

Elastio Ransomware Recovery Assurance Platform

Benefits

Early detection of ransomware that bypasses preventative EDR/XDR, network, application security solutions.

Early detection of malicious encryption by insider threats.

Assures safe recovery options by continually verifying that your last-known copy of data is uncompromised and ready for restoration.

Inspects storage and backups **across platforms.**

Compliance: The Elastio platform provides dynamic and graphical resilience reports that meet the needs of auditors and insurers.

Results:

Protects Major AWS Services and Integrations: Works with AWS services such as EC2, EBS, S3, ECS, EKS, EFS, AWS Backup, LAG Vaults, and more.

Protects Primary Backup Vendor Backups on VMware: tight integration with all primary backup and security software solution providers ensures clean backups and snapshots are available for fast recovery.

Incident Response Premium Support Experience: Our Premium Support Experience checks all Elastio Platform ransomware findings and provides a detailed playbook for restoring a clean copy of data, helping you act fast to protect your environment.

Improved Recovery Capabilities: The framework ensures that data can be restored efficiently without paying ransoms, minimizing downtime and financial losses.

Ransomware attacks are becoming increasingly sophisticated, evading advanced prevention tools and perimeter security systems. Current solutions focus on server activity, but Elastio's Ransomware Recovery Assurance platform takes a different approach by prioritizing data integrity.

Elastio's platform is uniquely engineered to address a critical gap.

Unlike current solutions, Elastio doesn't just monitor servers—it focuses on your data. By deeply understanding how ransomware encrypts data and leveraging its AI/ML data integrity technologies, Elastio provides critical protection against ransomware's most advanced tactics that other solutions can't and alerts you before it's too late.

By continuously monitoring the data integrity of your critical infrastructure, Elastio enables you to stop ransomware attacks before they become uncontrollable. This also ensures that your backups remain ransomware-free, **giving you the confidence to identify and recover from an attack without hesitation.** When ransomware targets your data, Elastio is the safeguard that ensures you'll always have a quick and clean way back.

Why Elastio Is Different

- **Detecting Zero-Day Ransomware with the Elastio Platform**
RansomwareIQ, the data integrity engine that powers the Elastio Platform, analyzes behavior within storage and backups beyond traditional signature and anomaly-based methods. By detecting early signs of ransomware, Elastio identifies and alerts you of threats **before** they spread, compromising your storage and backups.
- **Zero Trust Scanning**
Today's ransomware operates beneath the radar, slowly encrypting data at the storage layer while staying invisible to signature and anomaly detection tools found in other solutions. Elastio uses a **zero-trust scanning** approach to inspect data outside the compromised operating system. This ensures Elastio cannot be bypassed or "unhooked."
- **Deep inspections** are performed off the production system without impacting production performance.
- **Elastio will identify, alert, and help remediate corrupted data**—preventing it from creeping through infrastructure and into backups.
- **Recovery Made Simple with Clean Recovery Assurance**
Elastio continuously inspects storage and backups to record the **last known clean copy** of your data. When ransomware strikes, Elastio has already pinpointed a clean recovery point—pre-tested and verified—so you can recover quickly and confidently. Elastio saves critical downtime, data loss, and revenue loss, quickly getting your business-critical data and applications back online.
- **Impactful ROI for your Organization**
Elastio can find advanced ransomware infections in your backups, snapshots, and data and proactively discover other more common recoverability issues that would prevent a successful restore.

"Knowing my data is clean gives me confidence that my backups are secure and recoverable, whether it's an attack or just an outage. Ensuring our backups are free of latent ransomware is critical - without this, undetected threats could compromise backups, and once the retention period expires, we'd have no clean recovery points."

Cloud Architect at a Global Fortune 100 Insurance Company

About Elastio

Elastio is a pioneer in Ransomware Recovery Assurance, offering advanced solutions to protect critical business data from sophisticated cyber threats. Powered by its AI-driven RansomwareIQ engine, Elastio validates data integrity by detecting hidden ransomware across cloud and on-premises environments with 99.99% accuracy. Elastio integrates effortlessly into existing workflows, providing multi-cloud and multi-backup protection, while its compliance-ready reporting supports adherence to regulations like NYDFS and DORA. Elastio empowers organizations to minimize downtime, recover swiftly, and confidently combat modern ransomware threats by prioritizing data integrity and operational resilience.