VISION · AI-NATIVE RECOVERY ASSURANCE

Multi-agent AI that predicts, reacts, and rescues.

CyberSnap is building the AI-native Recovery Assurance layer for cyber recovery. The platform starts close to production, where the strongest recovery evidence lives, and turns recovery history into real-time recovery decisions. **The goal is simple:** know what is safe to recover, from where, and when, before recovery becomes a second failure.

Today, recovery still depends too much on human investigation under pressure. Teams must inspect evidence, compare recovery points, decide what is clean, contain the spread, validate recovery candidates, and restore production. **CyberSnap turns that manual loop into an AI-guided decision layer.** The starting point is production snapshots and NetApp environments. The direction is broader: multi-storage recovery assurance across on-prem platforms, then hybrid cloud plus on-prem recovery operations. It is the decision layer that determines what is safe to resume.

> **CyberSnap redefines the next age of recovery:** AI-driven decisions from production evidence, not manual recovery guesswork.

THE FIVE AGENTS

01 Predict & Detect
Finds early cyber signals across production snapshots and production telemetry. CyberSnap can correlate storage evidence with network logs, monitoring data, identity activity, workload behavior, anomaly detection, entropy shifts, YARA indicators, and slow-moving attack patterns.

02 React & Contain
Guides or triggers containment actions: network isolation, configuration freeze, permission cuts for risky users or service accounts, and DR replication pause.

03 Rescue & Validate
Restores candidate recovery points into an isolated clean room, runs validation scripts, analyzes usability, and recommends the safest recovery point.

04 Recovery Decision
Coordinates the agents, ranks recovery candidates, produces confidence signals, and determines what is safe to resume.

05 Prevent & Prove
Finds exposed sensitive files, reduces attack surface, and runs active simulations that prove recovery readiness before the real incident.

INPUTS · RECOVERY EVIDENCE

01 · PROTECTED DATA
Production snapshots and storage evidence
Across production storage and the broader environment.

02 · RECOVERY EXECUTION
Workloads can be restored
Orchestration is in place. Restore mechanics work.

03 · CLEAN VALIDATION
Recovery candidates tested
Restore candidates pass baseline integrity and isolation checks.

→

OUTPUT · AI RECOVERY ASSURANCE

CYBERSNAP. THE NEW LAYER.

04 · AI RECOVERY ASSURANCE
Predicts. Reacts. Rescues.
Multi-agent AI decides what is safe to resume. Recovery decisions in minutes, not hours or days.

● Safe to resume ● Requires investigation ● Unsafe to resume

STRATEGIC DIRECTION

From production recovery intelligence to hybrid cyber recovery assurance.

CyberSnap starts with a clear cloud and production-side recovery wedge: turning recovery evidence into actionable intelligence across cloud, storage, and production environments. **The broader direction is clear:** extend the same AI-based Recovery Assurance model across additional on-prem storage vendors, then across hybrid cloud plus on-prem recovery operations.

01 Production-side value

CyberSnap sits close to production evidence, not only backup metadata. That gives teams stronger recovery truth, with the goal of reducing decision and recovery cycles from hours and days to minutes.

02 NetApp wedge, multi-storage direction

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

03 Hybrid cloud plus on-prem vision

The long-term vision is not storage-only. Recovery Assurance should span production storage, backup environments, cloud infrastructure, and on-prem systems in one decision layer.

04 AI-native recovery actions

The platform moves from AI-guided recommendations to stronger action: detect suspicious changes, contain spread, pause risky replication, validate clean recovery candidates, and guide safe return to production.

05 Built for autonomous resilience

IN THE PRODUCT

AI agents analyze production evidence, timelines, scan results, recovery candidates, YARA priorities, anomaly detection, user activity, validation outputs, and more.

IN THE COMPANY

CyberSnap is AI-native from the outset, with an AI-first development model. AI shapes how the team builds, analyzes, tests, iterates, accelerates execution, and improves the product roadmap.

ON THE ROADMAP

The roadmap moves from guided recovery decisions toward autonomous recovery operations: slow-attack prediction, automated containment, clean-room validation, policy-based recovery actions, and zero-touch recovery with guardrails.

BOTTOM LINE

CyberSnap is building the AI Recovery Assurance layer for cyber recovery.

The starting point is production evidence, with NetApp snapshot intelligence as the first validated wedge. The direction is broader: multi-storage on-prem recovery assurance, then hybrid cloud plus on-prem recovery operations.

The long-term direction is autonomous recovery that works: policy-governed, evidence-based, and trusted enough to move from detection to recovery with minimal human delay.