AI RECOVERY ASSURANCE · AI AUTORESCUE

AI Cyber Orchestrator for ultra-fast ransomware recovery.

Clean operations in minutes, not days. Cybersnap.io is building the AI Recovery Assurance layer for ransomware recovery. The platform sits close to the primary production environment, where the strongest recovery evidence lives, and turns production snapshot history into fast, evidence-based recovery decisions. When ransomware hits, the business does not only need backups. It needs to know what can safely resume now.

Backup and DR remain important, but they can take hours or days. Production snapshots can bring workloads back in minutes, but only if the organization can prove which snapshot is clean, usable, and safe. **Cybersnap.io reads production evidence, inspects snapshot history, validates recovery candidates, and orchestrates the safest path back to operation.** At the center is the AI Cyber Orchestrator. It coordinates specialized cyber AI agents across production evidence, snapshot history, ransomware indicators, sandbox validation, and recovery confidence scoring. Each agent performs a focused task. The orchestrator turns their findings into one decision: what can safely resume now.

> Born from high-pressure Israeli government recovery environments, **Cybersnap.io** became an AI Cyber Orchestrator for ultra-fast ransomware recovery. Built with elite Israeli cyber-intelligence expertise, Cybersnap.io now gives enterprises access to recovery thinking usually reserved for national security environments: clean, verified production recovery in minutes instead of days.

THE AI AUTORESCUE AGENTS

01 — Retrospective Threat Discovery
Looks back through production snapshot history after an attack is detected. Identifies when suspicious behavior began, which workloads show signs of compromise, and which recovery points remain clean candidates.

02 — Recovery Isolation Guidance
Guides what should not be brought back, what requires investigation, and which recovery candidates should be isolated before production resumes. Focused on safe recovery in the primary production environment.

03 — Ultra-Fast Rescue & Validate
Validates candidate recovery points in an isolated environment, runs usability and integrity checks, and confirms clean recovery candidates. Clean, verified production recovery in minutes instead of days.

04 — Recovery Decision
Coordinates the evidence, ranks clean recovery candidates, produces confidence signals, and determines what is safe to resume. This is the core decision layer.

05 — Prove & Prepare
Proves recovery readiness, validates clean restore candidates, and prepares the organization for a safe recovery event.

INPUTS · RECOVERY EVIDENCE

01 · PRIMARY PRODUCTION EVIDENCE
Production snapshots and scan results
Storage evidence, ransomware indicators, anomaly signals, validation outputs, and recovery history.

02 · RECOVERY CANDIDATES
Workloads and restore points
Tested close to the primary production environment before the business resumes operations.

03 · CLEAN VALIDATION
Inspected, isolated, validated
Candidate restore points are inspected, isolated, and validated before they are trusted.

→

OUTPUT · AI AUTORESCUE

CYBERSNAP.IO · AI AUTORESCUE

04 · AI AUTORESCUE
Investigates. Validates. Rescues.
AI Cyber Orchestrator decides what can safely resume from primary production evidence. Clean, verified production recovery in minutes instead of days.

● Safe to resume ● Requires investigation ● Unsafe to resume

STRATEGIC DIRECTION

From production recovery intelligence to AI AutoRescue.

Cybersnap.io began in high-pressure Israeli government recovery environments and now extends that recovery discipline into a broader AI AutoRescue platform. **The starting wedge is production-side recovery:** turning primary production snapshots and recovery evidence into fast, trusted recovery decisions.

01 Primary production value

Cybersnap.io sits close to the primary production environment, not only backup metadata. Built for environments where recovery cannot depend on delay, guesswork, or unsafe restore points.

02 NetApp wedge, multi-storage direction

NetApp is the first validated entry point. The same AI Recovery Assurance model can expand across Pure, Dell, Nutanix, NAS, and other storage platforms through a connector-based architecture.

03 Ultra-fast recovery at the source

Cybersnap.io's strongest value is helping teams resume from trusted production-side recovery evidence. Clean, verified production recovery in minutes instead of days.

04 AI AutoRescue actions

The platform moves from AI-guided recommendations toward policy-governed rescue actions: inspect snapshot history, identify clean candidates, isolate questionable recovery points, validate workloads, and guide safe production resume.

05 Autonomous recovery with guardrails

Autonomous recovery must be policy-governed, evidence-based, validated, and human-approved where required.

IN THE PRODUCT

AI agents analyze primary production evidence, snapshot history, ransomware indicators, entropy shifts, file-change behavior, YARA priorities, anomaly signals, validation outputs, and recovery candidates.

IN THE ORCHESTRATOR

The AI Cyber Orchestrator coordinates specialized agents and turns separate findings into one recovery decision: safe, investigate, or unsafe.

ON THE ROADMAP

The roadmap moves from guided recovery decisions toward AI AutoRescue: retrospective attack discovery, recovery exposure simulation, clean-room validation, policy-governed rescue actions, and safe production resume in minutes.

STRATEGIC TAKEAWAY

Cybersnap.io turns primary production evidence into clean, verified recovery decisions in minutes. Born from high-pressure Israeli government recovery demands, the platform is now expanding into a broader AI AutoRescue layer for enterprises, MSPs, storage vendors, and cyber recovery platforms.

The long-term direction is autonomous recovery that works: policy-governed, evidence-based, validated, and human-approved where required.