COHESITY

Version 1.1

April 2020

Cohesity's Solutions for Air-gap Data Protection

Cohesity 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 two simple methods for implementing air-gap protections in your data infrastructure.

Table of Contents

1 The Need for Air-Gap Data Protection 3
2 Traditional Air Gap: Archive to Tape 5
2.1 Archive to Tape Using QStar ASM 5
3 Modern Air Gap: Archive to NAS and Replication 7
3.1 Archive to NAS External Target with WORM 7
3.2 Replicate to Cohesity Cluster with DataLock Policy 9
4 Your Feedback 11
5 About the Authors 11
6 Document Version History 11

Figures

Figure 1: Air Gap Methods with Cohesity 4
Figure 2: Archive to Tape — Traditional Air-gap Data Protection 5
Figure 3: Recover from Tape to Original or New Cluster 6
Figure 4: Archive to NAS External Target with WORM — Modern Air-gap Data Protection 7
Figure 5: Recover from NAS External Target to Original or New Cluster 9
Figure 6: Replicate to Cohesity Cluster with DataLock — Modern Air-gap Data Protection 10

Tables

Table 1: Archive to Tape — Air Gap Benefits and Trade-offs 6
Table 2: Archive to NAS External Target with WORM — Air Gap Benefits and Trade-offs 8
Table 3: Replicate to Cohesity Cluster with DataLock — Air Gap Benefits and Trade-offs 10

1 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.

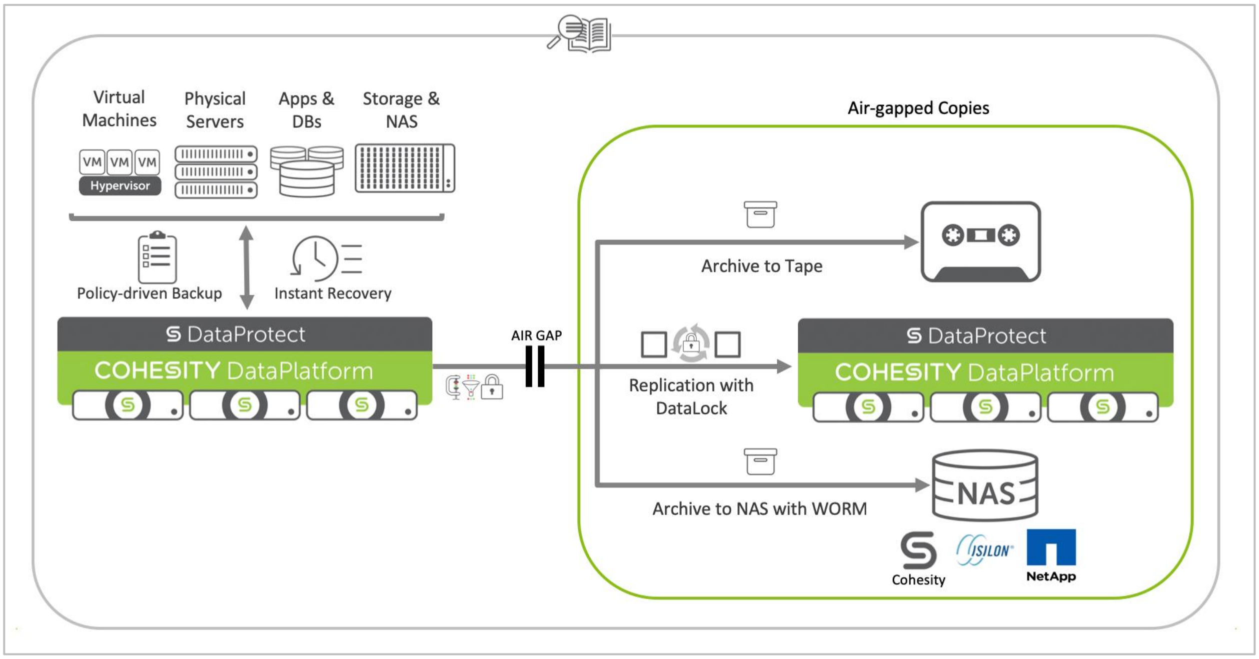
In the context of data management, the term ‘air gap’ describes keeping a copy of the data in a location that cannot be accessed without being physically present, thus preventing malicious actors from attacking the data over the network. Enterprises require such protection around the clock, and need 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?’

Cohesity’s platform provides multiple methods for implementing air-gap data protection, each with its own benefits and tradeoffs. Understand and decide which method best suits your organization’s needs.

- **Traditional Air Gapping (Physical)**. 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 DataPlatform’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).
- **Modern Air Gapping (Virtual)**. Cohesity also supports a more modern approach that enables air-gap data protection with lower RTOs and RPOs by using replication or archival to remote External Targets. Flexible air gapping maintains network connectivity only during data transfer to the remote Target and uses WORM (Write Once Read Many) semantics to keep the remote copy immutable.

Figure 1: Air Gap Methods with Cohesity



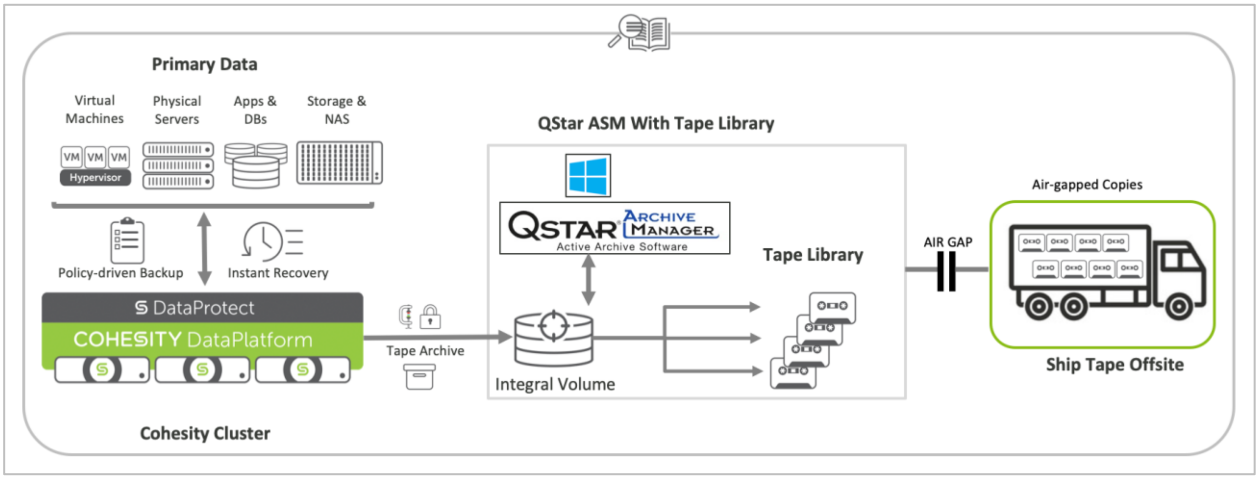
Choose the traditional or modern approach based on the trade-offs and your organization's operational needs. Or take the best of both worlds by using both Archive to Tape *and* Replication, to avoid compromising on RTOs and RPOs while also leveraging the physical separation of tape. Cohesity's platform allows you to choose the solution that best matches your operational needs, current infrastructure, and budget.

2 Traditional Air Gap: Archive to Tape

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 2: Archive to Tape — Traditional Air-gap Data Protection



2.1 Archive to Tape Using QStar ASM

Cohesity DataPlatform'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.

At a high level, the steps to archive your data to a tape library include but are not limited to:

1. Install a QStar tape environment.
2. On Cohesity DataPlatform, create an External Target that connects to your QStar tape library.
3. Create a Cohesity Protection Policy that archives your data to that External Target in the QStar tape library.
4. Physically ship the archive tapes to an offsite location.

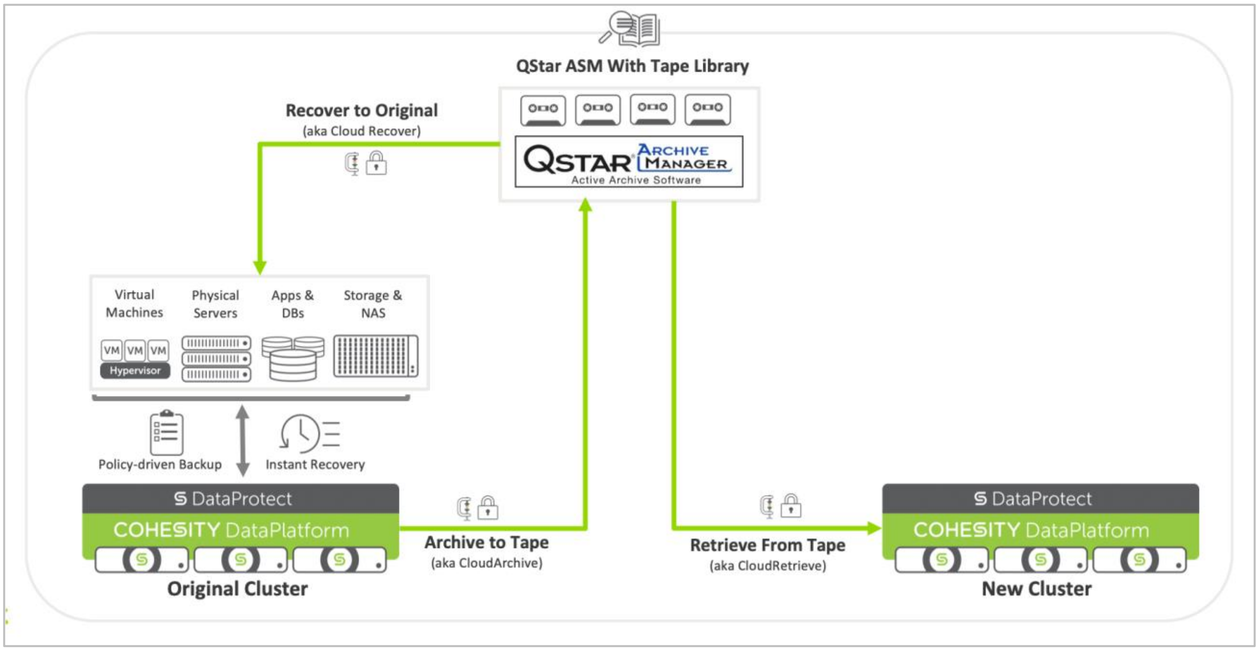
For detailed instructions, see the Archive Data to Tape with QStar & Cohesity DataPlatform guide.

Table 1: Archive to Tape — Air Gap Benefits and Trade-offs

BENEFITS	TRADE-OFFS
A full copy of your data is remote and disconnected from all other data centers and networks.	RTO is higher given that recovering from tapes is a slower process.
Retrieve data from tape using Cohesity CloudRetrieve even if the source cluster is unavailable.	RPO is higher as full archives to tape are typically scheduled only once a week or month, at best.

In this solution, the archive is a fully self-contained copy of the backup stored on an External Target (tape) 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 tape library, providing an additional layer of protection.

Figure 3: Recover from Tape to Original or New Cluster



3 Modern Air Gap: Archive to NAS and Replication

Organizations running mission-critical applications require near-real-time data snapshots with lower RPO/RTO and a faster recovery process to bring applications back online. This is critical for business agility and continuity. Cohesity solves this challenge in a flexible and modern way while keeping copies of your data safe from attack.

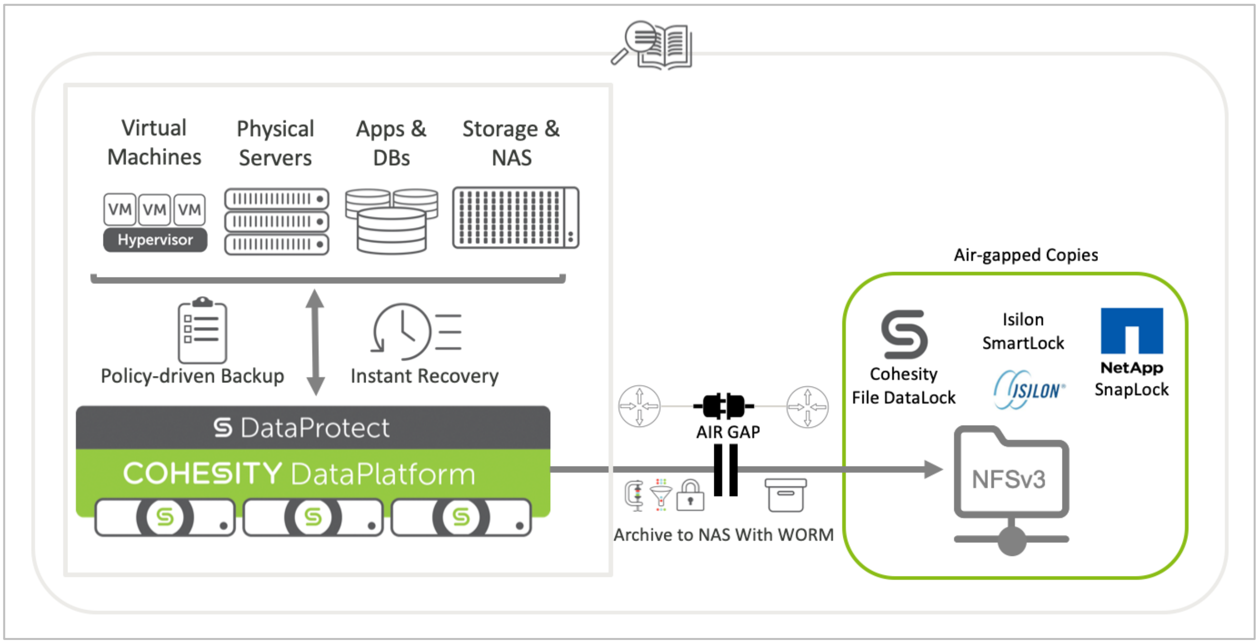
Cohesity DataPlatform supports two approaches to implement this modern, or virtual, strategy: archive to NAS and replication to another Cohesity cluster. In both approaches, there are two requirements:

- The NAS External Target or Cohesity cluster should be in an isolated network and disconnected from the enterprise network except temporarily, during data transfer.
- The External Target should support WORM (Write Once Read Many) technologies that ensure the immutability of the data that is written.

3.1 Archive to NAS External Target with WORM

Cohesity DataPlatform supports the archive of 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: Archive to NAS External Target with WORM — Modern Air-gap Data Protection



At a high level, the steps to archive your data to NAS (from a Cohesity NFS View) include but are not limited to:

1. Configure your NAS and enable WORM.
2. Create a NAS External Target (NAS Archive) on the cluster to point to a Cohesity NFS View.
3. Create a Cohesity Protection Policy that archives your data to that NAS External Target.

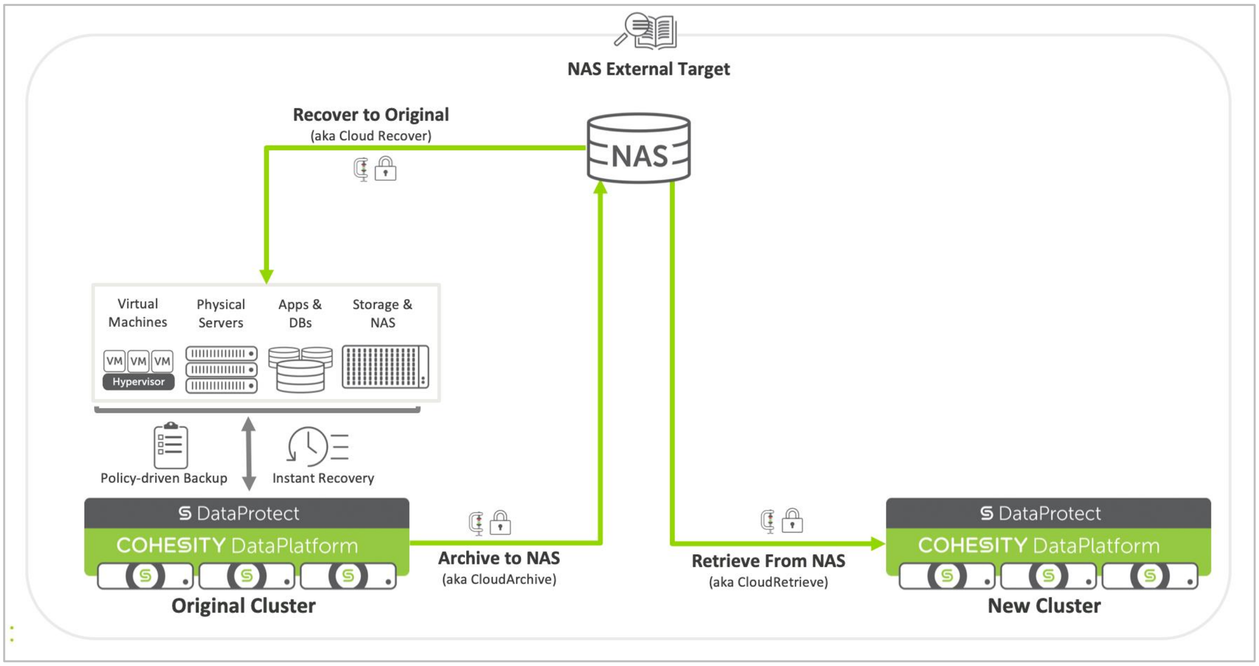
For detailed instructions, see the CloudArchive & CloudRetrieve Deployment & Recovery Guide for NAS guide.

Table 2: Archive to NAS External Target with WORM — Air Gap Benefits and Trade-offs

BENEFITS	TRADE-OFFS
Provides shorter RTO and more frequent RPO.	The NAS External Target is accessible to the rest of the enterprise network during the data transfer window.
The archived data is immutable with WORM.	
Incremental forever archiving with source-side deduplication and compression reduces network bandwidth requirements.	

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.

Figure 5: Recover from NAS External Target to Original or New Cluster



3.2 Replicate to Cohesity Cluster with DataLock Policy

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

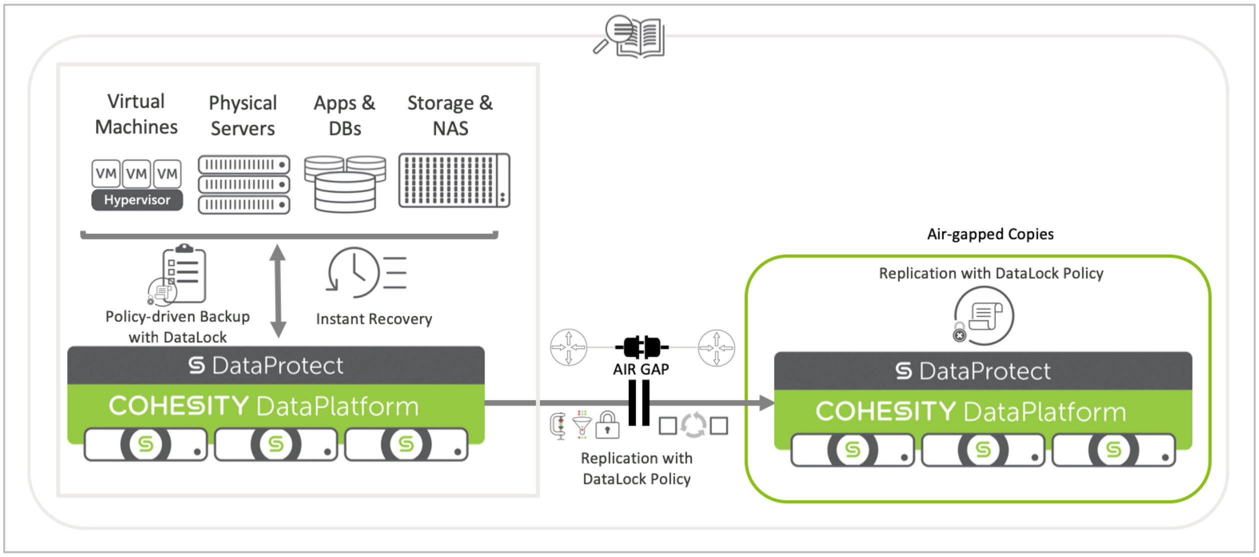
- Provides a modern air-gap solution, as it can meet both requirements — can reside on an isolated network and supports WORM.
- Acts as disaster recovery (DR) solution by frequently replicating data from the primary to remote clusters.

DataLock is a feature that empowers the Data Security role in Cohesity DataPlatform 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.

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: Replicate to Cohesity Cluster with DataLock — Modern Air-gap Data Protection



To use Cohesity Replication to implement air-gap data protection:

1. Configure a second Cohesity cluster.
2. Add a remote (second) cluster on the primary cluster.
3. Create a Protection Policy with DataLock enabled and add Replication to the second cluster.

Table 3: Replicate to Cohesity Cluster with DataLock — Air Gap Benefits and Trade-offs

BENEFITS	TRADE-OFFS
Provides shorter RTO and RPO.	The cluster is accessible to the rest of the enterprise network during the replication window.
The replicated data is immutable and cannot be deleted until DataLocked expires.	
Recoveries from replicated clusters are faster and serve as a disaster recovery (DR) solution.	
Incremental forever replication with source-side deduplication and compression reduces network bandwidth requirements.	

4 Your Feedback

Was this document helpful? Send us your feedback!

5 About the Authors

Sridhar Parimi is Senior Director, Engineering, at Cohesity. In his role, Sridhar focuses on enterprise data protection and software usability.

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 Architect
- Sunil Moolchandani, VP, Product Solutions

6 Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.0	Mar 2020	Original Document
1.1	April 2020	Minor updates

ABOUT COHESITY

Cohesity ushers in a new era in data management that solves a critical challenge facing businesses today: mass data fragmentation. The vast majority of enterprise data — backups, archives, file shares, object stores, and data used for dev/test and analytics — sits in fragmented infrastructure silos that makes it hard to protect, expensive to manage, and difficult to analyze. Cohesity consolidates silos onto one web-scale platform, spanning on-premises, cloud, and the edge, and uniquely empowers organizations to run apps on that platform — making it easier than ever to back up and extract insights from data. Cohesity is a 2019 CNBC Disruptor and was named a Technology Pioneer by the World Economic Forum.

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

The information in this publication is provided "as is" for information purposes only. Cohesity, Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

2000027-002-EN