Protect Your AWS Data from Ransomware

Isolate and recover your data from cyberthreats

Key Benefits

- Enterprise class backup service for AWS data sources and more
- Data isolation enhances protection against ransomware
- Fast and reliable recovery when you need it
- Enhanced security and access controls
- Flexible pricing options
- Available on AWS marketplace

Market trends and the rapid shift to remote work has accelerated cloud adoption and growth of your AWS data. Unfortunately, the looming threats of ransomware attacks have also rapidly increased in both frequency and damaging impact. Just because you moved to the cloud, doesn't mean you're safe. In fact, recent research conducted by Ermetic found that 70% of examined AWS environments contained machines that could be exploited by ransomware[1].

Your Cloud Data – Your responsibility

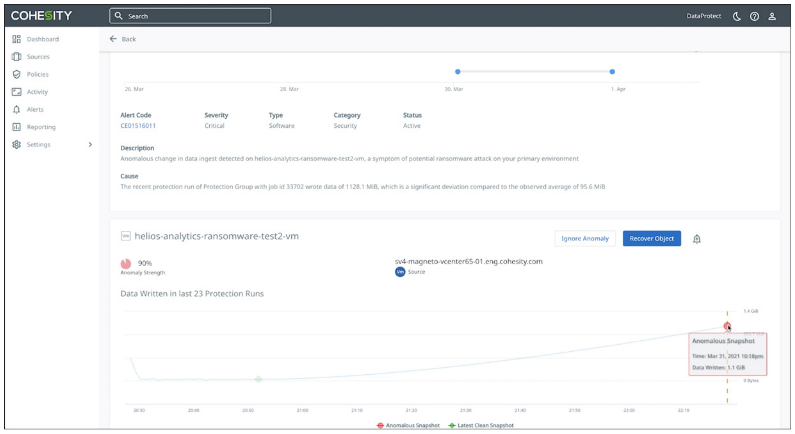
Cloud providers like AWS provide uptime SLAs and store multiple copies of data, but securing and protecting your data against ransomware is ultimately your responsibility. If and when an attack occurs, it will be your responsibility to figure out what happened and recover your data.

The Struggle with Snapshots

Most AWS services come with an optional snapshot feature that stores a copy of data on Amazon S3 for some added protection. The problem with snapshots is that they provide limited point in time capabilities (usually daily) and are managed and stored under the same AWS account as the production copy. So if your account is compromised by ransomware it's very easy for cybercriminals to get access to your snapshots and destroy them. That's not even considering snapshot limitations around app-consistency and slow recovery times when recovering data from native S3 to your production services.

Better Backup for AWS Helps Beat Cybercriminals

Cohesity DataProtect delivered as a Service is an enterprise class backup service that delivers ransomware protection for AWS workloads and more. It provides comprehensive, flexible, and efficient protection, helps isolate data from cyberattacks, and delivers fast and reliable recovery when you need it.



Alert Code	Severity	Type	Category	Status
CE01516011	Critical	Software	Security	Active

Description
Anomalous change in data ingest detected on helios-analytics-ransomware-test2-vm, a symptom of potential ransomware attack on your primary environment

Cause
The recent protection run of Protection Group with job id 33702 wrote data of 1128.1 MiB, which is a significant deviation compared to the observed average of 95.6 MiB

helios-analytics-ransomware-test2-vm

90% Anomaly Strength

sv4-magneto-vcenter65-01.eng.cohesity.com Source

Data Written in last 23 Protection Runs

Anomalous Snapshot
Time: Mar 31, 2021 10:18pm
Data Written: 1.1 GiB

[1] Ermetic, October 2021. "New Research: The Urgent Threat of Ransomware to S3 Buckets Due to Misconfigurations"

Cloud Needs Better Backup

More Protection

Protect Amazon EC2, Amazon RDS, and Amazon S3 with enterprise class backup while simultaneously delivering a unified backup solution across hybrid and multicloud by protecting other on-premises and SaaS workloads such as virtual machines, files, databases, and Microsoft 365.

More Flexible

Meet your business SLAs with flexible retention that allows you to keep data from a few days to indefinitely. Easily fulfill database portability, database migration, and cloud DR for business continuity requirements. Cohesity DataProtect also provides both flexible capacity and user based pricing options, and is available on the AWS marketplace to best meet your business needs.

More Efficient

Improve backup times and efficiency with fast incremental backups that reduces the data transferred across network boundaries. Further reduce costs, storage footprint, and backup and data transfer times with global variable block data deduplication.

Keep Data Away from the Bad Guys

Isolate Backup Data

Backup data is ingested to the Cohesity service and stored in a separate AWS account managed and secured by Cohesity. This creates an seperate copy of your data that is safely isolated making it difficult for cybercriminals to gain access if your account gets compromised.

Immutable Backups

Prevent tampering, modification, or deletion of your backup data. With Cohesity DataProtect, your backup data is stored in an immutable state making it possible to recover your data after a ransomware attack.

Secure Data and Access

Data is encrypted at rest and in transit with flexible key management using self managed or Cohesity managed Amazon KMS keys. SAML based single sign-on (SSO) and multi factor authentication (MFA) provides secured access.

Fast and Reliable Recovery

Clean Copy Restores

Ransomware can infect and lurk for weeks before launching an attack. Cohesity uses ML based anomaly detection to recommend the latest clean backup copy for fast and clean recoveries.

Global Search and Recovery

Whether recovering from a full scale attack or for forensics, Cohesity provides global granular search to find the most critical workloads or data to restore to help you recover more quickly and safely from an attack.

Flexible Recovery Location

With Cohesity you have the flexibility to restore data to its original location or to a completely different location and account to provide a clean recovery environment and prevent reinfection.

Stay One Step Ahead with Cohesity

Cloud is the new battleground where cybercriminals continue to work around the clock to threaten businesses and extort ransoms. With Cohesity DataProtect delivered as a service on your side, you can stay one step ahead with enterprise grade backup and protection, data isolation, and fast and reliable recovery against ransomware and other threats.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and © is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY.com | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110

3000081-002-EN 2-2024