

MirrorCorp - Benefits & Features

SI Continuity Assurance

The next evolution in cybersecurity: assurance that pays in uptime, not just dollars.

What MirrorCorp Is

MirrorCorp is SI continuity assurance for corporations. We clone your entire digital operation - every system your digitization vendor built - onto our own hardened, off-site servers, and keep that clone current. No vendor can guarantee you will never be hacked. MirrorCorp guarantees you will be back.

How It Works: Clone. Sync. Quarantine. Secure Burn. Flip.

1. Clone - full duplication of your systems into our isolated vault at onboarding.
2. Sync - the clone stays current, backed up two to four times daily, never more than hours behind.
3. Quarantine - on attack, the infected environment is isolated; nothing spreads, and nothing is salvaged in place.
4. Secure Burn - the infected environment is destroyed securely, never revived.
5. Flip - we flip the switch to the clean clone. Back online in hours, not weeks - an interruption, not a shutdown.

How It Runs: The Agent. The Tunnel. The Vault. The Standby.

- The Agent - a small program on each of your servers does the copying, and encrypts everything before it leaves your building - sealed at the source.
- The Tunnel - your clone travels over your own internet connection, through a private encrypted tunnel that dials out from your side. Your firewall never opens to us.
- The Vault - immutable storage inside audited U.S. data centers - SOC 2 Type II and ISO 27001 audited facilities. Inside the retention window the copy cannot be altered or deleted - not by an attacker, not by a rogue employee, not even by us.
- The Standby - a powered-down copy of your environment, pre-built and tested, sits beside the vault. On the Flip it wakes up and runs your company; we drill it on schedule and you get the drill report.
- No hardware for you to buy: your existing connection carries the sync, and a very large first clone can be seeded on an encrypted drive instead of your bandwidth.

Benefits & Features

- A living mirror of your company: systems, data, and configuration, mirrored whole and kept current.
- An isolated, untouched vault: air-gapped and immutable by design, built to a SOC 2-grade standard and operated by MirrorCorp ourselves. The mirror is never the infected environment.
- Burn-and-flip recovery: no forensic salvage of infected code in place, no hourly meter running during your worst week.
- Deterrence by Denial: a protected company is back before a ransom note is read, so a successful attack gains the attacker nothing. No leverage. No payday. No point.
- Aligned with NIST SP 800-61 Revision 3 (April 2025), the federal incident-response model - preparation, detection, response, recovery, and improvement after every event.
- The MirrorCorp shield in the bottom-right corner of every protected screen - certified seal, pulsing light, MIRRORCORP ACTIVE: the live SECURED state confirming the mirror is current and protection is on; out-of-sync machines change state and alert our team.
- Coverage tiers up to 100% of the rebuild value of the systems covered, scaled to what you have built.
- Sequenced honestly: MirrorCorp launches as recovery assurance (a service contract), with a carrier partnership as Phase 2. Nothing here is an offer of insurance.

Trust & Compliance Roadmap

- Phase 1 - Foundation (live / in progress): incident response aligned with NIST SP 800-61 Rev. 3 is live today; written security policies and access controls in progress; cyber liability and technology E&O program being placed; independent penetration test next.
- Phase 2 - SOC 2 Type I (target: first half of 2027): compliance-platform readiness, then an independent CPA audit of control design.
- Phase 3 - SOC 2 Type II (target: observation window opens 2027): controls proven operating over time, annual penetration tests, published recovery-drill evidence.
- Phase 4 - ISO 27001 and sector readiness (target: Year 2): ISO 27001 certification path; HIPAA readiness attestation and BAA for healthcare clients.
- Founding clients sign with this roadmap written into their agreement as a Compliance Commitment Schedule - milestone dates, reports shared under NDA, and the right to exit if a milestone is missed. MirrorCorp is not SOC 2 or ISO 27001 certified today, and claims neither.

Why It Matters

Traditional incident response investigates and rebuilds infected systems at emergency rates, over weeks. MirrorCorp does not revive infected code at all. They sell recovery. We sell being back.

"When your corp goes dark, MirrorCorp turns the lights back on."

MIRRORCORP - YOU ARE ACTIVE

Request a private assessment: info@SyntheonSi.Tech | MirrorCorp.SyntheonSi.Tech