Ensure Clean, Ransomware-Free Recovery
with Elastio & AWS Logically Air-Gapped Vaults

Benefits

Enhanced Security:
Combining AWS Backup's Logically Air-Gapped Vaults with Elastio Platform's scanning capabilities provides a fortified defense against ransomware.

Regulatory Compliance:
Continuous validation supports compliance with frameworks like DORA, NYDFS, and MAS TRM.

Operational Efficiency:
Automated data scanning reduces manual intervention, ensuring backups are clean and ready for recovery.

Peace of Mind: Organizations can confidently rely on AWS Logically Air-Gapped Vault backups utilising Elastio Platform, knowing their data is clean and uncompromised.

The Challenge - Ransomware's Threat to Backups

Modern ransomware attacks are increasingly sophisticated, often targeting backup systems to compromise recovery efforts. Last year, 96% of ransomware incidents involved attacks on backup data*. While AWS Backup's Logically Air-Gapped Vaults provide enhanced security by isolating backups with AWS-owned encryption keys and compliance-mode vault locks, ensuring the integrity of these backups remains a critical concern.

* ESG - ESG Research Finds Immutable Backup Storage Following Zero Trust as the Best Defense Against Ransomware April 9, 2025

Results:

Organizations leveraging Elastio with AWS Logically Air-Gapped Vaults are realizing measurable improvements in cyber resilience and operational readiness:

Faster Recovery Validation

Automated ransomware scanning validation of backup data reduces recovery test cycles from days to minutes, enabling rapid, clean restoration when it matters most.

Zero-Incident Backup Data Compromise

Customers using pre- and post-vault scanning have reported zero incidents of ransomware reinfection through data recovery points, dramatically lowering business continuity risk.

Audit-Ready Compliance Reporting

Continuous snapshot data backup validation helps teams confidently meet regulatory demands, with clean evidence trails for DORA, NYDFS, and MAS TRM audits — no manual testing required.

Reduction in Manual Backup Operations

Integrated automation minimizes human error and frees IT resources, increasing productivity while ensuring backup integrity.

Executive Confidence at Every Layer

With clean, verified recovery points, security teams can assure boards and leadership that "We can recover—cleanly and quickly."

The Solution: Integrating Elastio Ransomware Recovery Assurance with AWS Backup LAG Vaults

Elastio Ransomware Recovery Assurance Platform (Elastio Platform) complements AWS Logically Air-Gapped Vault by validating backup data snapshots and ensuring recovery points are free from ransomware, insider threats, and corruption.

Customers can choose between different deployment configurations:
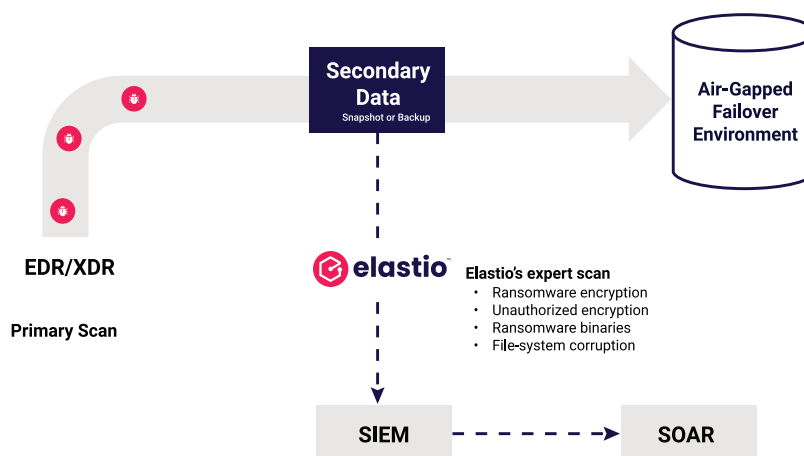
1. Pre-Vault Scanning in the Workload Account

- **Automated Scanning:** Elastio Platform is deployed within the workload account to scan recovery points immediately after creation, before being copied to the AWS LAG Vault.
- **Early Threat Detection:** Organizations can identify malicious activity early to prevent compromised data from being stored in the AWS LAG Vault.
- **Implementation Steps:**
  - » Deploy Elastio Platform using a CloudFormation template in the workload account.
  - » Configure AWS LAG Vault plans to tag recovery points with elastio:action=scan.
  - » Set up Amazon EventBridge and AWS Lambda to trigger Elastio Platform scans based on these tags.

2. Post-Vault Scanning in the Recovery Account

- **Centralized Validation:** Elastio can also be deployed in a separate recovery account to scan backups after they have been copied to the AWS Logically Air--Gapped Vault
- **Secure Sharing:** Using AWS Resource Access Manager (RAM), the AWS Logically Air--Gapped Vault is shared with the recovery account, allowing Elastio to perform restore testing and validation without compromising security.
- **Compliance Assurance:** This approach ensures backups meet regulatory requirements and are ready for rapid, clean restoration.recoverability — so they can act confidently when recovery is on the line.

Elastio's Data Integrity Layer Protects Your Organization

Secondary Data
Snapshot or Backup

Air-Gapped Failover Environment

EDR/XDR

Primary Scan

elastio

Elastio's expert scan
- Ransomware encryption
- Unauthorized encryption
- Ransomware binaries
- File-system corruption

SIEM

SOAR

Get Started

Implementing this integrated solution enhances your organization's resilience against ransomware threats.

See Elastio in action. Request a Demo Today.
Available on AWS Marketplace
Learn more at www.elastio.com

Contact us at sales@elastio.com

About Elastio

Elastio specializes in ransomware mitigation and recovery, providing businesses with advanced tools to validate their data. By bridging the gap between traditional security measures and immutable backups, the Elastio Platform ensures clean recovery from zero-day ransomware attacks, giving organizations the confidence to restore operations quickly and securely. For more information, visit www.elastio.com.