COHESITY

Version 3.2

July 2024

Cohesity Ransomware Protection — Prepare and Recover

Protect Your Data Assets from Today's Growing Ransomware Attacks

ABSTRACT

Backup is your last line of defense against crippling ransomware attacks, which increasingly put organizations at risk in today's landscape. Unfortunately, backup data has lately become the prime target of sophisticated ransomware attacks. Cohesity's best-in-class anti-ransomware solution protects, isolates, detects, and rapidly recovers your data to reduce downtime and ensure business continuity. Cohesity also offers a host of security controls and best practices to help protect your data and resources from intrusion, encryption, or destruction.

Table of Contents

Figures

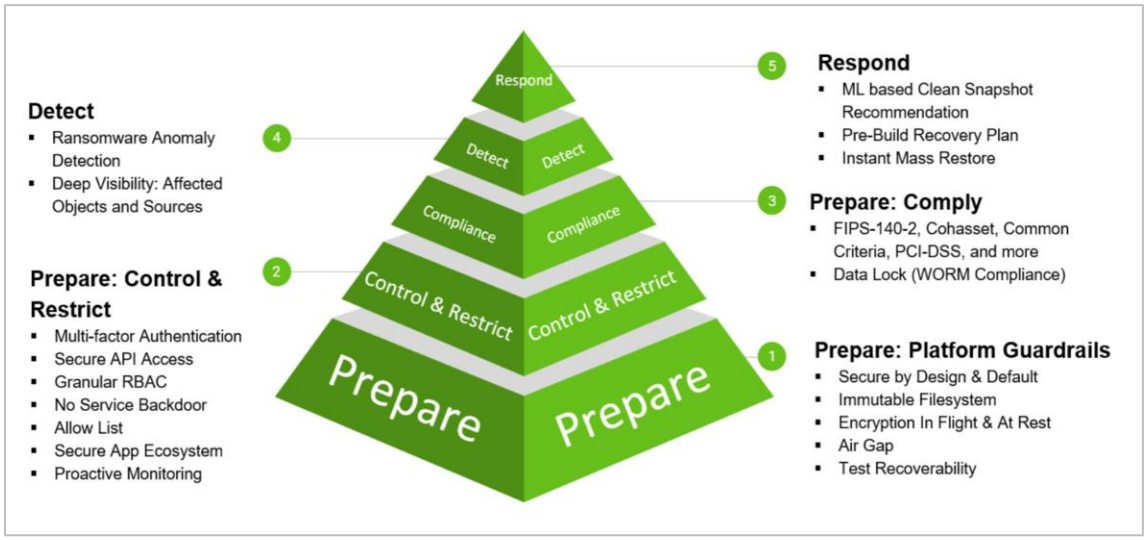
Tables

The Need for a Strong Security Posture

Each day, organizations block several cyberattacks that put their systems and data at risk. Hackers specifically use ransomware to take your critical enterprise data hostage and make it inaccessible through encryption, demanding an exorbitant ransom to decrypt or restore it. Ransomware attacks result in customer distrust and significant loss of data, revenue, productivity, and resources, which take a long time to recover. To put up a strong defense against these attacks, organizations take proactive preventive measures and strive to build a resilient security posture.

Given such a cybersecurity climate and the multitude of breaches that recur across industries worldwide, Cohesity works with partners and customers to provide robust guidance around preparing for and protecting your organization's data against ransomware. In this guide, we provide a set of recommendations that will improve the security of data that resides in your Cohesity environment.

Figure 1: Cohesity's Framework against Ransomware Attacks



You can use the measures outlined in this document that are relevant to your organization's security requirements as a framework to further secure data in your environment.

Some exploits are designed for compromising on-premises systems in limited and targeted attacks. In such instances, which are part of more extensive ransomware campaigns, threat actors attempt to exploit weak password configurations and administrative commands with the direct intent to compromise data backups.

Due to the increase in volume and severity of security threat activities by bad actors, Cohesity strongly recommends that you adhere to the best practice recommendations in the Cohesity Security Hardening Guide and Cohesity Security White Paper to bolster your security posture by taking full advantage of the Cohesity security controls available to you. Given the critical nature of these measures, we recommend that you undertake these steps without delay.

Preparing Against Ransomware Attacks

Heightened security threats arising out of hazardous activities by bad actors call for adherence to security best practices to prevent and recover from a potential ransomware attack. The best practices mentioned in this section apply equally to physical, virtual edition, and cloud editions.

Install the most current LTS release of all editions: physical, virtual, and cloud

Cohesity recommends keeping your cluster up-to-date with the latest LTS release and patches available at downloads.cohesity.com. Keeping your software up to date is critical in ensuring that any vulnerabilities are addressed, and latest security patches are applied to your cluster. Therefore, we always recommend that our customers stay current with the latest LTS release.

Read the release notes for all the critical information associated with upgrading to a version. You can manage software upgrades of your cluster either locally on each cluster or by centrally scheduling through the Helios SaaS portal, in case you have the Helios subscription.

Secure Cluster Access

In a ransomware attack, the primary motive of the attacker is to get access to the system, ports, applications, gateway, etc. Weak or insecurely stored passwords are the primary attack vectors. Therefore, you must secure access to the system by following these best practices:

- **Secure Password Management**

  Cohesity recommends changing all the default passwords. Starting 6.5.1b, Cohesity enforces changing the default passwords and mandates a strong password policy. Store the passwords in a secure vault protected by a different additional Two-Factor Authentication than the one used for Cohesity.

- **Apply Firewall Policy**

  To restrict the network access and manage the inbound traffic on the Cohesity cluster, use Cohesity application-based firewall rules.

- **Multifactor Authentication**

  Setting up the MFA requires users of a specific account to provide an additional verification factor along with the password credentials to log in to Helios. See Multifactor Authentication.

  Enable multi-factor authentication for both “admin” and “support” user accounts. For more information, refer to Multifactor Authentication for Local Users and Multifactor Authentication for the Support User Account. MFA for AD users (Non floating) is enabled by default from 6.8.

- **Integrate SSO**

  Configure the Cohesity cluster to use an Identity Provider (IdP) for single sign-on (SSO) access to the cluster (ADFS, Okta, Duo, Azure, Ping).

- **Enable Encryption**

  Cohesity Data Cloud leverages strong FIPS-approved AES 256 encryption algorithm for data at rest and TLS 1.2 with strong ciphers for securing data in flight; in order to protect the data from multiple attack vectors.

  NOTE: Cohesity does not support TLS v1.1 or below based encryption.

Ensure Least Privileges

Ensuring least privileges reduces the attack surface in case of a breach. The following best practices will help you make sure the users have restricted access to the system:

- **Configure RBAC to enforce least privilege**. Use role-based access control to assign access privileges to specific users/groups based on their role for UI and API access.
- **Two-person rule for password configuration**. For 6.5.1 or later, enforce the two-person rule to set passwords for Cohesity CLI access. Allow **sudo** access to the 'support' user account when absolutely needed. By default, keep it disabled.

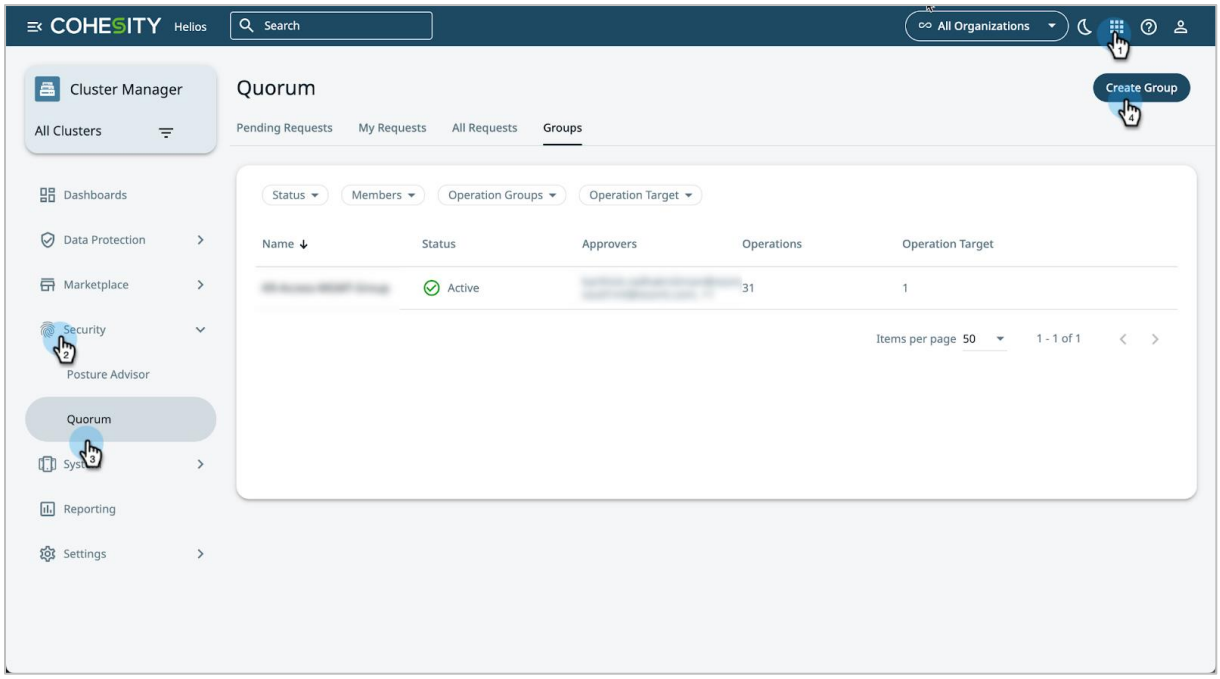
Configure Quorum Group

Data is the most valuable asset for any enterprise and like any precious asset, it is coveted, under attack and needs safeguarding. Significant amount of threat comes from insiders who have unrestricted access to data. Data Management from a Cohesity Data Cloud platform requires tight security controls and safety from enterprise data being compromised by a few reckless, malicious or external attackers.

Cohesity Data Cloud has a unique feature called **"Quorum Groups"** to ensure sensitive or privileged operations must be approved by multiple people before those operations are executed. As soon as the requested operation reaches the approval threshold defined in the quorum group (within a defined time limit), the requested operation is executed immediately.

Cohesity recommends configuring sensitive data operations to require approval by a quorum group, which helps prevent the misuse of executing the privileges operations on the Cohesity Data Cloud without authorization.

Refer to product documentation to learn more about supported operations and best practices to use quorum in Helios.



Secure Critical Backups

When you secure the system, you also secure the data on it. However, as an additional layer of protection, you can enable DataLock on the protection groups for your critical data.

DataLock is the WORM (write once read many) feature that locks and retains data for regulatory compliance purposes. It prevents attackers from tampering or deleting your protected data, including local backups, archives, and replication. Once applied, a DataLocked protection job will be deleted only after its retention period expires. In the event of compromised Cohesity cluster credentials, having the DataLock feature enabled can prevent a bad actor from modifying and/or deleting backups before the expiration date.

DataLock prevents all users, including those who have the Data Security role in Cohesity, from modifying or deleting any DataLock-enabled protection run. Only users with the authorized Cohesity Data Security role can add, modify, or remove DataLock from a Protection Policy.

Enable Data Lock on policies associated with critical data for safe retention. Turning on Data Lock/WORM on at least one policy ensures protection against destructive commands.

Important: Using DataLock with longer retention periods and for auto-protected sources can result in significant cluster space usage. See Cohesity's protection policy documentation to understand DataLock functionality and analyze your disk space requirements and capacity.

Use Helios for Ransomware Anomaly Detection

Once considered a defense against ransomware, backups have now become a prime target for sophisticated ransomware attacks. Helios uses machine learning algorithms to continuously monitor changes in the backup data ingestion rate and data entropy for your organization. If any of these is out of the normal range—based on daily and historical data—Helios flags it as a potential ransomware attack and alerts both your IT administrators and the Cohesity Support team. Administrators can then perform rapid restores from the last healthy snapshot and recover VMs, files, and application objects.

- **Register Cohesity Cluster to Helios**. In order to take advantage of Cohesity's ability to detect anomalies resulting from possible ransomware attacks, register your Cohesity cluster with Helios. See How to register your Cohesity cluster with Helios for more information**.**
- **Install Helios Mobile App**. Install the Helios mobile application to administer and get notified of alerts on the go.
- **Enable Email Notification**. Be sure to enable email notifications in the event of a possible ransomware attack. See How to enable email notifications through Helios for more information.

DataHawk

Today's companies and organizations are overwhelmed with the exponential growth in the data they collect, manage, and store. To ensure the quality and security of such data, organizations need robust data security and management solutions that help them understand the breadth and depth of data and enforce protection and security policies across the data footprint.

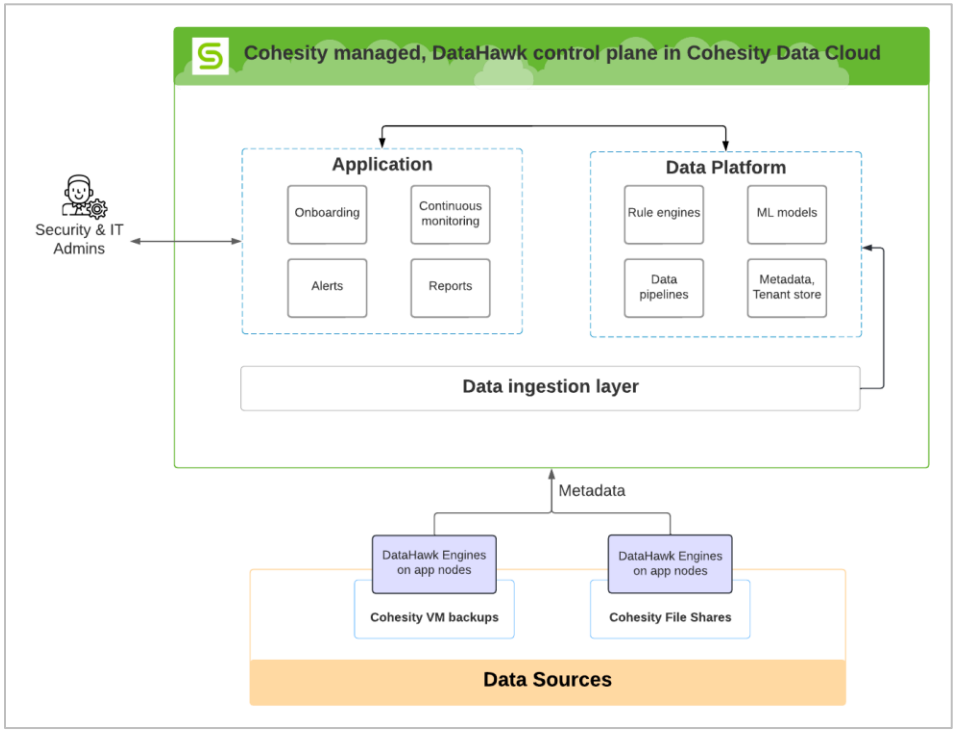
Cohesity DataHawk offered as a service on the Cohesity Data Cloud platform, lends the capabilities that organizations require to secure data across on-prem data sources, DataHawk provides actionable insights that improve your cyber resiliency.For security analysts and IT admins, DataHawk supports the following use cases:

- Assess the impact of ransomware prior to recovery by identifying sensitive data in compromised objects.
- Scan for threats using ransomware Indicators of Compromise (IOCs).
- Analyze the user behavior by auditing the user activities on Cohesity Fileshares

The following diagram illustrates the detailed architecture of DataHawk.

For more information, refer Cohesity Product documentation.

Figure 2: DataHawk



Set Up Backup for Active Directory

One of the focus areas for ransomware attacks is the identity access management systems of the environments they attack. Compromised identity access management systems make it extremely difficult for authorized users to secure and access mission-critical systems. For more information, refer to Active Directory protection requirements.

Keep the Support Channel Disabled

As a best practice, you must have tighter control over the service doors. Keep the support channel disabled at all times unless there is a need to troubleshoot.

Responding to a Ransomware Attack

In the event of a ransomware attack, you must respond quickly to contain and limit the potential damage inflicted to your organization's digital assets. The following section contains recommendations that will assist you with the stabilization of your environment.

Change Passwords

One of the first casualties in any ransomware attack is the passwords, which are invariably compromised. In order to protect the copies of data in your Cohesity cluster and limit the level of exposure to the ransomware attack, you must immediately reset the passwords of the Cohesity instances in your environment.

Create a Support Case

After a Ransomware attack, you may need to perform several restrictive as well as recovery tasks. Contact Cohesity Support for expert advice and step-by-step instructions on how to carry out these tasks. Create a P1 support case with Cohesity Support either through the Cohesity Support Portal or by email. Alternatively, you can call **1-855-784-2293**.

Notify Cohesity Account Team

Make sure to notify your Cohesity account team so that they can mobilize additional internal resources as needed. Also, alert the Technical Account Manager immediately if your organization has been assigned one.

Enable Legal Hold on Protection Runs for Critical Workloads

Once an organization confirms a ransomware attack, Cohesity recommends that their data security user enables Legal Hold for all business-critical workloads to prevent malicious deletion of backups. Often, ransomware attacks go beyond just jeopardizing the primary copy of data and target the backup copies to prevent the victims from accessing their data. Putting your critical data on Legal Hold ensures that snapshots of protection groups put on Legal Hold will not be deleted until the Legal Hold is removed or disabled. To enable Legal Hold, follow the instructions in Enable legal hold through the user interface. You can also enable Legal Hold programmatically on multiple protection runs using APIs.

Pause Future Protection for DataLock-Enabled Environments

Ransomware may encrypt the data that backup clients manage. In order to prevent the rapid consumption of the storage capacity with encrypted data in your environment, Cohesity recommends that all protection groups be paused, especially those with DataLock enabled.

Identify Hosts in Environment Impacted by Ransomware

A critical requirement to limit the proliferation of ransomware is your ability to identify and isolate the hosts that have come under attack. Using machine learning and artificial intelligence, Cohesity enables you to identify compromised hosts protected with Cohesity in the environment. For more, see Counter Ransomware Attacks in the online Help.

NOTE: Organizations must do their due diligence and evaluate whether other areas of the environment are impacted by a ransomware attack.

Identify Known Good Recovery Points

Once you have identified workloads in the environment that have been compromised, the next step is to identify recovery points that you can leverage in order to reverse the effects of the ransomware attack. For details, see How to identify the latest clean snapshot and perform recovery.

Recover Active Directory Objects to Rollback Compromised Access Management

It is common for ransomware attacks to target Active Directory Domain Controllers during a breach. When this occurs, many organizations have challenges around recovering access to distributed applications that are dependent on identity access management systems such as Active Directory. Given the vast number of objects in an Active Directory environment, you'll find it extremely difficult to identify the specific Active Directory objects that may have been compromised.

With Cohesity, you can compare a live Active Directory environment with Active Directory protection jobs that reside on a Cohesity cluster to easily compare and determine the attributes, which have been changed since the last protection run. For more information on active directory recovery, see How to recover Active Directory Objects.

Instant Mass Restore Your Mission-Critical Workloads

Cohesity's Instant Mass Restore (IMR) feature provides an efficient way to recover some of the workloads, thereby dramatically reducing the Recovery Time Objective (RTO) for bulk restores.

- IMR VMware VMs—With IMR, you can use the Cohesity NFS views as the datastore, for a faster recovery process that circumvents the need to copy the VMs to the original datastore before booting. For more details, see How to perform Instant Mass Restore of VMware virtual machines.
- IMR NAS Backup—With IMR, you can clone a volume's backed-up data to a new view within the Cohesity cluster. Manually access or mount the View via SMB or NFS to the system of your choice and then perform the desired operation with the recovered data. For more details, see How to perform Instant Mass Restore for file workloads leveraging NAS adapters.

Appendix A: Cohesity Security Hardening Checklist

The following checklist will help you secure your Cohesity deployment against a potential attack.

Table 1: Cohesity Security Hardening Checklist

NO.	ACTIONS	IN PLACE
1	Upgrade Cohesity to the latest LTS with latest patches	☐
2	Change default passwords (admin, support and IPMI). Set a unique password for each cluster.	☐
3	Disable “sudo” access for the ‘support’ user account.	☐
4	Enable Multifactor Authentication (MFA).	☐
5	Configure Quorum Group	☐
6	Store password in strong vault.	☐
7	Configure Role-based Access Controls (RBAC).	☐
8	Enable DataLock on protection policies applied to critical data or at least on one policy (dummy view).	☐
9	Configure centralized logs and auditing.	☐
10	Setup active directory protection group	☐
11	Keep the support channel disabled.	☐
12	Integration with Threat Management SIEM/SOAR tools	☐

Appendix B: Ransomware Attack Response Checklist

Follow the checklist in table 2 when you respond to a ransomware attack.

Table 2: Ransomware Attack Response Checklist

NO.	ACTIONS	IN PLACE
1	Change passwords.	☐
2	Create a support case.	☐
3	Notify the Cohesity account team.	☐
4	Enable Legal Hold on critical workloads protection jobs.	☐
5	Pause future protection for DataLock-enabled environments.	☐
6	Identify hosts in an environment impacted by Ransomware using Helios.	☐
7	Identify known good recovery points and perform recovery.	☐
8	Recover Active Directory protection group.	☐
9	Instant mass restore of critical workload.	☐

Appendix C: Leverage the Runbook App for Automated Recovery of Workloads

Cohesity Runbook automates and orchestrates migration and recovery of workloads that are protected by Cohesity Data Cloud to a target location. It provides hybrid-cloud mobility and disaster recovery for a single application or an entire environment, making the process easier, reliable, and repeatable. For more details, see:

- How to install and use the Runbook App from Cohesity Marketplace Apps
- API documentation that you can use with the Runbook App to automate tasks.

Appendix D: Backup vCenter Appliance to NFS on Cohesity

The Management-Tools Backup for VMware App automates backups of VMware management software components using file transfer services. The app provides the following features:

- Automated discovery using native APIs of your VCF environment (workload and management domains)
- Automatic configuration of File-Based Backups of NSX T Manager, SDDC Manager, and vCenter, including schedules, retention, and on-demand backups where supported.
- Provides Secure FTP (sFTP) service and persistent storage to hold encrypted backed-up datasets.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Sagar Sethi is a Staff Technical Solution Engineer at Cohesity. In his role, he focuses on various aspects of Cybersecurity to secure the Cohesity product design & solutions to solve the customer's current challenges for data protection & Zero Trust from advanced threats & organizational risks.

A.J. Aquino and Joseph Thomas are Senior System Engineering Managers at Cohesity. In their roles, they focus on architecting, designing, and delivering secure data management solutions for use cases such as data protection, file and object services, test/dev, analytics, cloud, and ransomware detection.

Other essential contributors include:

- Subash Babu, Staff Technology Editor, Technical Solution Engineering

Document Version History

VERSION	DATE	DOCUMENT HISTORY
3.2	July 2024	Republishing
3.1	July 2023	Added Quorum
3.0	May 2023	DataHawk updates
2.0	July 2022	Feature updates
1.0	June 2021	First release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

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