KVM / DR

SOLUTION BRIEF

DISASTER RECOVERY FOR KVM

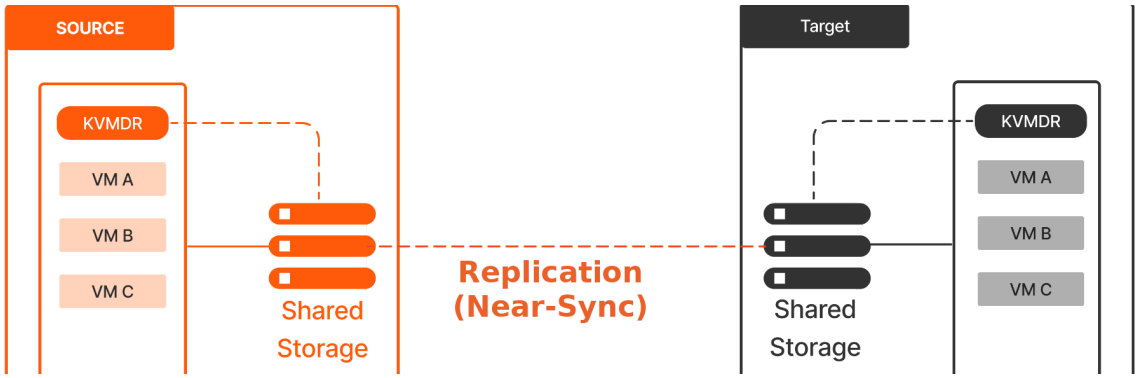
Continuous DR. In flight ransomware detection. Instant failover.

Native to KVM based hypervisors — replication, orchestration, AI powered archival and DR automation.

KVMDR replicates KVM workloads continuously via change block tracking, orchestrates the full **Protect → Failover → Reverse Protect → Fail Back** lifecycle, and analyses the replication stream for ransomware as data moves, flagging suspicious write patterns and pointing to the cleanest pre encryption recovery point. All on premises, air gap capable; replicated VM data never leaves the appliance.

~0 RPO, continuous	Instant failover	In flight detection
CBT VS HOURS BETWEEN BACKUPS	RUN AT SPEED, NOT FROM BACKUP	LIVE STREAM SCAN · AUTO RECOVERY

HOW REPLICATION WORKS



Per site Manager pair orchestrates change block tracking replication from source to target over a near sync journal.

AI NATIVE BY DESIGN

In flight detection.

ML entropy analysis inspects in stream blocks as data moves, identifying encryption activity live: entropy jumps, rewrite bursts, mass renaming.

AI triage and clean point recovery.

AI scores each alert, separates noise from genuine encryption activity, and pinpoints the cleanest recovery point before the attack. One step restore.

Natural language assistant.

Ask about protection status, recovery points, jobs and alerts in plain English. Answers are grounded in live system state, and the same interface drives archive search.

Offline or cloud AI.

Run fully offline against local models for isolated sites, or connect cloud LLMs. Only operational metadata is used; replicated VM data never leaves the appliance.

One platform, four disciplines. KVMDR unifies DR, orchestration, automation and archive in a single appliance: continuous replication with instant failover, sequenced runbooks that orchestrate whole application recovery, automation that drives protection, drills and reporting hands free, and an AI searchable archive for long term retention and one step restore.

KVM / DR

SOLUTION BRIEF

CROSS HYPERVISOR DISASTER RECOVERY

One DR plane across Proxmox, OLVM, oVirt and RHV.

Estates are no longer single vendor. KVMDR treats the hypervisor as a detail: protect a workload on one platform and recover it on another, with conversion handled automatically at failover. Proxmox to OLVM, oVirt to Proxmox, or like for like. One product, one licence, one workflow.

Replicate across hypervisors

Protect on one platform, recover on another. Replication behaves identically regardless of vendor.

- Proxmox VE to oVirt / OLVM / RHV, or the reverse.
- Conversion is automatic at failover.
- DR drills validate the result without touching production.

Migration without lock in

The same engine that powers DR doubles as a migration path. Fail over once, verify, and stay. A supported route between KVM platforms, with no separate migration SKU.

One console for mixed estates

A single management plane discovers, protects and recovers workloads across Proxmox, OLVM, oVirt and RHV clusters side by side. Policies, reporting and audit stay uniform across platforms.

Same intelligence on every platform

In flight ransomware detection, AI triage and clean point recovery operate on the replication stream itself, so every protected platform gets identical protection. Fully offline and air gap capable.

Pre recovery simulation

Rehearse a failover before committing: measure real RTO and verify each VM's state at a chosen point in time, in an isolated bubble network. Production untouched.

Platform: Proxmox VE 8.x and 9.x · oVirt / OLVM 4.5 and oVirt / RHV / OLVM 4.4 (Advanced Virtualization) · Debian 12 / EL8 / EL9 hosts · QEMU 5.2+ with libnbd.

Storage: NFS, iSCSI, Fibre Channel, cloud object storage as filesystem · **Deploy:** one Manager appliance per site; host components pushed to hypervisors over SSH.

See in flight detection and clean point recovery on your own workloads → **sales@kvmdr.ai**