COHESITY

Deploying the Cohesity Clean Room solution

Quick Guide

The Cohesity Clean Room solution provides a trusted environment that speeds incident response and supports SecOps investigations while minimizing the risk of secondary attacks.

Thanks to a modular design, Cohesity rapidly creates an isolated environment, supporting the response and recovery process and allowing teams to mitigate threats faster.

Our staged approach

1 **Prepare**
Prepare for a cyberattack

2 **Initiate**
Build Minimum Viable Response Capability (MVRC)

3 **Investigate**
Determine the scope and cause of the attack

4 **Mitigate**
Remediate, patch, harden, test

5 **Recover**
Last mile validation and trusted production recovery

STAGE 1

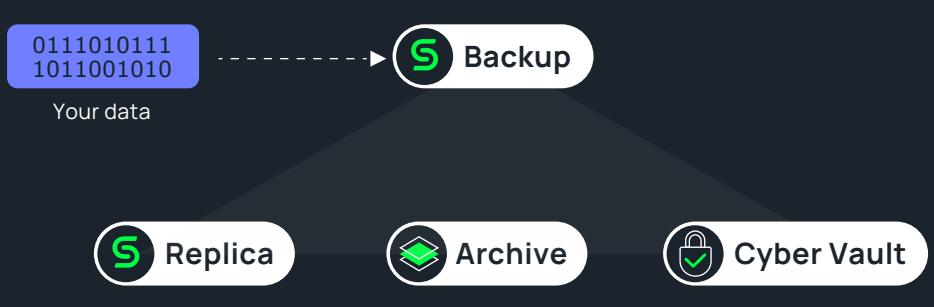
Prepare

The Prepare stage focuses on taking proactive measures to reduce the impact of an attack so businesses have trusted resources available when they need them.

3-2-1 backup rule

Create at least 3 copies of your data.

(2 copies stored onsite on different media and 1 copy stored offsite)

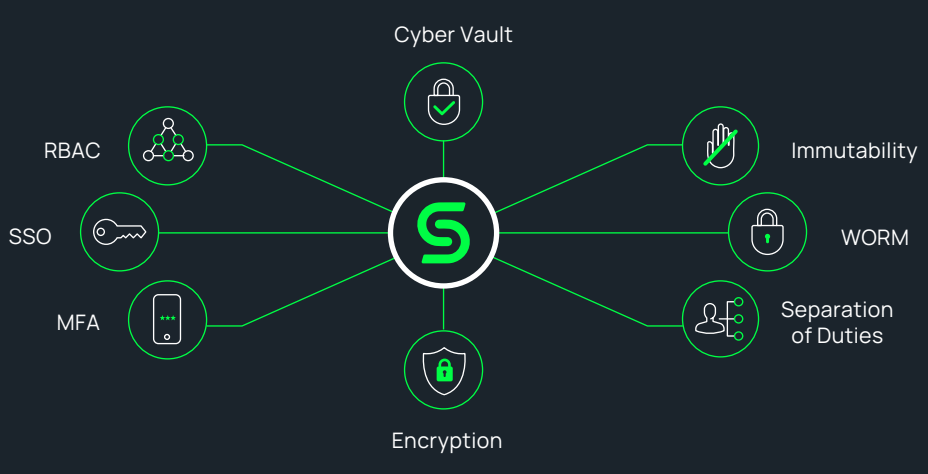


Deployment Topologies

		Backup	Replication	Dual-Replication	Archive	Dual-Archive
Basic (2 or fewer copies)	Topology 1	✓	-	-	-	-
	Topology 2	✓	✓	-	-	-
	Topology 3	✓	-	-	✓	-
Enhanced (3 copies)	Topology 1	✓	✓	-	✓	-
	Topology 2	✓	-	✓	-	-
Mission-Critical (4 or more copies)	Topology 1	✓	-	✓	✓	-
	Topology 2	✓	✓	-	-	✓
	Topology 3	✓	-	✓	-	✓

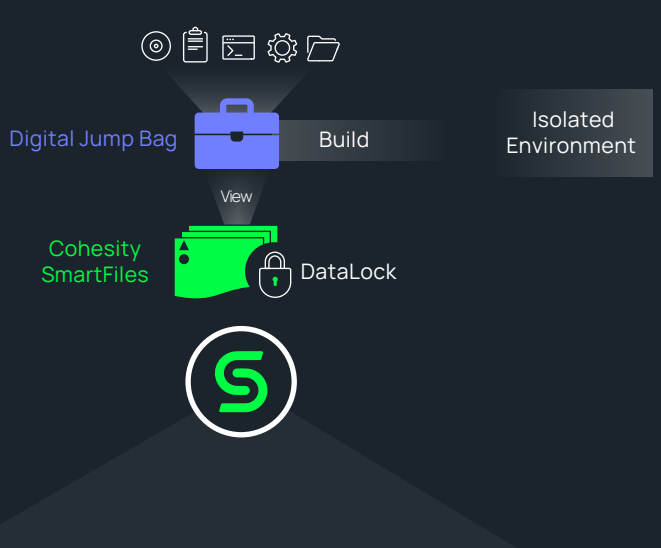
Harden your Cohesity platform

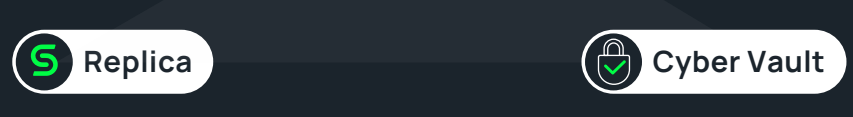
Enhance the security of your data by implementing proactive measures to reduce vulnerabilities and mitigate potential risks.



Get your digital jump bag™ ready

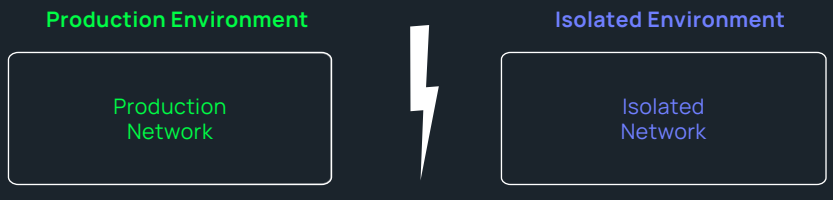
Prepare a software repository on Cohesity SmartFiles View to keep golden images of your critical workloads' ISO, software, configuration files, documents, templates, etc., which is necessary for building the isolated environment.





Isolate your network

Plan for network segmentation to ensure the isolated environment is completely disconnected from the production network using either a dedicated network switch or VLAN.



Establish communication protocols

A clear communication protocol ensures efficient coordination, reduced confusion, and minimized downtime.

Process	Purpose
Roles and Responsibilities	Ensures Accountability. You can assign specific tasks to team members (incident coordinators, IT responders, legal advisors, and executives) who make decisions.
Communication Channels and Tools	Secure and Centralized Communication. Establish dedicated channels like Slack or Microsoft Teams for internal communication (VPN enabled) and ProtonMail for secure external updates.
Communication Plan	Effective Coordination. Create a structured plan using tools like Confluence or Google Docs, detailing who communicates what and when during recovery stages.
Regular Updates	Real-time Update. Use dashboards in ServiceNow or PagerDuty to inform all stakeholders of progress and next steps.

STAGE 2

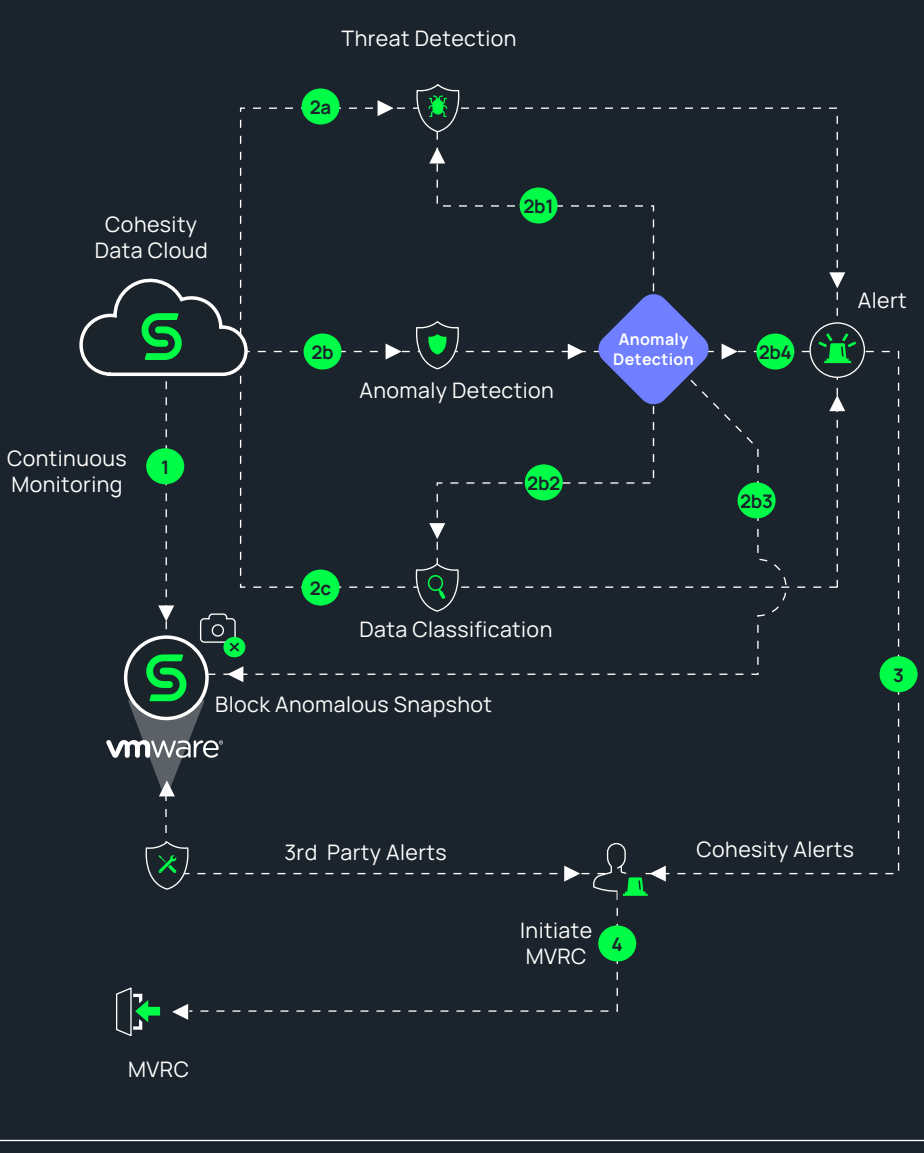
Initiate

The initiate stage involves establishing a Minimum Viable Response Capability (MVRC), which encompasses critical tools and processes necessary to contain the breaches, restore essential operations, and minimize downtime to help ensure operational continuity during cyberattacks.

1

Detect cyberattack

Cyberattacks are either automatically detected by Cohesity anomaly and threat detection or by a customer using other security tools. As soon as the cyberattack is detected, the initiate stage begins.



2

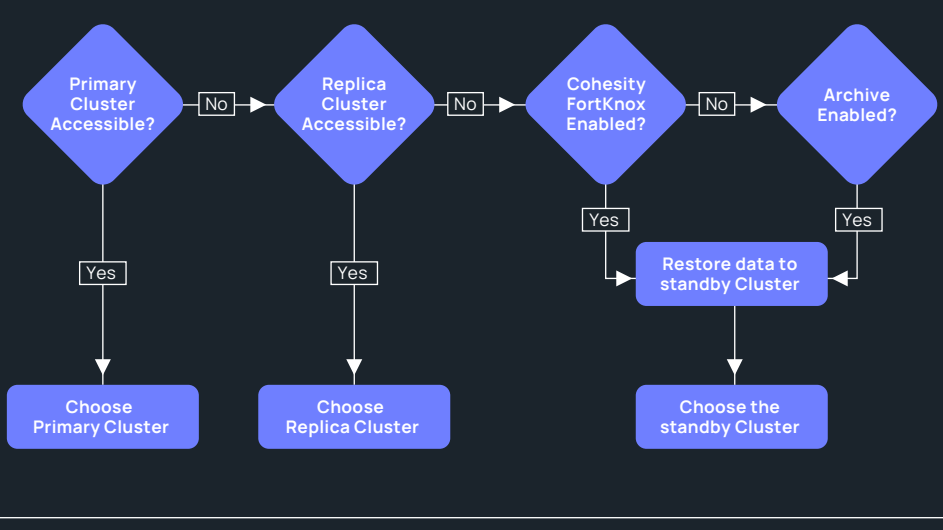
Identify the Cohesity Source Cluster

Identify the Cohesity Source Cluster from which to retrieve the data/snapshots for forensic analysis in the Clean Room.

Select the data or snapshot to be used for forensic analysis from the Cohesity Source Cluster.

Location	Form Factors
Self-Managed On-Premise Locations/ Data Centers	• Primary Cluster • Replication Cluster • Virtual air-gapped Replication Cluster • NAS Archive
Cloud	• FortKnox (Vir tual air-gapped cyber vault) • Cloud Archive (AWS / Azure / GCP)

Cohesity can recover data from any of the above form factors.

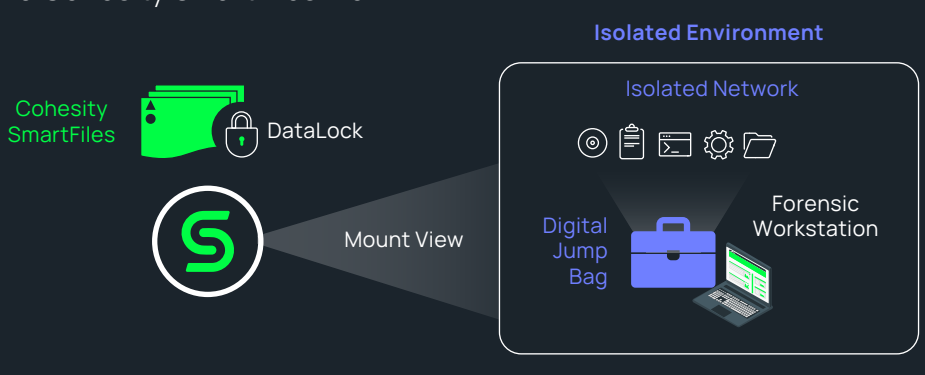


3

Retrieve your digital jump bag

Mount the digital jump bag on a host in the Clean Room.

As discussed in the Prepare stage, a digital jump bag is on a Cohesity SmartFiles View.



Digital jump bag retrieval strategies

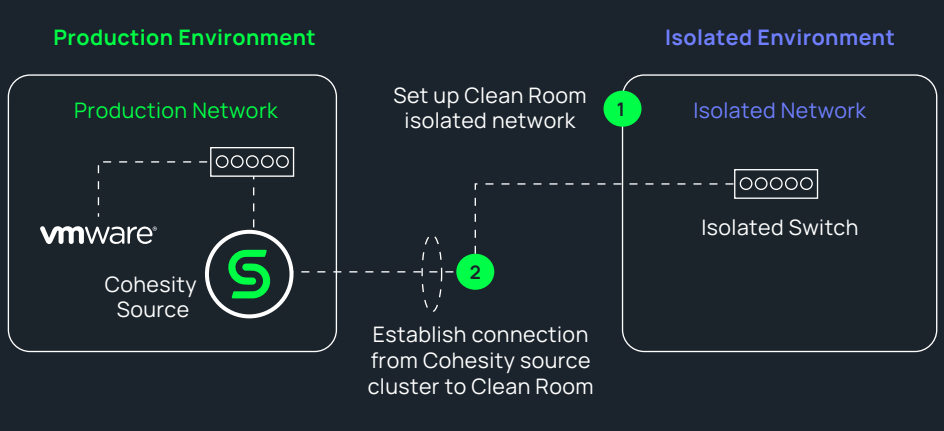
Location	Description	Use case
Primary Cluster	Cohesity Cluster in DC or production location	• When your production environment is trusted • For security drills
Isolated Replica Cluster	Cohesity Cluster on the DR site has the replicated copy	• When Primary Cluster is down • To retrieve a digital jump bag on the DR site
FortKnox	Cohesity secured vaulting solution	• When both primary and replicated clusters are inaccesible

---

4

Set up an isolated Clean Room network

As discussed in Prepare stage, set up an isolated network in Clean Room and establish connection between Clean Room and your Cohesity Source (chosen in previous step).

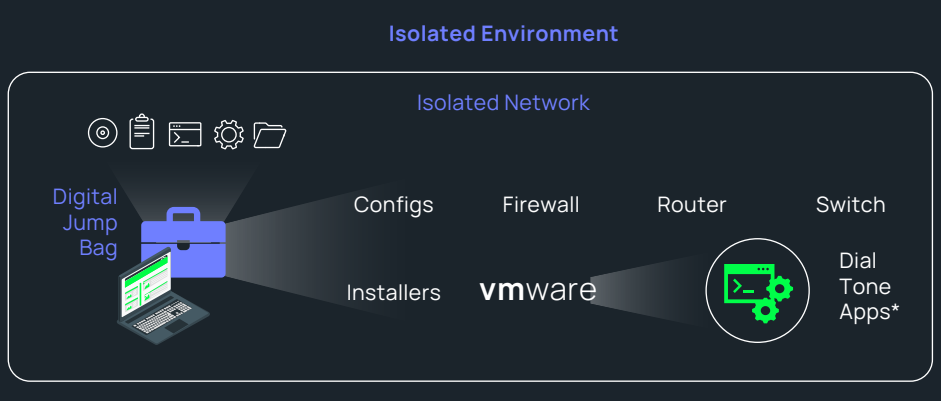


5

Set up your Clean Room infrastructure

Build your clean room infrastructure from digital jump bag components.

Use your digital jump bag to set up Network Components, Virtual Environment and Dial Tone Applications in the Clean Room.



The Virtual Environment installed in the Clean Room must be registered as a source on the Cohesity Source Cluster (Production or Replication), from which you intend to restore the snapshots to Clean Room for investigation

*Dial Tone Applications are essential business functions such as phone systems, IAMs, emails, DNS, security tools, etc.

STAGE 3

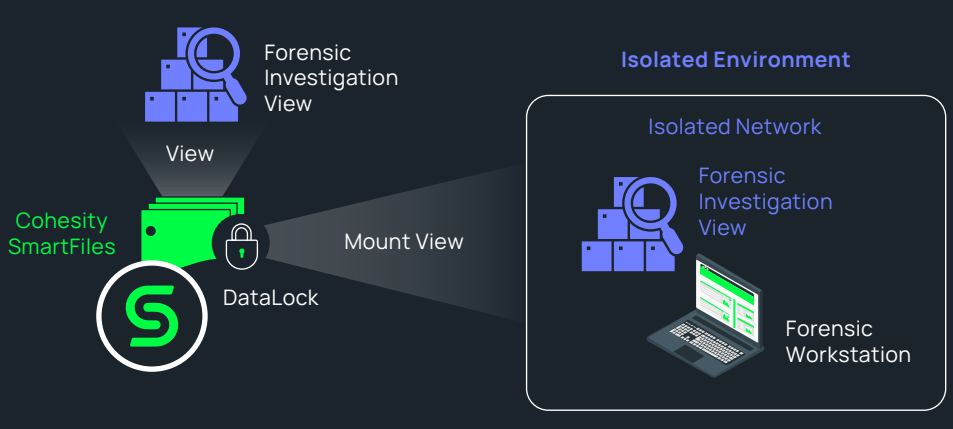
Investigate

The investigate stage focuses on understanding the scope and impact of the cyberattack, identifying the cause of the attack, assessing how deeply it has affected the system, and preserving evidence for further investigation.

1

Create a forensic investigation view

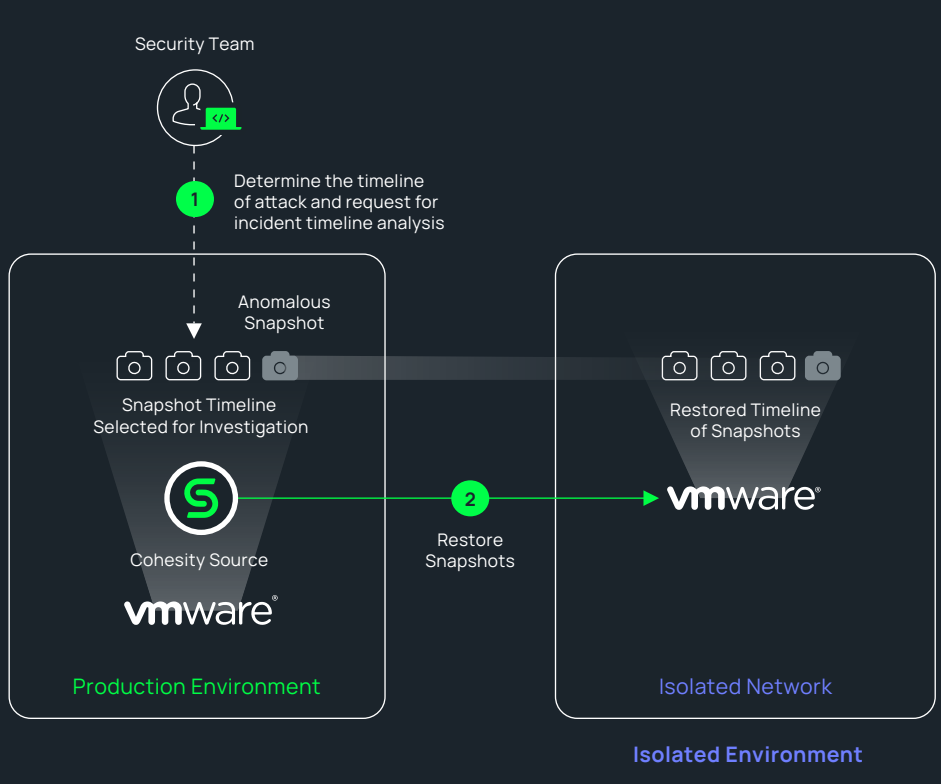
Prepare a forensic repository on Cohesity SmartFiles View for forensic evidence collection. Then mount this forensic investigation view onto a forensic workstation in the Clean Room.



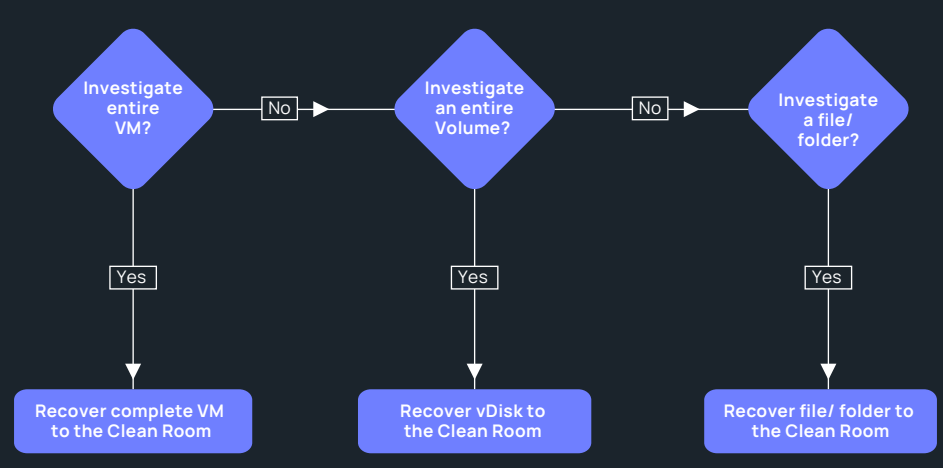
2

Restore systems and data of interest for investigation

Restore systems, volumes, and files/folders of interest with other collected evidence into the Clean Room. Determine the timeline of events and correlate details of the attack to be used for mitigation.

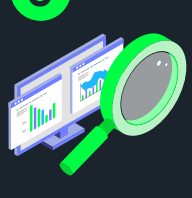


Choose your recovery method



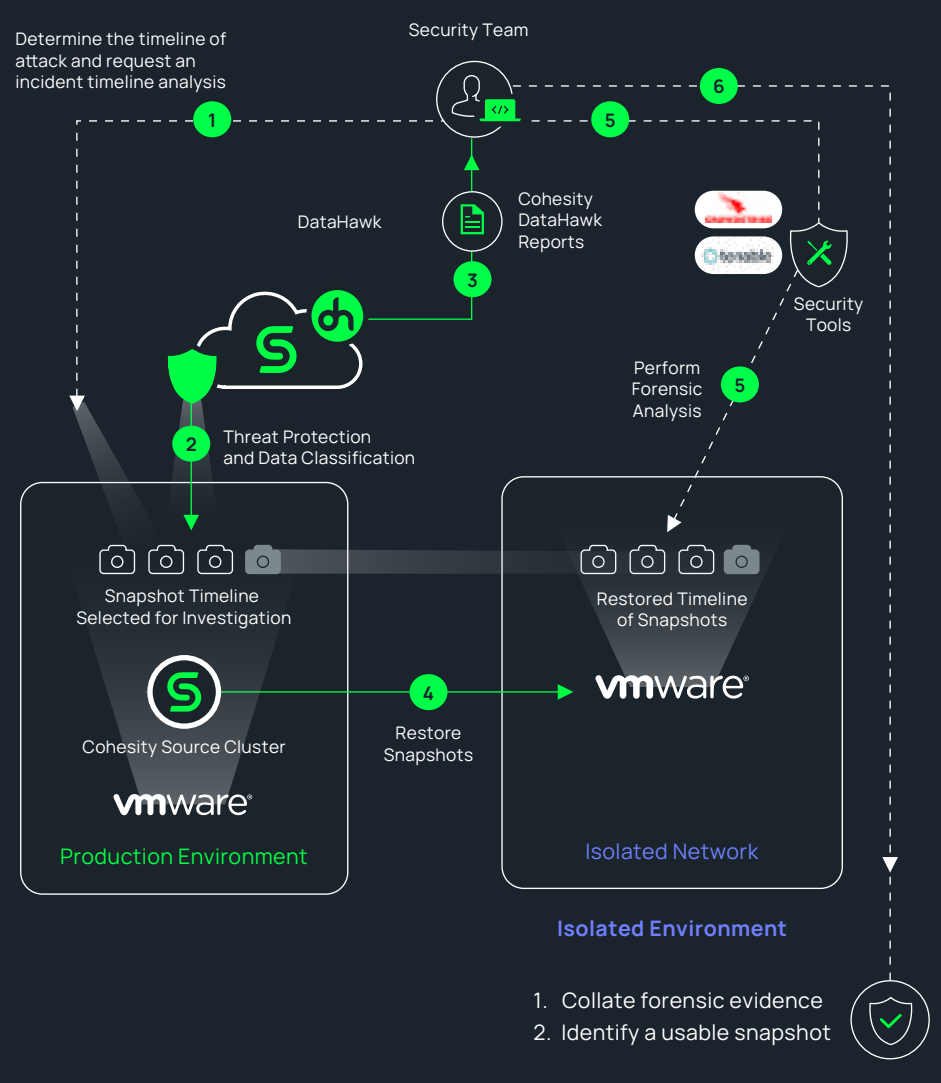
*Based on your SecOps decision, choose whether to restore an entire volume, folder, or file.

3



Perform a forensic investigation

Perform a forensic examination of the restored snapshots in the Clean Room using security tools and Cohesity DataHawk reports.



- Involve your Incident Response teams during Forensic Investigation.
- Compare Active Directory changes to ensure integrity of user accounts, permissions, and configurations.

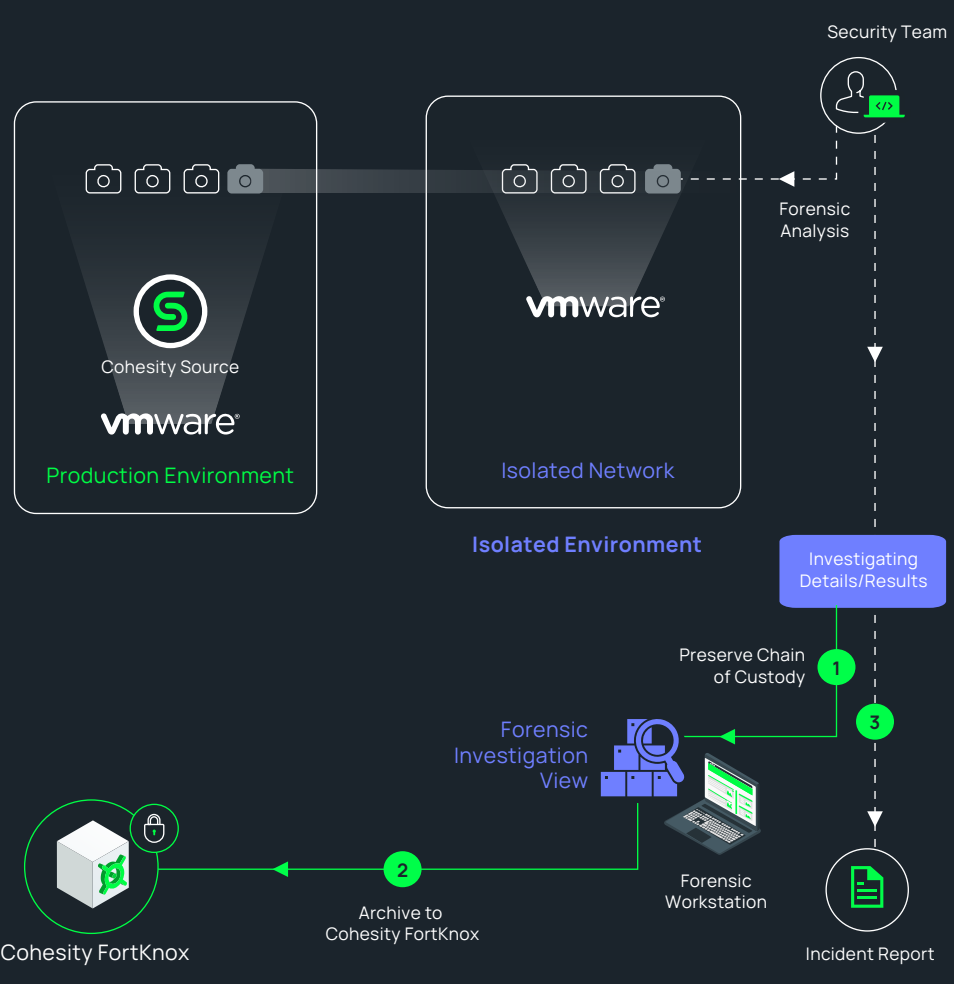
Recommendation
Use Cohesity DataProtect to secure your Active Directory and compare your AD snapshots effortlessly.

[1]DataHawk operations are performed on the desired range of snapshots within the period of interest.
[2]The desired range of snapshots are restored to the Clean Room and investigation is performed on them.

4

Preserve forensic evidence

Collect all the forensic investigation details and results and preserve them in the Forensic Investigation View created in Step 1.



Outcomes of the Investigate stage

- Create a usable snapshot to use for mitigation.
- Create an incident report detailing remediation and eradication steps.

STAGE 4

Mitigate

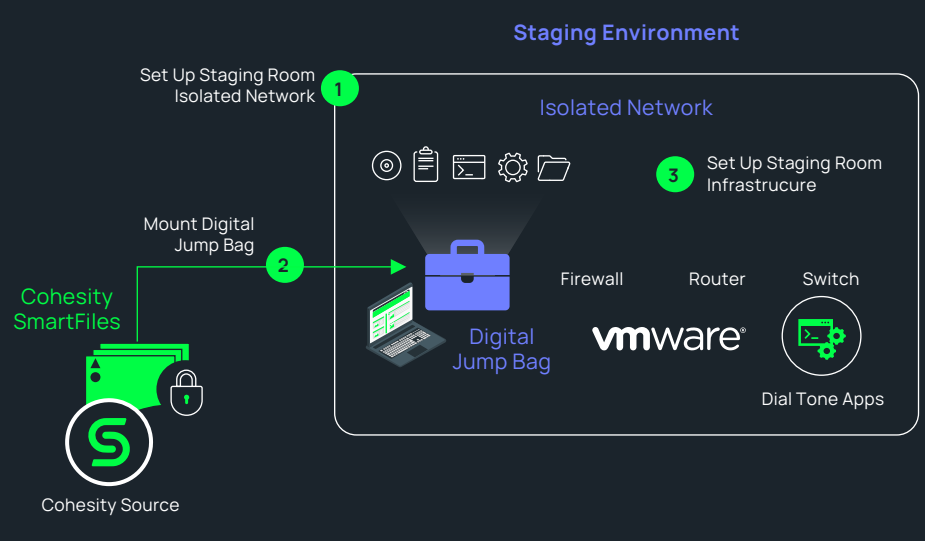
The mitigate stage focuses on taking steps to limit the damage, recover and test the affected systems in a staged environment, remove the malware from the network, and prevent further infections.

1

Set up a staging room

A staging room is an isolated and controlled environment like a clean room, where data and systems undergo comprehensive remediation and validation so they're free from threats or corruption.

Follow the same steps for preparing a staging room as you did for preparing a clean room. See the Initiate stage for details.



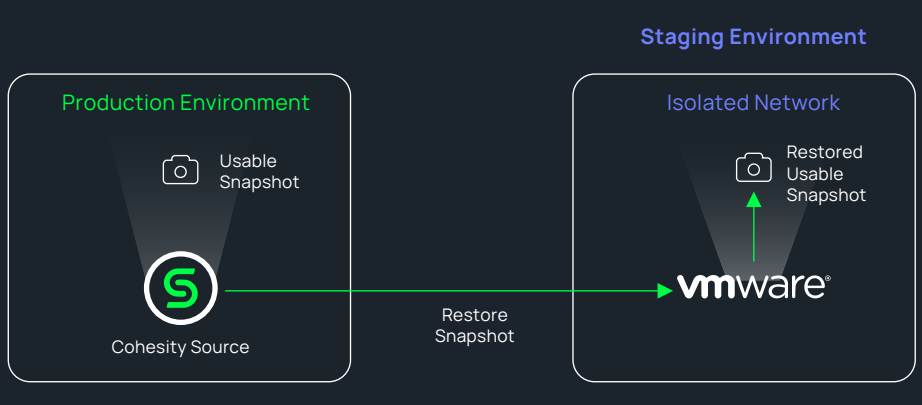
2

Recover your system and data

Recover the system and data to the staging room for remediation.

Decide whether to restore or rebuild the system and data

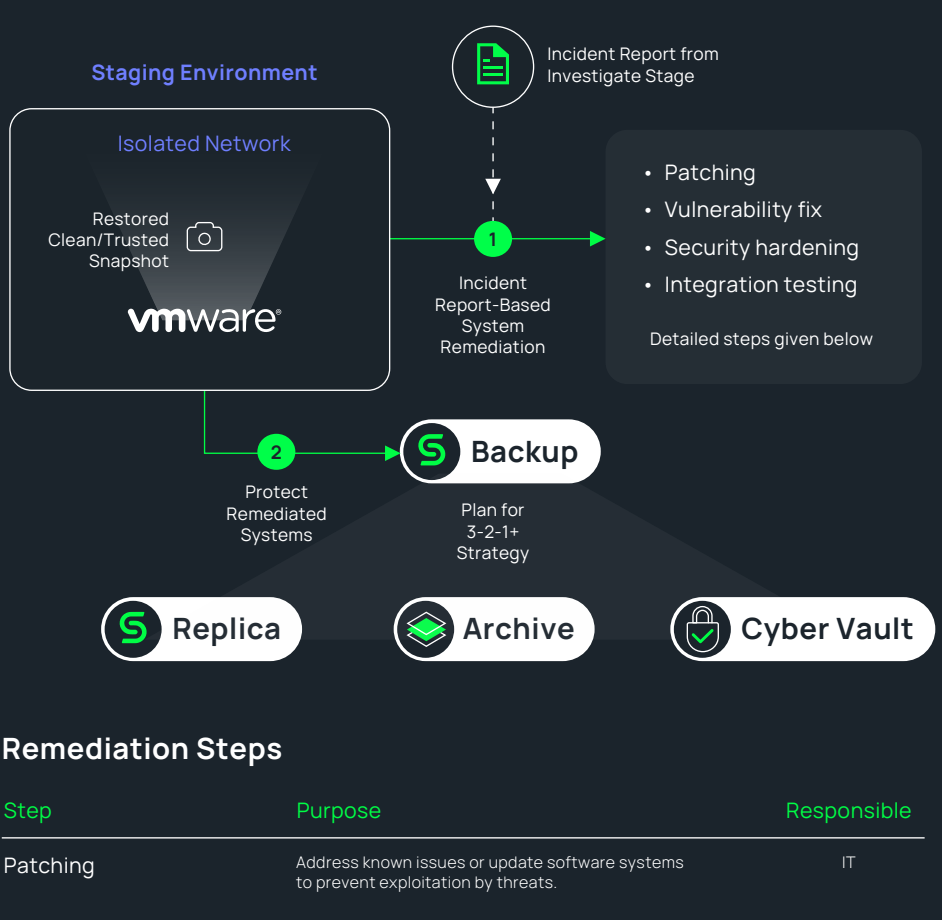
1. Restore both the system and data from a Cohesity backup to the staging room and remediate it.
2. Rebuild the system entirely from golden images in the staging room. Recover the data from Cohesity backup to the staging room for remediation.



3

Remediate

Use the incident report from the Investigate stage to remediate the affected workloads.



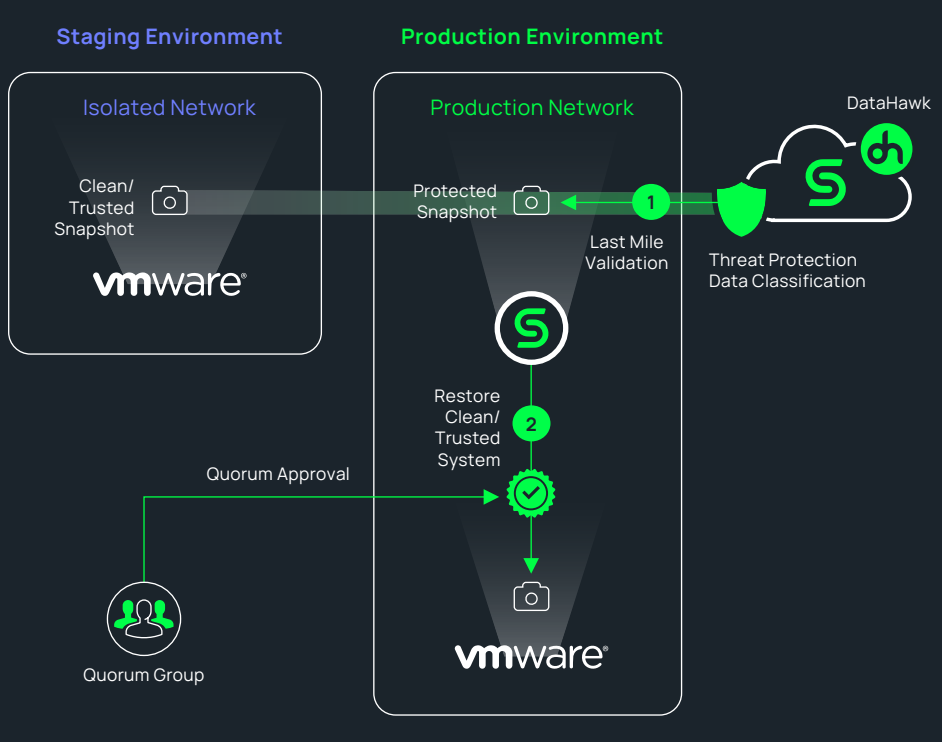
Remediation Steps

Step	Purpose	Responsible
Patching	Address known issues or update software systems to prevent exploitation by threats.	IT
Vulnerability Fix	Address security weaknesses and loopholes in systems to prevent exploits and attacks, including patching the systems.	IT
System Hardening	Enhance a system's security by minimizing its attack surface and applying security controls to guard against threats and unauthorized access.	IT/Security
Integration Testing	Ensure different components and systems work together seamlessly and identify and resolve any issues before deployment to the production environment.	IT/Security

STAGE 5

Recover

The recover stage focuses on final validation and secure recovery of clean systems to production along with the implementation of long-term changes to prevent future attacks.



RESOURCES

Blog
Introducing the Cohesity clean room design.
Read Now

Blog
Data clean rooms done right in a world of destructive cyberattacks.
Read Now

White Paper
Building cyber resilience in a world of destructive cyberattacks.
Read Now

Video
Cohesity Clean Room: Delivering resilience to destructive cyberattacks.
Watch Now

Video
Tech Insights - Using a clean room for security investigations.
Watch Now

Webinar
How to use a clean room for incident response.
Watch Now