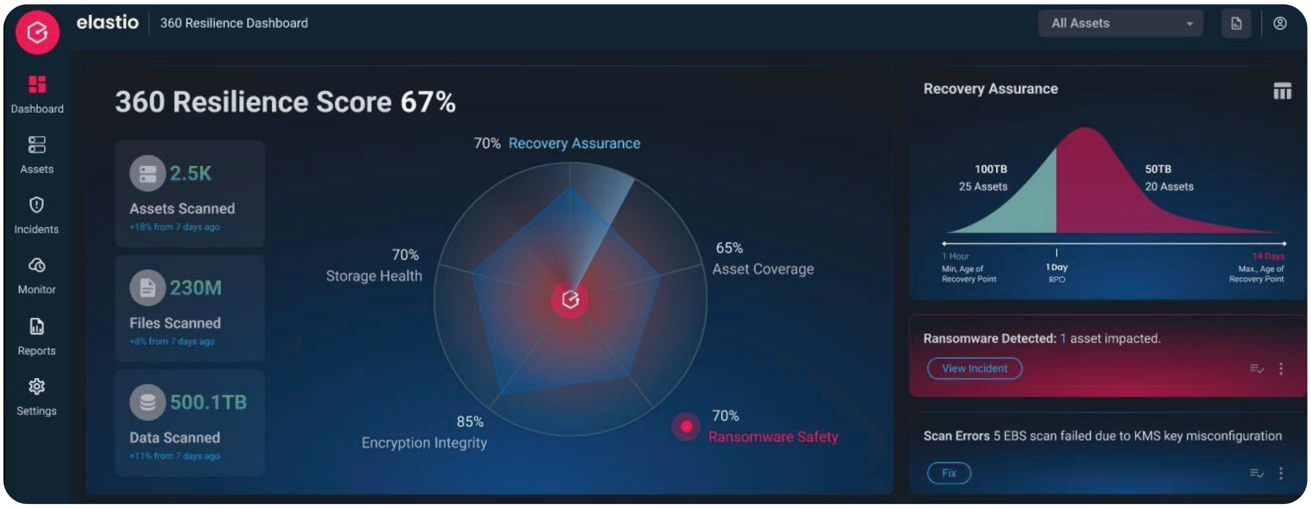
elastio™
Ransomware Recovery Assurance

Solution Brief

Proactive Defense:

Ensuring Clean Recovery Points in a World of Sophisticated and Evolving Ransomware

Recover quickly from ransomware attacks and stand up to extortion: Clean backups ensure that uncorrupted data is always available, allowing organizations to restore systems to their last known safe state before the attack. Rapid recovery mitigates reputational risk by minimizing downtime, reducing data loss, and ensuring business continuity.



Ransomware Detected: 1 asset impacted.

Scan Errors 5 EBS scan failed due to KMS key misconfiguration

Problem Statement

With sophisticated ransomware slipping past Endpoint Detection and Response, Managed Detection and Response, and Cloud Security Posture Management defenses, companies risk unknowingly backing up infected data—leaving no safe recovery option when an attack hits. The engine of the Elastio Ransomware Recovery Assurance, RansomwareIQ, proactively inspects backup data for hidden threats to ensure clean, uncompromised recovery points. Manage the integrity of your backups with Elastio and recover with confidence.

Why Elastio Ransomware Recovery Assurance

Zero Trust Approach to Ransomware, Malware, Recovery Assurance. Under Zero trust, you operate under the assumption that a breach will or has occurred. Since ransomware attacks commonly compromise the workload, any scans running on the workload cannot be trusted. Data must be scanned off the host (data at rest), bypassing the potentially compromised workload. Backups and Snapshots are ideal sources of data at rest.

Because backups are your last line of defense, they must be continuously validated to ensure their uncompromised recovery.

Quickly identifying the last known clean backup is crucial in an organization with tens of thousands of recovery points. Knowing which one to recover from saves critical time. The average Netbackup customer has over 70,000 recovery points.

ROI: Quick recovery means less time spent offline, which helps maintain business operations and minimizes financial losses

Novel Ransomware Detection

Elastio is the leader in Ransomware Recovery Assurance, delivering unmatched ransomware detection and data protection for cloud and on-premises environments. Powered by AI-driven RansomwareIQ technology, Elastio ensures clean, uncompromised backups and rapid recovery, helping businesses strengthen resilience, maintain compliance, and minimize downtime in the face of evolving cyber threats.

Elastio Ransomware Recovery Assurance (Elastio platform) offers a unique approach to ransomware detection. The Elastio platform engine, Elastio RansomwareIQ, detects ransomware encryption without requiring signatures and can **identify never-before-seen novel threats.**

Integration with existing workflows and systems

The Elastio platform integrates into your existing security workflows, allowing you to easily incorporate Elastio's robust ransomware detection telemetry into your existing Security Information Event Management (SIEM) system.

Traditional tools don't do what the Elastio platform does.

Extended Detection and Response (EDR) and Managed Detection and Response (MDR)

Industry-leading vendor examples: CrowdStrike, Arctic Wolf

EDR and MDR solutions do not identify the last known clean backups in case of an attack, nor do they scan for ransomware. They can and are being bypassed. (See Zero Trust). They are also usually agent-based.

Cloud Security Posture Management (CSPM)

Industry-leading vendor examples: Wiz and Orca Security

CSPM inventory and look for vulnerabilities to help perform patch management for cloud workloads and make the system more secure. However, this represents only 36% of typical ransomware attack vectors. Elastio protects your recoveries when threats still get through.

Integrated Anomaly Detection Solutions

In recent years, some backup providers have added anomaly detection algorithms to their platforms. However, these systems often produce false positives because they are designed to flag any unusual activity. Many of these alerts are triggered by harmless or routine changes—such as new data, updates, and minor adjustments—that the system may mistakenly interpret as threats. Worse yet, anomaly detection does not catch real ransomware threats, which have been designed to stay undetected by anomaly detection tools.

The Elastio platform directly inspects the files' integrity, identifying ransomware detonations that are in progress. Modern ransomware attacks and detonations are explicitly designed to encrypt data on live systems at rates undetectable by anomaly detections. Only by inspecting the files themselves can these threats be identified and limited.

About Elastio

Elastio is the leader in Ransomware Recovery Assurance, enabling businesses to protect critical data from modern ransomware threats. With AI-powered RansomwareIQ technology, Elastio provides unparalleled detection accuracy, ensuring clean backups across multi-cloud and on-premises environments. By integrating seamlessly into existing workflows, Elastio delivers rapid recoveries, regulatory compliance, and operational resilience, empowering organizations to combat cyber threats and recover confidently. Elastio's mission is to ensure businesses remain secure and prepared in the face of evolving ransomware attacks.