

# GuestKit

Offline VM disk intelligence, diagnostics, and repair in pure Rust.

6

DISK FORMATS

5

SECURITY PROFILES

18

TUI VIEWS

80K

RUST LOC

## Client overview

GuestKit gives teams a way to understand a VM image without booting it, which matters during migration validation, root-cause analysis, security review, and remediation planning.

## Primary audience

Migration engineering, incident response, platform reliability teams

- Use this when a client asks how to understand or repair a guest image before boot.
- Position it as the safest inspection layer for at-risk, failed, or compliance-sensitive disk images.

# Why Zyvor AI Labs

Platform-first infrastructure modernization without vendor lock-in.

## Mission

Zyvor AI Labs builds HyperSDK Platform to make VM migration, lifecycle control, and infrastructure portability predictable, repeatable, and low risk.

- Open standards over proprietary lock-in: KVM, libvirt, and KubeVirt.
- Enterprise-first design with APIs, auditability, and operational discipline.
- A single suite spanning migration, operations, and infrastructure governance.

## Why clients engage

Customers engage Zyvor when they need one operating narrative across migration, virtualization, platform operations, observability, and infrastructure modernization.

- VMware exit and cloud cost pressure need a real operating plan, not point tooling.
- Migration projects now have to connect directly to day-2 platform operations.
- Leadership teams want one portfolio story they can scale over time.

# Where GuestKit fits in the portfolio

Each product solves an immediate problem, but gains more value when positioned inside the broader HyperSDK Platform story.

SUITE ALIGNMENT	WHAT THAT MEANS IN CLIENT TERMS
Fit 1	Acts as the inspection and diagnosis layer alongside hyper2kvm conversion workflows.
Fit 2	Useful independently for hypervisor teams that need safer disk forensics and remediation evidence.
Fit 3	Bridges migration engineering, operations, and security review teams with the same source-of-truth artifact.

# GuestKit

Offline VM disk intelligence, diagnostics, and repair in pure Rust.

GuestKit gives teams a way to understand a VM image without booting it, which matters during migration validation, root-cause analysis, security review, and remediation planning.

6 disk formats

5 security profiles

18 TUI views

80K Rust LOC

## Call framing

- Use this when a client asks how to understand or repair a guest image before boot.
- Position it as the safest inspection layer for at-risk, failed, or compliance-sensitive disk images.

## Why it matters

- Shortens diagnosis time for failed migrations and broken guest images.
- Supports pre-cutover validation without starting workloads.
- Produces structured artifacts for engineering and audit teams.

## What it does well

- Partition, filesystem, bootloader, network, and OS inspection.
- Actionable repair plans and reports.
- Compliance-oriented export formats for review workflows.

## Best-fit clients

- Migration programs with strict validation requirements.
- Incident response teams handling failed guest boots.
- Security and compliance reviews around offline images.

# Recommended follow-through

Use this deck to align stakeholders, then move quickly into a tailored technical session.

## Recommended next moves

- Run GuestKit against a failed or at-risk image from the client environment and review the generated fix plan.
- Follow with disk-level remediation demonstrations and migration deep dives.

## Discussion prompts

- What first-wave problem is GuestKit solving in the target environment?
- Which teams own the operational outcome after rollout?
- What proof point or demo would shorten the path from interest to design review?