KVM / DR

BEST PRACTICES GUIDE

# Ransomware Recovery Playbook

A field-tested approach to detecting, containing, and recovering from ransomware on KVM-based virtualization — built around immutable recovery points and a clean, verified restore.

Published by **KVMDR** · kvmdr.ai · 2026

A vendor-neutral guide for infrastructure and security teams

EXECUTIVE SUMMARY

# Detection buys time. Recovery ends the incident.

Ransomware has shifted from encrypting endpoints to crippling the virtualization layer — and modern campaigns deliberately target the backups and recovery copies an organization would use to avoid paying. For KVM estates moving mission-critical workloads onto oVirt, RHV, and OLVM, the question is no longer whether protection copies exist, but whether a clean, uncompromised one can be **found and restored quickly**.

This playbook frames ransomware resilience as a recovery discipline, not only a detection problem — moving from preparation, through detection and containment, to a verified, pre-encryption restore. It is written to be useful whatever tooling a team chooses.

## THE THREE OUTCOMES THAT MATTER

**An untouchable point**
A recovery point that predates the attack and can't be altered for a defined retention period.

**Confidence it's clean**
The means to pinpoint the last good copy fast — by signal, not trial-and-error restores.

**A rehearsed restore**
A tested path to recover and validate in isolation, then return without reinfecting.

The sections that follow take each in turn — prepare, detect and contain, then recover — so the capability is built methodically rather than assembled during an outage.

WHY NOW

# The threat is accelerating

Ransomware was already growing. AI has changed its slope — lowering the skill needed to attack and the time needed to do it. The numbers from 2025 make the trend hard to ignore.

**+58%**

Growth in claimed ransomware victims in 2025 — the most active year on record, with over 7,500 organizations posted to leak sites.

GuidePoint Security, 2025

**44%**

Share of breaches that involved ransomware in 2025 — up roughly 37% year over year, and present in 88% of breaches at small and mid-sized businesses.

Verizon 2025 DBIR

**+49%**

Rise in active ransomware groups, as AI and leaked tooling lower the barrier for smaller, transient operators.

IBM 2026 X-Force Index

**~44 days**

Median time from a vulnerability's disclosure to a working exploit in 2025 — down from over 700 days in 2020.

Industry threat reporting

## AI LOWERS THE BARRIER

Generative and agentic AI now drafts convincing phishing, surfaces exploitable weaknesses, and assembles tooling that once demanded skilled operators. CrowdStrike's 2025 survey found **85% of organizations believe traditional detection is becoming obsolete** against AI-enhanced attacks — more attackers, moving faster than detection alone can keep pace with.

**Why this raises the stakes for recovery.** Among organizations that paid a ransom, 83% were attacked again and 93% had data stolen anyway (CrowdStrike, 2025). Paying is not protection. The control that scales with the threat is a clean, immutable recovery point you can restore quickly.

PREPARE

# Resilience is built before the attack

Every option you have during an incident was decided beforehand. The following controls determine whether recovery is a routine operation or an improvisation under pressure.

PRE-INCIDENT CHECKLIST

### Put these in place now

- ✓ Immutable recovery points — tamper-proof for a defined retention window, so a clean copy survives
- ✓ Retention depth that exceeds attacker dwell time — campaigns often wait days or weeks before triggering
- ✓ Change-rate monitoring with a known baseline, so anomalies stand out immediately
- ✓ An isolated recovery network for testing and restore, separate from production
- ✓ Least-privilege access to the DR control plane and recovery storage
- ✓ A written, rehearsed recovery runbook with named owners
- ✓ Regular non-disruptive recovery tests that prove restores actually work

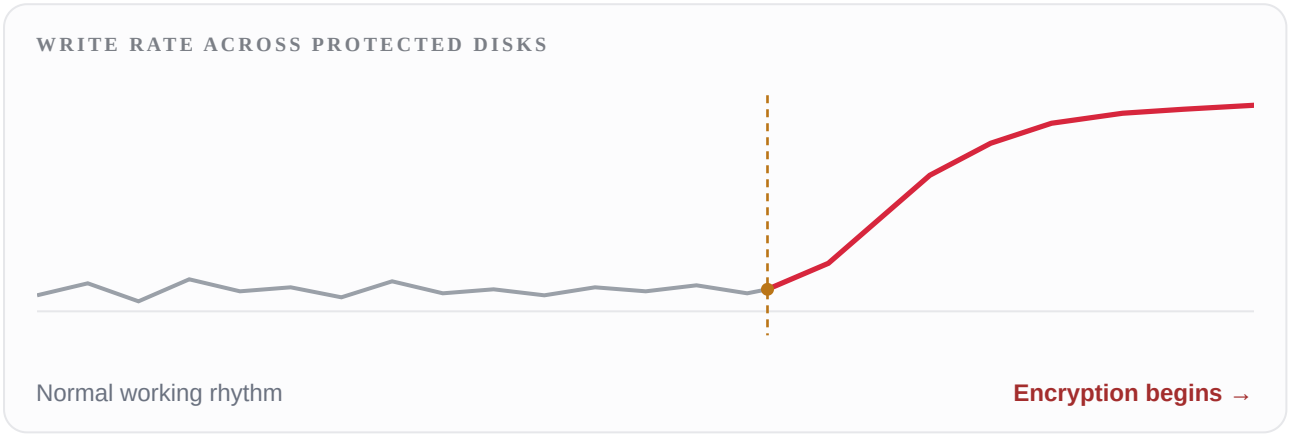
TEST WHAT YOU WILL ACTUALLY RESTORE

A recovery point is only proven once it has been restored. Schedule non-disruptive tests that bring a recent point up in isolation, confirm the workload boots and its data is intact, and rehearse the exact runbook the team will follow under pressure — including who decides, who executes, and how success is verified.

DETECT & CONTAIN

# Catch it early, preserve what’s clean

Bulk encryption produces a distinctive signature in a replication stream long before a human notices locked files. A protection layer that watches *how* data changes — not just that it changed — can surface an attack while there is still a clean point to fall back to.




## SIGNALS TO WATCH

- **A change-rate spike.** Sudden, sustained, and across many disks at once.
- **Deltas that stop compressing.** Encrypted data is effectively random, so a compression ratio jumping toward 1.0 is a strong, early red flag.
- **Correlated change** in user-data regions across unrelated workloads simultaneously.

## FIRST ACTIONS

- **Preserve, don’t overwrite.** Protect existing immutable points and extend retention — don’t let healthy points age out mid-incident.
- **Isolate.** Contain affected hosts and segments to slow lateral spread.
- **Mark the timeline.** Record the first anomalous cycle; it bounds the search for the last clean point.
- **Hold off on failover** that would simply replicate the encryption to the recovery site.

RECOVER

# A step-by-step path to clean restore

01 **Locate the last clean point.** Work backwards from the first anomalous cycle to the most recent point that predates the change-rate spike.

02 **Restore into isolation.** Bring that point up in an isolated sandbox on the recovery network — never directly into production.

03 **Validate.** Confirm the workload boots, data is intact, and no encryption artifacts are present before trusting it.

04 **Re-IP and stage.** Re-address recovered workloads for the recovery network and bring consistency groups online in dependency order.

05 **Cut over deliberately.** Promote the validated environment, keeping the compromised primary preserved for forensics.

06 **Recover forward, resume protection.** Once stable, re-establish replication so the restored site is protected again.

## AFTER THE INCIDENT

Treat the compromised primary as evidence: preserve it for forensics, rotate credentials and keys, close the entry vector, then rebuild and re-protect. Capture what worked and what slowed you down in the runbook while it is still fresh — the next drill should be faster than this one.

CONCLUSION

# The goal is a clean restore, fast

Ransomware resilience is ultimately measured by one outcome: how quickly an organization can stand up a verified, pre-encryption copy of its workloads. Detection and containment matter because they protect that copy and narrow the search for it — but recovery is what ends the incident.

Teams running oVirt, RHV, and OLVM can put this discipline in place today: immutable recovery points with adequate retention, change-rate anomaly detection, an isolated recovery path, and a rehearsed runbook. The time to build it is before the alert, not during it.