elastio®

Elastio - New Release Update

September, 16th 2024

Elastio is excited to announce new and enhanced features for cloud and on-premise environments designed to safeguard customers' business-critical data from ransomware attacks with increased flexibility and efficiency.

These updates introduce more robust, smarter capabilities to enhance ransomware readiness and stay ahead of ransomware threats.

Major Features

Cloud Protection

- Centralized Ransomware Protection Using an AWS Backup Bunker Account
- Non-Ransomware Entropy Detection
- AWS Backup Logically air-gapped vault (LAG) Vault Integration
- VMware Backups Support
- Elastio Incremental Inspections for S3
- Enhanced S3 Ransomware Detection

On-Premise Protection

- Elastio for Rubrik on VMware Support
- Elastio for Cohesity on VMware Support

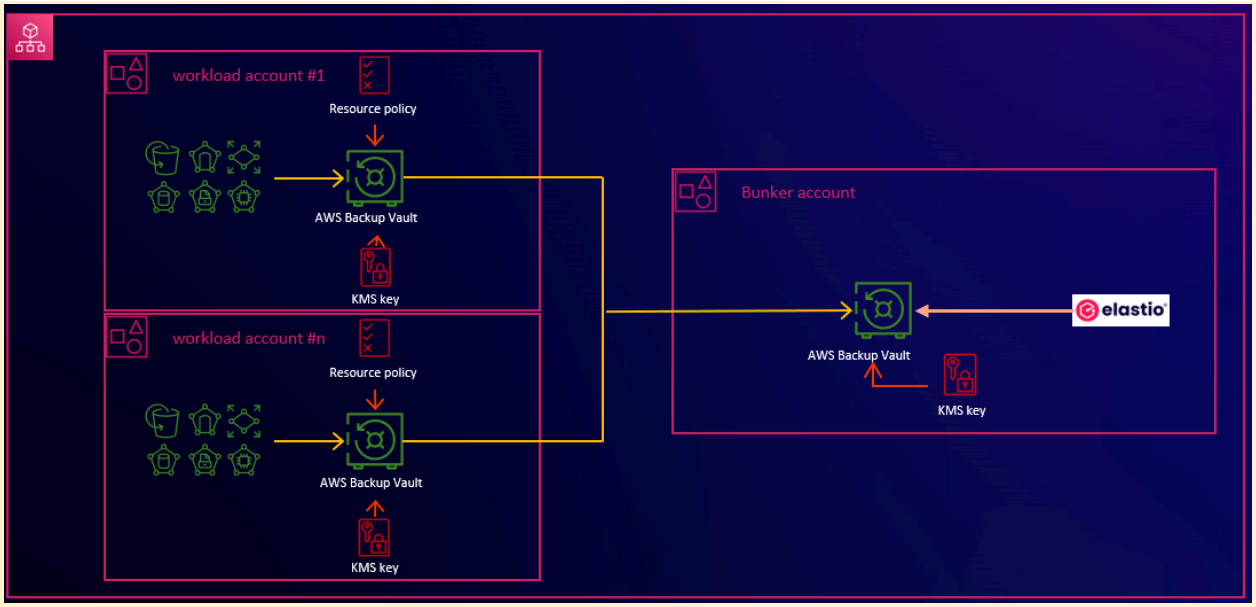
Other Enhancements

- CloudConnector Deployment
- SSO Integration
- EC2 Restoration Workflow
- Expanded Filesystem Checks
- Enhanced Reporting
- AWS Backup Integration
- Improved Misconfiguration Analysis
- Tag Propagation
- Flexible On-Prem Inspections

Cloud Protection

Centralized Ransomware Protection Using an AWS Backup Bunker Account

This new enhancement fulfills a critical customer request by providing the ability to easily inspect backups from multiple AWS accounts within a single, secure AWS Bunker account, where backups are copied from several accounts.



With Elastio, customers can continuously ensure that data in the Bunker Account is ransomware-free, enabling reliable recovery and fast restoration of operations during an attack.

Try now

1. Deploy Elastio in the Bunker account.
2. Deploy the CFN in the workload accounts to tag EC2 backups. These tags include the metadata from the EC2 and the attached EBS volumes.
3. Add "**elastio:action=scan**" in the workload account Backup Plan. You can add the tag by AWS Backup> Backup Plans> Backup Rule.

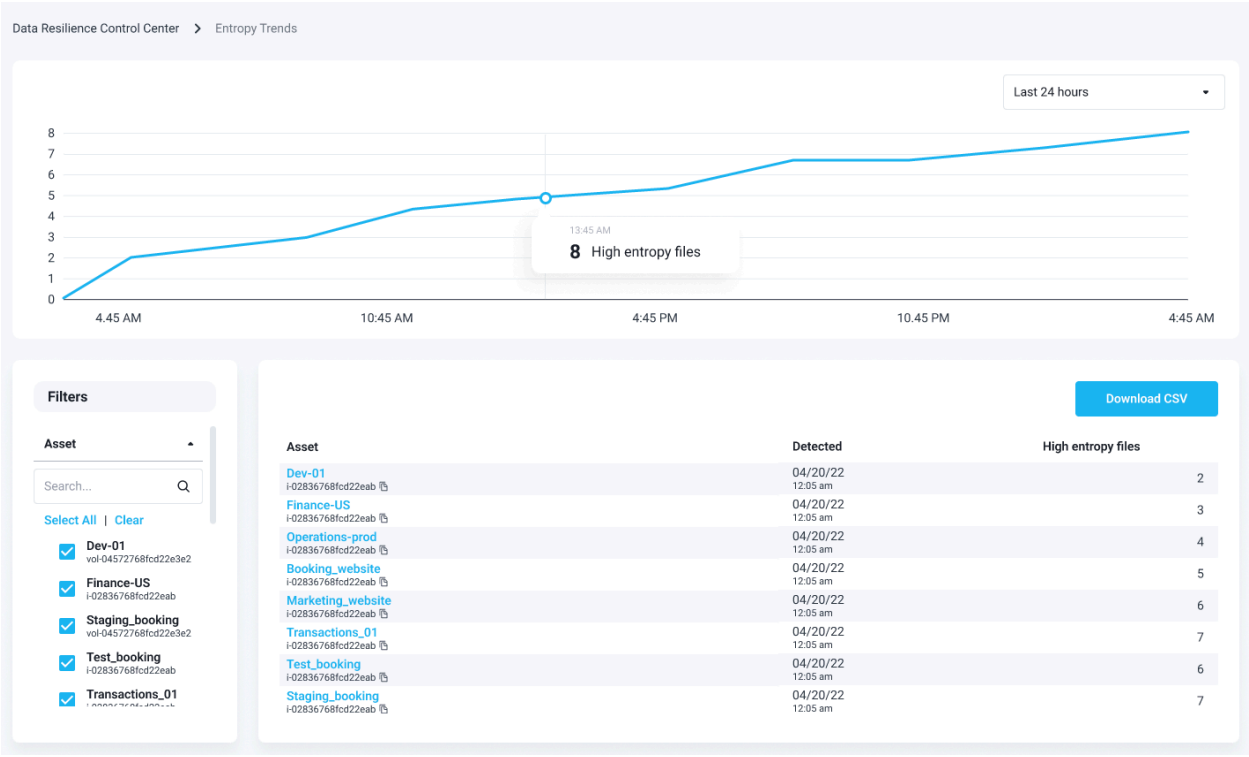
FAQs

1. **Can I inspect backups in a Workload account before they are copied to the Bunker account?**
   Yes. You can deploy Elastio in Workload accounts to inspect backups before they are copied to a Bunker account in order to detect ransomware even earlier. Backups will still be copied, whether clean or infected, but since AWS Backups are immutable, you can always restore to the last known clean state.

2. **Why do I deploy a CFN to tag the AWS Backups in the workload account?**
   AWS Backup does not pass on EBS volume metadata when a Recovery Point is copied to another account. Deploying this Cloud Formation Template from AWS ensures the metadata is included in the Recovery Point tags, allowing for more accurate results in the Elastio Tenant UI and reports.
   If the CFN is not deployed, Elastio will still inspect the backups, but we add a pseudo volume name, making it difficult to track and analyze backup integrity across accounts. We strongly recommend deploying the CFN.

Non-Ransomware Entropy Detection

Elastio now detects potential internal threats by identifying newly encrypted or suspiciously modified files across your network. This behavioral model analyzes file changes between backups, flagging files that show signs of encryption, and includes file type analysis to help safeguard your company's data.



Try now

Create/ edit the Elastio policies. You can do it by going to Policies>New Policy/ Edit an existing policy> Integrity Scan > Enable High Entropy Detection.

FAQs

1. **I have some non-ransomware encrypted files in my directory. Will Elastio's entropy detection alert on all of these?**
   Elastio's sophisticated entropy detection model is designed to minimize false positives by focusing on genuine threats, not benign encryption. Here are key strategies it uses to enhance accuracy:
   - **Exclude low-entropy:** Elastio only alerts on files with high entropy.
   - **Exclude directories with low percentage of change**: Elastio excludes directories with less than 50% of files new or modified from analysis to focus on areas of significant change.
   - **Exclude baseline inspection**: Elastio's entropy detection does not alert on the results of the initial baseline inspection but only uses over-time analysis, comparing the current state of files and directories to previous inspections.
   - **Exclude previously flagged files**: Files that have already been alerted on are not reported again, preventing duplicate alerts.

2. **Which asset types are supported?**
   EC2 and EBS asset types are supported with this launch.

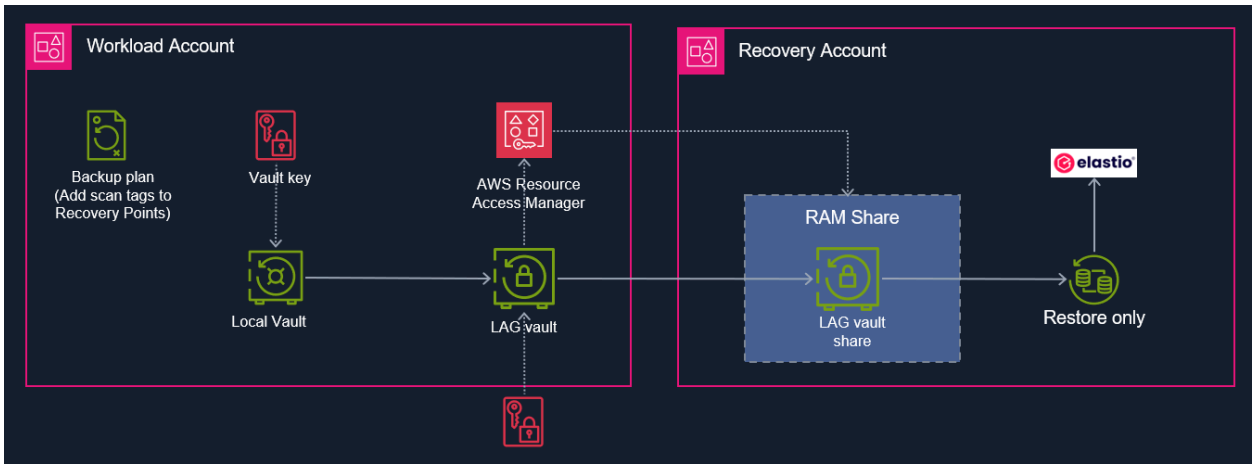
AWS Backup Logically air-gapped vault (LAG) Vault Integration

Backups in the recently GA AWS Backup LAG Vault are stored in an AWS-owned account and encrypted with AWS-owned keys, ensuring they remain secure and accessible even if your entire environment is compromised or corrupted.

With this integration, Elastio customers can inspect backups in the **LAG Vault** immediately upon creation using the AWS restore testing feature. This ensures

that backups are clean and free from ransomware, providing an essential safeguard when recovery is needed.

Additionally, the ability to instantly share and restore backups across accounts, including those outside your Organizational Unit, accelerates recovery during a ransomware attack, minimizing downtime and disruption.



Try now

1. Deploy Elastio in the Recovery account.
2. Deploy the restore testing CFN in the Recovery account for Elastio to scan Recovery points as part of restore testing.
3. Deploy the CFN in the workload accounts to tag EC2 backups. These tags include the metadata from the EC2 and the attached EBS volumes.
4. Add **"elastio:restore-test=scan"** in the workload account Backup Plan. Add the tag to AWS Backup> Backup Plans> Backup Rule. All the recovery points that have this specific tag and are part of restore testing will automatically be inspected.

FAQs

1. **Can I inspect backups in a workload account before they are copied to the LAG Vault?**

   Yes, Elastio customers can still inspect backups in workload accounts before

they are sent to the LAG Vault. This new launch provides the additional option to inspect backups in the LAG Vault via restore testing for an extra layer of ransomware detection and data validation.

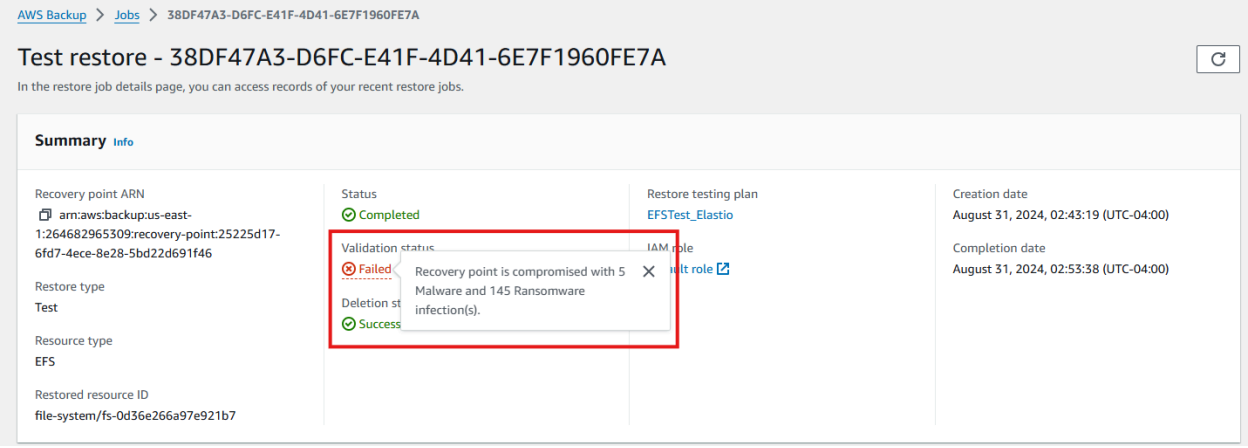
2. **Can I inspect backups in the LAG Vault without Restore Testing?**
   At this stage, customers cannot inspect backups within the LAG Vault without Restore Testing since AWS Backup does not enable Recovery Points to be mounted directly from the LAG Vault.

3. **Why do I deploy a CFN to tag the AWS Backups in the workload account?**
   AWS Backup does not pass on volume metadata when a Recovery Point is copied to another account. Deploying this Cloud Formation Template from AWS ensures the metadata is included in the Recovery Point tags, allowing for more accurate results in the Elastio Tenant UI and reports.

   If the CFN is not deployed, Elastio will still inspect the backups, but AWS adds a pseudo volume name, making it difficult to track and analyze backup integrity across accounts. We strongly recommend deploying the CFN.

4. **What does the Restore testing CFN do?**
   The Restore Testing CFN enhances AWS Backup Restore tests by automatically inspecting backups tagged with **"elastio:restore-test=scan."** Once an inspection is complete, the results are returned to AWS Backup to verify that your backups are safe and ransomware-free before restoration.

5. **Does this integration enable me to see the results of Elastio inspections in the AWS Backup UI?**
   Elastio's integration with LAG Vault lets customers view inspection results directly in the AWS Backup console. Check the **"Validation Status"** in the restore test job details: a **"Failed"** status means Elastio has detected ransomware in your backup. Hover over the *validation status* for more information about the ransomware findings to support remediation and forensics efforts.



VMware Backups Support

Elastio extends its protection coverage to VMware backups taken by AWS Backup, adding an essential layer of security for VMware environments.

Try now

1. Deploy Elastio in the Recovery account.
2. Deploy the restore testing CFN in the Recovery account for Elastio to scan Recovery points as part of restore testing.
3. Add **"elastio:restore-test=scan"** in the workload account Backup Plan. You can add the tag by going to the AWS Backup console and navigating to **AWS Backup> Backup Plans> Backup Rule**.
   All the recovery points that have this specific tag and are part of restore testing will automatically be inspected as part of restore testing.

FAQs

1. **Can I view VMware backup inspection results in the AWS Overview Dashboard on the Elastio console?**
   Elastio uses a separate dashboard for on-premises assets. To view and inspect results for VMware backups managed by AWS Backup, click the "+" on the dashboard tab and select "Backup Connector: AWSB VMware." You can now monitor the VMware assets in the dashboard.

2. **How does the inspection work?**
   Elastio restores the VMware backup into an EC2 instance, which is then inspected by Elastio. Since AWS Backup does not support restore testing for VMware backups, Elastio restores the VMware backup and inspects the restored copy of the virtual machine.

Elastio Incremental Inspections for S3

With this release, Elastio dramatically enhances the performance of its S3 Ransomware Protection, enabling it to provide more efficient inspections of very large S3 buckets.

After an initial full base inspection, Elastio incremental inspection utilizes Amazon EventBridge to efficiently track and only inspect objects that have been modified or created since the previous inspection, saving time and resources.

Try now

Incremental Inspections for S3 CFN Deployment

FAQs

1. **What's the difference between Standard S3 scans and Incremental Inspections for S3?**
   Incremental inspection utilizes Amazon EventBridge to monitor all S3 object changes and inspects only new or modified objects. In contrast, without Incremental Inspections for S3, Elastio lists all objects in the S3 bucket during each inspection.

2. **Is there any advantage to using standard S3 inspections over S3 Incremental Inspections?**
   While Incremental Inspections are efficient for large buckets, standard S3 inspections offer enhanced security. By comparing current objects with previous scans, they can detect potential ransomware encryption across the entire bucket, providing more comprehensive protection.

Enhanced S3 Ransomware Detection

Elastio's ransomware protection for S3 already inspected data for pre-detonated ransomware using a signature scanner to catch known threats. Now, Elastio has extended its proprietary ransomware encryption detection to S3 objects, allowing customers to identify ransomware in the early stages of encryption.

This advanced feature sets Elastio apart from other S3 ransomware protection solutions, like GuardDuty, and enables businesses to defend against ransomware encryption threats that bypass traditional signature-based scans.

Try now

Create/ edit the Elastio policies. You can do it by going to Policies>New Policy/ Edit an existing policy> Integrity Scan > Ransomware Detection

FAQs

1. **I already have Ransomware Detection enabled in my Elastio S3 policy. Will this enhancement run by default?**
   Elastio's enhanced detection for S3 will automatically run on all existing S3 buckets with an Elastio S3 policy enabled with ransomware scans.

2. **Do ransomware scans work with SmartScan for S3?**
   No. This new enhancement does not work with Elastio SmartScan for S3. We will add this support in a future release.

On-Premise Protection

Backup connector for Rubrik on VMware

- With this release, Elastio extends its coverage capabilities to Rubrik backups on VMWare, leveraging native APIs to automatically inventory Rubrik backups upon creation and inspect them for ransomware.

Backup connector for Cohesity on VMware

- With this release, Elastio extends its coverage to Cohesity backups on VMWare, leveraging native APIs to automatically inventory Cohesity backups upon creation and inspect them for ransomware.

Other Enhancements

- **CloudConnector Deployment:** Introduced bulk CloudConnector deployment using Terraform for streamlined setup.
- **SSO Integration:** Added Single Sign-On (SSO) support to enhance security and user management.
- **EC2 Restoration Workflow:** Implemented a new workflow to restore EC2 instances from the last known clean or infected EBS snapshots.
- **Expanded Filesystem Checks:** Added Filesystem corruption check support for Live Scan and AWS Backup.
- **Enhanced Reporting:** Introduced the ability to download any table as a CSV report for improved data analysis.
- **AWS Backup Integration:** Deepened integration with AWS Backups by adding direct links to AWS Backup Recovery Points from the Elastio UI.
- **Improved Misconfiguration Analysis:** Enhanced the misconfiguration drill-down feature with additional filters for more detailed insights.
- **Tag Propagation:** Implemented propagation of tags from EBS Volumes to Elastio-created resources during scans, supporting compliance and cost tracking.
- **Flexible On-Prem Inspections:** Added flexible scheduling options for inspecting on-premises workloads, with customers able to set separate schedules for malware and ransomware encryption scans based on business need.