elastio™

Take Control of Cyber Recovery

Top Five Reasons: Why Elastio?

Data Integrity for Cloud Defense and Provable Recovery

Malware makes you sick. Ransomware is terminal. If your data integrity isn't verified, ransomware-encrypted backups are useless for recovery. Elastio closes that gap.

Only Elastio detects ransomware. We go beyond signatures and alerts to identify encryption at scale, integrity drift, and backup sabotage. While immutability may address these issues, pinpointing your last clean recovery point with proof is critical. And only Elastio reliably detects ransomware encryption.

Alerts don't save you. Controlling your recovery does. With Elastio, you don't just detect problems. You control your recovery.

1. Zero-Day Detection

Elastio provides AI-driven ransomware detection on known variants that goes beyond traditional malware scanners. Unlike conventional defenses that only detect known threats, Elastio identifies ransomware hidden in backups and snapshots. This ensures every recovery point is verified as clean and safe, protecting against attacks that bypass endpoint and traditional security.

2. Continuous Validation

Continuous validation of data integrity ensures backups are truly recoverable. Backups can appear intact, but hide ransomware, and endpoint tools don't validate storage or replicas, and without proof of clean backups, recovery risks failure, downtime, and data loss.

3. Seamless Integration with Existing Backups

Elastio integrates with Cohesity, Commvault, NetBackup, Rubrik, Veeam, and more to ensure backup integrity across platforms. Unlike traditional scanners that create noise with false alarms, Elastio detects real ransomware encryption and identifies the last clean recovery point with certainty. The result: faster, provable recovery without guesswork, saving days of trial and error.

Backups are the new bullseye: 96% of ransomware now targets backups. Once compromised, your "last line of defense" disappears.

4. Compliance Made Simple with Audit Dashboards

Elastio goes beyond backups and immutability by proving recovery is possible. With AI detection, continuous validation, and R-RPO, it generates audit-ready dashboards aligned with regulations like NYDFS, DORA, PCI DSS, NIST, and ISO/IEC 27001—giving boards and auditors confidence that recovery is compliant and provable.

5. Proven Recovery

Your CEO doesn't care about alerts. They care about the business, recovery time, clean data, and reputation. Backups alone aren't proof, and malware scanners often miss ransomware encryption hidden in snapshots. Elastio is different; it validates every recovery point, ensuring they're clean and turning recovery into a measurable security control.

Why Customers Care

- Backups can lie: Encryption may be hidden even when scans look "clean."
- Endpoint tools fail: EDR can't protect backups—over 3,800 malware samples have been found inside them.
- Compliance demands proof: Regulators and boards (NYDFS, DORA, SEC) now require evidence that recovery actually works.

Control your recovery >> elastio.com