CONFIDENTIAL CLOUD SECURITY

The Secure VMware Exit.

A migration framework for regulated and sensitive workloads that need hardware-enforced isolation, customer-held keys, and proof that administrators cannot access data in use.

Confidential Computing | Customer-held Keys | Attestation | Multi-Cloud · Zero Trust

PAGES

06 / inc. cover

READING TIME

~ 8 min

CONFIDENTIAL CLOUD SECURITY

The Secure VMware Exit.

A migration framework for regulated and sensitive workloads that need hardware-enforced isolation, customer-held keys, and proof that administrators cannot access data in use.

Move regulated workloads without weakening the security model.

VMware exit is not only a platform migration. For payment systems, ledgers, patient repositories, trading engines, industrial systems, and citizen identity platforms, the security architecture has to move with the workload.

Classify

Rank workloads by data sensitivity, regulatory scope, dependencies, and target platform fit.

Attest

Release keys and secrets only to workloads that prove identity and integrity.

Scale

Apply one control model across confidential VMs, Kubernetes, sovereign cloud, and hybrid estates.

Executive outcome

Reduce VMware dependency and dual-run cost while keeping Tier 1 and Tier 2 workloads protected by confidential computing, sovereign key custody, and automated compliance evidence.

Primary next step

Run a workload assessment against the top 15–25 VMware applications and select the first 2–5 regulated workloads for a controlled first wave.

WHY MIGRATIONS STALL

Cost pressure is visible. Security readiness decides the timeline.

Dual-run cost expands

VMware and the target platform operate in parallel while teams migrate, validate, and wait for security approval. If sensitive workloads cannot move, the expensive source platform stays alive longer than planned.

One target will not fit the estate

Most organizations need all three paths: alternative VMs for legacy workloads, Kubernetes for modern services, and public or sovereign cloud where certifications, geography, and scale matter.

Security constraints follow the workload.

Protect data in use

Encryption at rest and in transit does not protect plaintext while it is processed in memory.

Remove privileged access

Platform operators, cloud administrators, and cluster administrators should not inspect regulated workload memory.

Generate evidence

Auditors increasingly expect proof of key custody, workload integrity, policy enforcement, and access controls.

Practical workload tiers

TIER	WORKLOAD TYPE	MIGRATION IMPLICATION
Tier 1	Restricted data, customer-critical systems, board-level risk	Move with confidential compute and customer-held keys.
Tier 2	Confidential data and compliance-mandated processing	Use confidential Kubernetes if containerizable; otherwise confidential VMs.
Tier 3	Internal operations with policy controls	Standard cloud or Kubernetes may be sufficient; use confidential compute where isolation matters.
Tier 4	Public or low-sensitivity systems	Move to standard infrastructure.

For regulated estates, migration speed depends on whether the new platform can satisfy the security posture the CISO, auditors, and regulators already require.

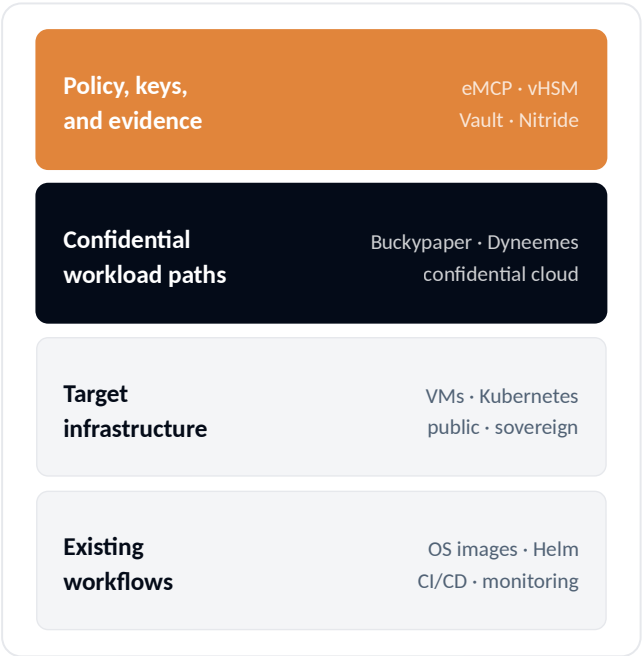
PLATFORM-INDEPENDENT CONTROLS

Confidential computing above the infrastructure choice.

enclaive sits above alternative hypervisors, Kubernetes, public cloud, sovereign cloud, and hybrid estates. The infrastructure provider does not need to be in the trust path for sensitive data.

Why native confidential compute is not enough

- Sovereign keys must remain under customer control, outside the provider key hierarchy.
- Secrets should only be released after workload identity and integrity are verified.
- The same controls must work across VMs, Kubernetes, cloud, and sovereign infrastructure.
- The security investment should not recreate single-vendor lock-in.



How enclaive maps to migration paths

Confidential VMs

Buckypaper protects legacy, licensed, monolithic, or OS-dependent workloads without forcing application or operating system changes.

Confidential Kubernetes

Dyneemes lets pods run in hardware-isolated enclaves while teams keep using Kubernetes tooling such as kubectl, Helm, and CI/CD.

Key and policy foundation

vHSM, Vault, Nitride, and eMCP provide sovereign key custody, secrets governance, attestation, policy control, and evidence.

Four-phase migration path

1. **Assess and classify workloads**
   Build a usable migration backlog from CMDB, vCenter inventory, application portfolio, and discovery conversations.
2. **Build the security foundation**
   Establish customer-held keys, secrets governance, attestation, access policy, audit trails, and HSM coexistence.
3. **Migrate the first wave**
   Move 2–5 Tier 1 or Tier 2 workloads, validate performance and key release, then cut traffic over.
4. **Scale across the estate**
   Enable “no attest, no key” for sensitive workloads while VM, Kubernetes, and cloud paths progress in parallel.

MIGRATION DECISIONS

Choose the target path by sensitivity and architecture.

WORKLOAD CONDITION	RECOMMENDED PATTERN	REQUIRED FOUNDATION
Regulated and not containerizable	Confidential VM on alternative infrastructure or cloud	Customer-held keys, attestation-gated secret release, policy, audit evidence
Regulated and containerizable	Confidential Kubernetes	Same control model across clusters and clouds
Sensitive but not formally regulated	Confidential VM or Kubernetes based on architecture	Workload identity, key governance, access policy
Internal, low sensitivity	Standard Kubernetes or cloud services	Policy controls and monitoring
Commodity	Standard infrastructure	Baseline platform controls

Workshop output

WORKLOAD	TIER	PATH	PRIORITY
Core ledger	Tier 1	Confidential VM	P1
KYC / AML	Tier 2	Confidential Kubernetes	P1
Risk engine	Tier 2	Confidential Kubernetes in cloud	P2

Success metrics

- Time to first secure workload: less than 12 weeks from kickoff.
- Privileged access eliminated for 100% of Tier 1 and Tier 2 workloads.
- Customer-held key coverage for 100% of Tier 1 and Tier 2 workloads.
- Audit-ready evidence generated in hours, not weeks.
- Migration throughput of 3–5 workloads per four-week cycle.

TCO categories to include

VMware renewal | Dual-run duration | Target platform unit cost | Infrastructure consolidation | Security integration | Operational overhead | HSM hardware reduction | Sovereign cloud premium | Audit preparation | Regulated analytics & AI economics

Book a workload assessment.

Run the Phase 1 assessment against the top 15–25 VMware applications, identify the first regulated migration wave, and define the Phase 2 security foundation for keys, attestation, and evidence.

Book Assessment →

Make the cloud the safest place for your digital business.

enclaive delivers a universal multi-cloud platform built on Zero Trust principles — empowering organizations to deploy regulated workloads across any infrastructure without giving up sovereignty, evidence, or control.

OFFICE

enclaive GmbH
Philipp-Keim-Str. 1
D-65719 Hofheim a. Ts.

CONNECT

contact@enclaive.io
www.enclaive.io

NEXT STEP

Book a workload assessment workshop with our solutions team.