Cohesity’s Solutions for Air-Gap Data Protection

Cohesity’s Security Approaches to Protect Your Data from Cyber Threats

ABSTRACT
Air gapping, a network security measure to ensure that at least one copy of critical data is stored on a secure network that is physically isolated from unsecured networks, is an essential component of any organization’s data-protection security strategy. Cohesity provides four simple methods for implementing air-gap protections in your data infrastructure.
Table of Contents

The Need for Air-Gap Data Protection ................................................................. 3
Air Gap to Cloud: Archive to Cloud or S3-Compatible Storage.......................... 5
Air Gap to NAS Target: Archive to NAS External Target ................................. 7
Air Gap to Cohesity Cluster: Replicate to Remote Cluster ............................... 9
Air Gap to Tape: Offsite Location .................................................................. 11
Your Feedback .............................................................................................. 13
About the Authors ......................................................................................... 13
Document Version History ............................................................................ 13

Figures

Figure 1: Air Gap Methods with Cohesity .......................................................... 4
Figure 2: Cohesity’s Cloud Air-Gap Solution ....................................................... 5
Figure 3: Recover from Cloud to Original or New Cluster ............................... 6
Figure 4: Cohesity’s NAS Air-Gap Solution with WORM ............................... 7
Figure 5: Recover from NAS External Target to Original or New Cluster ........ 8
Figure 6: Cohesity’s Replication Air-Gap Solution with DataLock ................. 9
Figure 7: Recover from Remote Cluster to Original or New Cluster ............... 10
Figure 8: Cohesity’s Archive to Tape Air-Gap Solution with QStar ASM ....... 11
Figure 9: Recover from Tape to Original or New Cluster ............................... 12
The Need for Air-Gap Data Protection

In the modern connected world, data is always at risk due to hackers, ransomware, and cyber threats. One of the methods that today's businesses adopt to combat this risk is by building multiple walls of security in their IT infrastructure. Traditionally, data has been protected by creating a copy (backup) of the primary data and storing it in an offsite location that is not connected to the network.

In the context of data management, the term ‘air gap' describes keeping a copy of the data in a location that cannot be accessed without being physically present, thus preventing malicious actors from attacking the data over the network. Enterprises require such protection around the clock, and need to deploy a strategy that ensures that a copy of the data is always remote and disconnected.

An air gap is not a replacement for your existing backup, recovery, or disaster recovery implementations, but, by being physically disconnected from hackers and ransomware attacks, it provides an additional layer of protection. Customers are asking, ‘How do we ensure that one copy of our data is always protected and kept where it is safe from attack?’

To achieve air-gap data protection, your solution must:

• Have an immutable file system, to protect the data from modification.
• Reside on an isolated network or in a separate physical location.
• Be able to prevent data deletion for a given period of time, to protect from insider attack.

Cohesity's platform provides multiple methods for implementing air-gap data protection, each with its own benefits and trade-offs. In addition to traditional tape archives, Cohesity offers three modern air-gap methods. The modern methods maintain network connectivity only during data transfer to the remote target and use WORM/DataLock/Object Lock storage to prevent modification and deletion of the remote copy.

Cohesity DataLock is a feature that empowers the Data Security role in Cohesity to prevent backed up, archived, and replicated data from being deleted until the DataLock expires, even by a user with the Data Security role.

DataLock is defined in a Cohesity Protection Policy and all runs of any Protection Group that uses that Policy inherit the DataLock. Disabling DataLock in the Protection Policy does not unlock any previously DataLocked data. A DataLocked snapshot can be deleted only after its retention period expires, regardless of the user's role. So DataLock meets all the criteria of WORM and is, as such, an ideal solution for air-gap data protection. DataLock is typically used for compliance and regulatory purposes and can be used as a WORM capability in our modern air-gap solution.
Understand and decide which method best suits your organization’s needs:

- **Cloud Air Gap**: Archive to Cloud or S3-compatible storage. A more modern approach that enables air-gap data protection with lower RTOs and RPOs by using archive to cloud or any S3-compatible storage that supports Object Lock and Object Versioning.

- **Air Gap to Target**: Archive to NAS External Target. This approach enables air-gap data protection with lower RTOs and RPOs by using archival to any NAS storage that supports WORM.

- **Air Gap to Cohesity Cluster**: Replicate to Remote Cluster. Cohesity can replicate data from your primary to remote clusters. In addition to acting as a disaster recovery (DR) solution, this also provides an air gap with lower RTOs and RPOs by using replication and Cohesity DataLock (Cohesity’s WORM feature).

- **Air Gap to Tape**: Offsite Location. Tape out the data from your backup and send the tapes after every archive to offsite storage, like Iron Mountain, ensuring that your data can never be accessed without physical access. Use Cohesity’s Archive-to-Tape capability to achieve the highest level of air-gap protection. However, the challenge with tape is that it leads to higher Recovery Time Objectives (RTOs) and missed Recovery Point Objectives (RPOs).

Cohesity’s platform allows you to choose the solution that best matches your operational needs, current infrastructure, and budget. You can even deploy several Cohesity methods to reap the benefits of each.
Air Gap to Cloud: Archive to Cloud or S3-Compatible Storage

Today, most organizations are moving out of tape and replacing it using object storage in the cloud. Cloud, with its cost economics, is acting as the viable long-term retention storage medium for both finite and infinite retention.

When you put a copy a backup in the cloud (that is, archive it) for air-gap protection, it needs to meet three requirements:

- **Immutability**, which is achieved using object versioning.
- **Prevent deletion of the data for a specified duration**, or indefinitely, using object locking.
- **Maintain a copy in a different location.**

Even though the archive in the cloud is connected to the network during the data transfer window, the copies on the AWS or S3-compatible storage are protected from modification by Object Versioning, and from deletion by Object Lock. It also delivers several key benefits to today’s modern data centers:

- **Provides shorter RTO and more frequent RPO.**
- **Physically separated from primary data in the cloud.**
- **Incremental forever archiving** with source-side deduplication and compression reduces network bandwidth requirements. (A significant benefit over tape archives, which require a full backup with each run.)
**NOTE:** Currently, this solution is supported for AWS S3, AWS Glacier, and any S3-compatible object storage that supports Object Lock and Object Versioning.

Note that today, Cohesity does not integrate directly with any versioning features available from cloud providers. This means that Cohesity will not be aware of versioning that is taking place in the background, which can lead to excess capacity being consumed in the archives, especially when the Object Lock is set to a longer period than the archive retention period. This is because when CloudArchive deletes archive snapshots that have passed the retention period, that data is not deleted from the object storage. Because this can lead to increased cloud storage costs when Object Versioning is enabled, we recommend that you carefully balance your archive retention and Object Lock periods.

In this solution, the archive is a fully self-contained copy of the backup stored on an External Target (in the cloud) that contains the backed-up data, metadata, and index. If, for any reason, the source cluster becomes unavailable, you can CloudRetrieve your data to a new cluster from the cloud archive, providing an additional layer of protection.

**Figure 3:** Recover from Cloud to Original or New Cluster

For detailed instructions on setting up Cohesity CloudArchive, see the [CloudArchive and CloudRetrieve Deployment and Recovery Guide for AWS](#). To implement this air-gap solution, when setting up your cloud archive, be sure to:

- Enable Object Lock and Object Versioning on the S3 bucket.
- Use a Protection Policy with [DataLock](#) enabled.
Air Gap to NAS Target: Archive to NAS External Target

The Cohesity platform supports archiving your data to a NAS External Target (on a Cohesity cluster or any other NAS-NFSv3-compatible storage) at regular intervals. Ensure the NAS External Target is on an isolated network behind a firewall & switch with access only to the primary cluster. Your network administrator can set up automation to enable the necessary ports only during the data transfer window and disable them again when data transfer completes. This ensures the data is isolated and air-gapped.

Figure 4: Cohesity’s NAS Air-Gap Solution with WORM

Even though the NAS External Target is connected to the network during the data transfer window, the copies on the External Target are protected from modification and deletion, as the NAS storage is configured with WORM. It also delivers several key benefits to today’s modern data centers:

- Provides shorter RTO and more frequent RPO.
- The archived data is stored on an immutable file system with WORM.
- Incremental forever archiving with source-side deduplication and compression reduces network bandwidth requirements. (A significant benefit over tape archives, which require a full backup with each run.)

In this solution, the archive is a fully self-contained copy of the backup stored on an External Target (NAS) that contains the backed-up data, metadata, and index. If, for any reason, the source cluster becomes unavailable, you can CloudRetrieve your data to a new cluster from the NAS External Target, providing an additional layer of protection.
For detailed instructions on setting up archives to a NAS External Target with Cohesity, see the CloudArchive and CloudRetrieve Deployment and Recovery Guide for NAS. To implement this air-gap solution, when setting up your NAS External Target, be sure to:

- Enable WORM on the NAS External Target.
- Use a Protection Policy with DataLock enabled.
Air Gap to Cohesity Cluster: Replicate to Remote Cluster

Another Cohesity strategy for air-gap data protection employs Cohesity replication with the **DataLock feature**. Using replication with DataLock solves two challenges:

- Provides a modern air-gap solution, as it can meet both requirements — can reside on an isolated network and supports WORM.
- Acts as disaster recovery (DR) solution by frequently replicating data from the primary to remote clusters.

Using replication with a DataLock Policy, a copy of the data is replicated to a Cohesity cluster at regular intervals. Ensure that the remote Cohesity cluster is on an isolated network behind a firewall with access only to the primary cluster. Your network administrator can set up automation to enable the necessary ports only during the data transfer window and disable them again when data transfer completes. This ensures the data is isolated and air-gapped.

Figure 6: Cohesity’s Replication Air-Gap Solution with DataLock

Even though the remote cluster is connected to the network during the data transfer window, the copies on that cluster are protected from modification, as the snapshot copies are immutable, and from deletion until DataLock expires. It also delivers several key benefits to today’s modern data centers:

- Provides shorter RTO and more frequent RPO.
- Recoveries from remote clusters are faster, as you can perform instant recovery.
- This configuration serves as a disaster recovery (DR) solution.
- Incremental forever replication with source-side deduplication and compression reduces network bandwidth requirements. (A significant benefit over tape archives, which require a full backup with each run.)

In this solution, recovery from the remote cluster is the same as recovery from your source cluster.
For detailed instructions on setting up replication with Cohesity, see Replication and Remote Access Setup in the online Help. To implement this air-gap solution, when setting up replication, be sure to use a Protection Policy with DataLock enabled.
Air Gap to Tape: Offsite Location

Archive-to-Tape is the approach of securing a copy of your data that can never be accessed remotely over the network by hackers and cyber threats like ransomware, because it requires physical access to retrieve the tape copy that is stored remotely.

Cohesity has partnered with QStar, a company established in tape libraries and drives, to provide an all-inclusive, data- and tape-agnostic archival solution that also serves as an air-gap strategy to secure your data from threats while also helping you achieve your long-term data retention and archival objectives.

Figure 8: Cohesity’s Archive to Tape Air-Gap Solution with QStar ASM

Cohesity’s Archive-to-Tape capability ensures that an unaltered copy of your data is available offsite by shipping the tape drives after every archive run.

IMPORTANT: To avoid the risk of previous backup copies being overwritten or compromised, use new tapes each time the data is archived.

While the RTO is higher with this solution, given that recovering from tapes is a slow process, and the RPO is higher, as full archives to tape are typically scheduled only once a week or month, it still offers unique benefits:

- A full copy of your data is remote and disconnected from all other data centers and networks.
- You can retrieve data from tape even if the source cluster is unavailable.
Figure 9: Recover from Tape to Original or New Cluster

For detailed instructions on setting up tape archives with Cohesity, see the Archive Data to Tape with QStar & Cohesity DataPlatform guide. To implement this air-gap solution, when setting up your tape archive, be sure to use a Protection Policy with DataLock enabled.
Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Adaikkappan Arumugam is Senior Manager, Tech Marketing, Solutions Engineering, & Tech Pubs at Cohesity. In his role, Adai focuses on connecting the technical expertise of Cohesity’s developer and product management staff with the needs and feedback from Cohesity’s customers, support staff, and sales enablement staff.

Other essential contributors included:

- Apurv Gupta, Chief Technology Officer
- Bart Abicht, Senior Technology Writer and Editor
- Sridhar Parimi, Senior Director, Engineering
- Sunil Moolchandani, Vice President, Product Solutions

Document Version History

<table>
<thead>
<tr>
<th>VERSION</th>
<th>DATE</th>
<th>DOCUMENT HISTORY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Mar 2020</td>
<td>Original document</td>
</tr>
<tr>
<td>1.1</td>
<td>Apr 2020</td>
<td>Minor updates</td>
</tr>
<tr>
<td>2.0</td>
<td>Apr 2020</td>
<td>Update with Cloud Air Gap</td>
</tr>
</tbody>
</table>
ABOUT COHESITY

Cohesity radically simplifies data management. We make it easy to protect, manage, and derive value from data -- across the data center, edge, and cloud. We offer a full suite of services consolidated on one multicloud data platform: backup and recovery, disaster recovery, file and object services, dev/test, and data compliance, security, and analytics -- reducing complexity and eliminating mass data fragmentation. Cohesity can be delivered as a service, self-managed, or provided by a Cohesity-powered partner.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.

© 2021. Cohesity, Inc.

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 (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

2000027-003-EN