparison }

VMs vs Buckypaper_

6 reasons to choose Vault_

1. 3D encrypted virtualization
2. Negligible performance overhead (+2% CPU)
3. Shield customer against compromised VMs on shared Hardware
4. Shield customer against untrusted CloudOS
5. Shield customers against physical compromise
6. Increase significantly TOMs (GDPR, NIS2, HISPA)

Product Dyneemes

Confidential Kubernetes anywhere

{Overview}

OUR Dyneemes_

// Always encrypted K8S

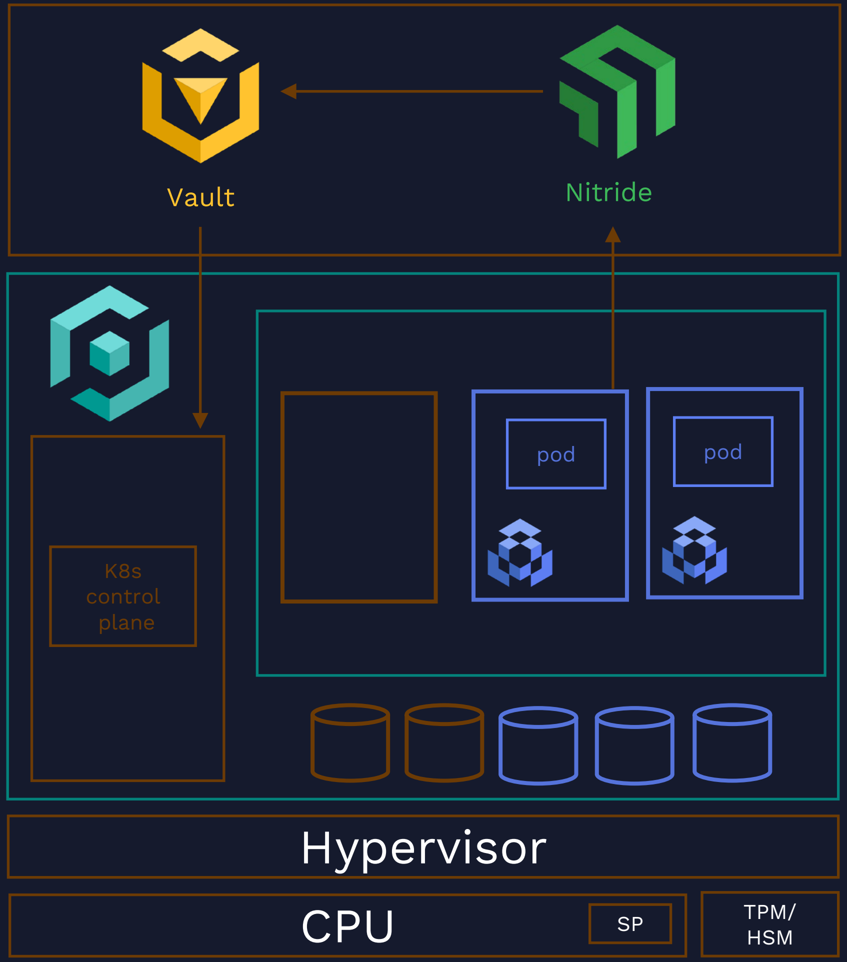
At any time nodes are encrypted, authenticated and integrity protected

// Always encrypted Discs

At any time, storage is encrypted

// Ease of Use

Use K8s as usual including plugins, sidecars. You do not notice the difference.



Hardware graded Security

Intel, AMD, ARM

Compatible

K8s, K5s, K1s, OpenShift

Zero Overhead

Negligible 2% more CPU cycles

In Use Security

Hardware graded memory encryption

At Rest Security

Resizable Disc Encryption

In Transit Security

End-point workload authentication with remote attestation

{ Comparison }

K8s vs Dyneemes_

6 reasons to choose Dyneemes_

1. Avoid container escalation
2. Negligible performance overhead (+2% CPU)
3. Shield customer against compromised VMs on shared Hardware
4. Shield customer against untrusted CloudOS
5. Shield customer against physical compromise
6. Increase significantly TOMs (GDPR, NIS2, HISPA)

Product Morphism

Serverless Always Encrypted Functions

{Overview}

OUR Morphism_

// Always encrypted K8S+knative

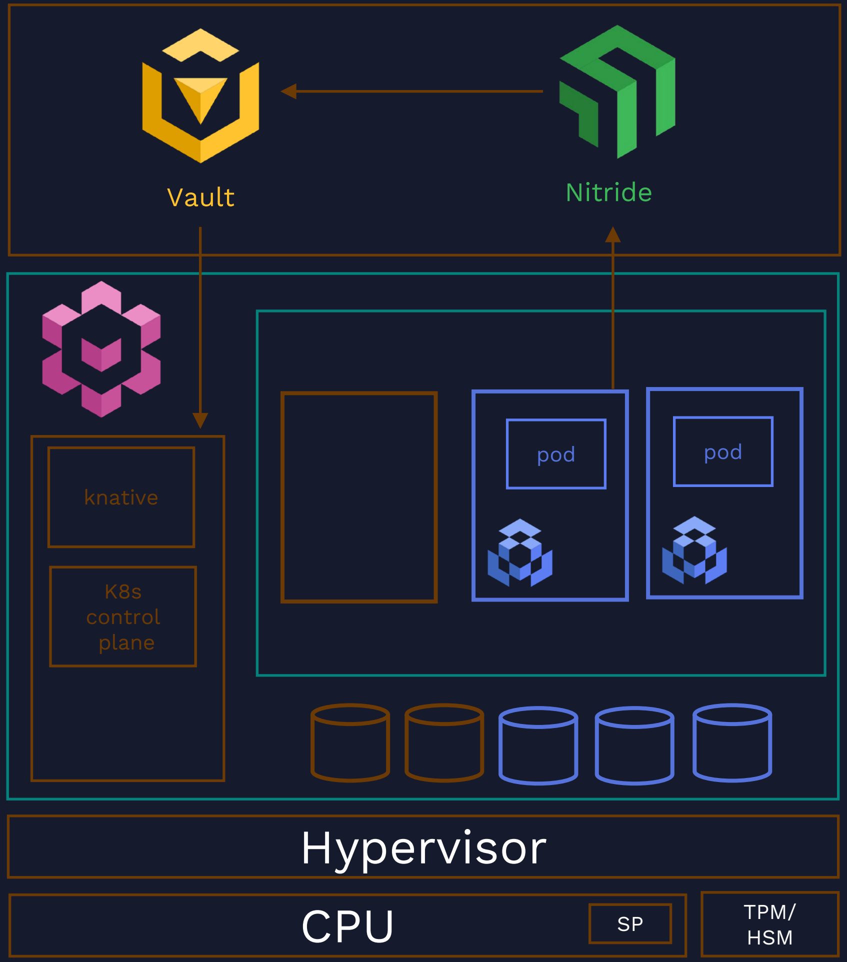
At any time nodes are encrypted, authenticated and integrity protected

// Always encrypted Discs

At any time, storage is encrypted

// Ease of Use

Use K8s as usual including plugins, sidecars. You do not notice the difference.



Hardware graded Security

Intel, AMD, ARM

Compatibility

Knative Kat Container

Life Cycle Management

Compatible with any Kubernetes tool

3D Security

Hardware graded memory volume and endpoint encryption

Zero Overhead

Negligile 2% CPU cycles

In Transit Security

Cluster cert provisioning via Vault/vHSM

{ Comparison }

Lambda vs Morphism_

6 reasons to choose Morphism_

1. Avoid container escalation
2. Negligible performance overhead (+2% CPU)
3. Shield customer against compromised VMs on shared Hardware
4. Shield customer against untrusted CloudOS
5. Shield customer against physical compromise
6. Increase significantly TOMs (GDPR, NIS2, HISPA)

Pricing Table

CHOSE YOUR PLAN_

Self Hosted	Managed
Licence	Pay as you need
Support	Support
CHOOSE	CHOOSE

{Contact}

CONTACT US_

☎ Phone
+49 30 233292970

E-mail
contact@enclaive.io

Address
Chausseestr. 40

10115 Berlin

enclaive

CONFIDENTIAL COMPUTING

MADE SIMPLE

Get Started ›

THANK YOU