Elastio Launches Ransomware Detection & Version Intelligence for Amazon S3

Real-Time Ransomware Detection and Provable Recovery for Amazon S3

RESTON, VA, UNITED STATES, March 23, 2026 /EINPresswire.com/ -- Elastio today announced Elastio Version Intelligence for Amazon S3, a new capability within its Active Cyber Resilience Platform. The release extends Elastio's data integrity control to Amazon Simple Storage Service (Amazon S3), enabling organizations to detect ransomware and malware events across objects in near real time, trace version lineage to identify the last known clean state, and perform non-destructive recovery without manual version inspection.

> Amazon S3 holds the data most organizations cannot afford to lose or recover slowly. Elastio Version Intelligence for Amazon S3 helps security teams get a precise answer under incident pressure."
>
> *Najaf Husain, CEO, Elastio*

The capability analyzes object version changes and helps security teams quickly identify a verified recovery point when investigating potential ransomware or unauthorized modification events.

Why Object Storage Security Matters

Amazon S3 stores critical data across many organizations, including AI training datasets, financial records, healthcare archives, and operational logs. As organizations increasingly rely on object storage for business-critical workloads, security teams must ensure that stored data remains recoverable and trustworthy following a cyber event.

While Amazon S3 provides strong durability, access control, versioning, and security capabilities, incident response teams may still need to determine which object version represents a clean recovery point when investigating ransomware or unauthorized modification scenarios.

Traditional endpoint and backup security tools were not designed to inspect individual object versions within object storage environments. Elastio adds an additional detection layer that analyzes object changes and version lineage, helping teams more quickly determine which version of data can be safely restored.

What Elastio Version Intelligence for Amazon S3 Does

Elastio Version Intelligence for Amazon S3 extends Elastio data integrity control to object storage and version history. The capability introduces three integrated functions that operate together:

1. Real-Time Object Hunting: Elastio hunts S3 object creation or modification in real time using deep object inspection. An ensemble of detection models trained on 2,300+ ransomware families assesses each object independently on change.

2. Lineage Hunt: When an object is flagged, Elastio automatically traces the version chain backward until it identifies the LNC version: the most recent version that passes all detection checks. The LNC version ID, detection type, and timestamp are surfaced immediately.

3. Copy-Forward Recovery: The LNC version is copied forward as the new current object. Non-destructive: the full version history, including compromised versions, is preserved for forensic review. Restores can be executed automatically by policy or embedded into an existing forensic investigation workflow.

"Amazon S3 holds the data most organizations cannot afford to lose or recover slowly. Version history tells you what existed. It does not tell you what is clean. Elastio Version Intelligence for Amazon S3 analyzes object changes and version lineage to help security teams identify a verified recovery target more quickly. Security teams get a precise, documented answer under incident pressure." - Najaf Husain, CEO, Elastio

Key Capabilities

1. Real-Time Object Hunting: Deep object inspection on every S3 create or modify event. Detection models trained on 2,300+ ransomware families assess each object independently on change

2. Lineage Hunt: Automated backward trace through the version chain to LNC identification on detection

3. Copy-Forward Recovery: Non-destructive recovery that preserves full version history and the forensic record

4. Dual Recovery Paths: Automated policy-driven restore or embedded forensic investigation workflow, configurable per deployment

5. Full Audit Trail: Every hunt result, version transition, and recovery operation logged with timestamp and version ID to the Elastio console and SIEM

Availability
S3 Version Intelligence is available immediately. Organizations can contact Elastio to begin a deployment review at elastio.com.

About Elastio
Elastio delivers Active Cyber Resilience, a security philosophy built on one principle: recovery must be continuously proven and not periodically tested or assumed. The Elastio Hunt Engine performs Deep File Inspection across live data, replicated data, and backups to detect ransomware and malware that has evaded prevention and detection tools. Recovery you can prove.

Cecily Polonsky
Elastio
email us here
