COHESITY

Version 7.2

June 2024

Cohesity Data Cloud Security White Paper

Secure By Design

ABSTRACT

In today's cyber-enabled world, establishing efficient and secure access to IT platforms is critical. This document elaborates on the key security principles that Cohesity follows to enhance confidentiality, data integrity, and controlled access to your data in the Cohesity Data Cloud.

Table of Contents

Figures

Tables

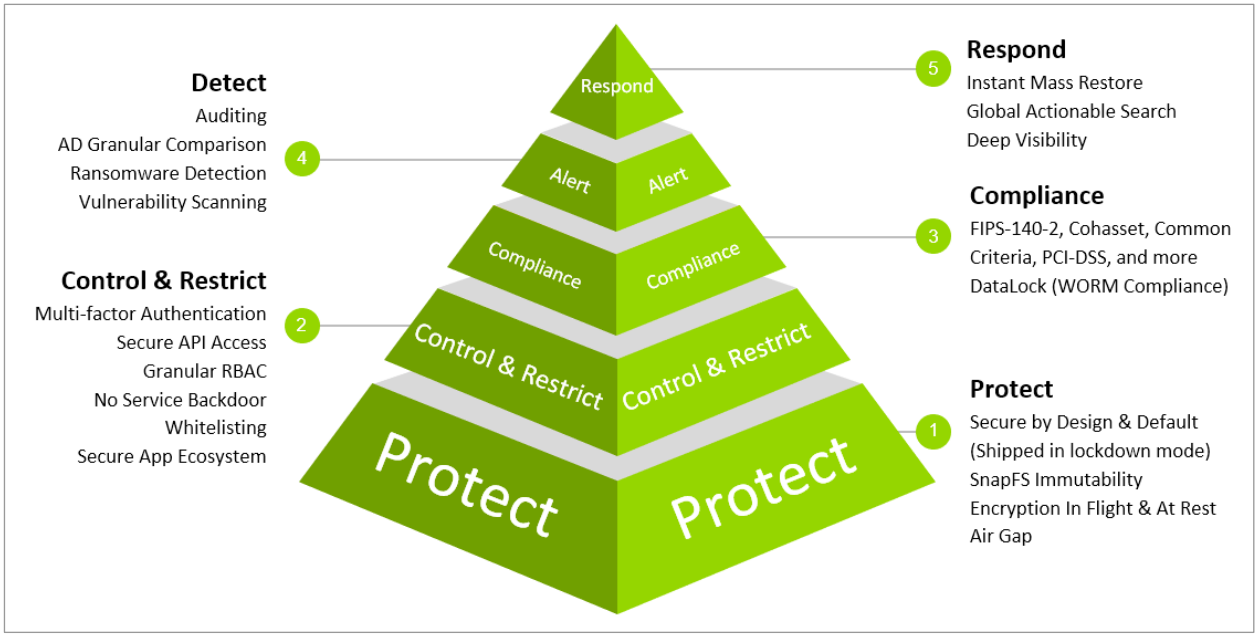
Cohesity Protects Your Data from Threats

Because your data is essential to your business and organization, establishing efficient, reliable, and secure access to your data is of paramount importance. Your data management platform should have defenses in place to guard against attacks on your data and platform. A vast majority of today's security threats can be classified as:

- Ransomware and other malware attacks.
- Breaches due to unauthorized access and insider threat.
- Accidental data leak and misconfigurations.

The aim of these attacks can be summarized as DUCT: Deletion, Unavailability, Corruption, and Theft of your data. Securing the primary and backup data is critical. After all, as the last line of defense, backup is an essential part of the security landscape. Cohesity has strong, built-in defense mechanisms that guard against attacks and breaches that can lead to data loss.

Figure 1: Cohesity Protects Against Data Deletion, Unavailability, Corruption, and Theft



Legacy technologies have created a mindset wherein product features and product security are considered inversely proportional to each other. A common misconception is that the more sophisticated and feature-rich a platform is, the less secure it is.

With Cohesity, however, you don't have to choose between the two. Thanks to Cohesity's security-first design Threat defense Architecture, platform intelligence & AI/ML capabilities are no longer inversely proportional to security.

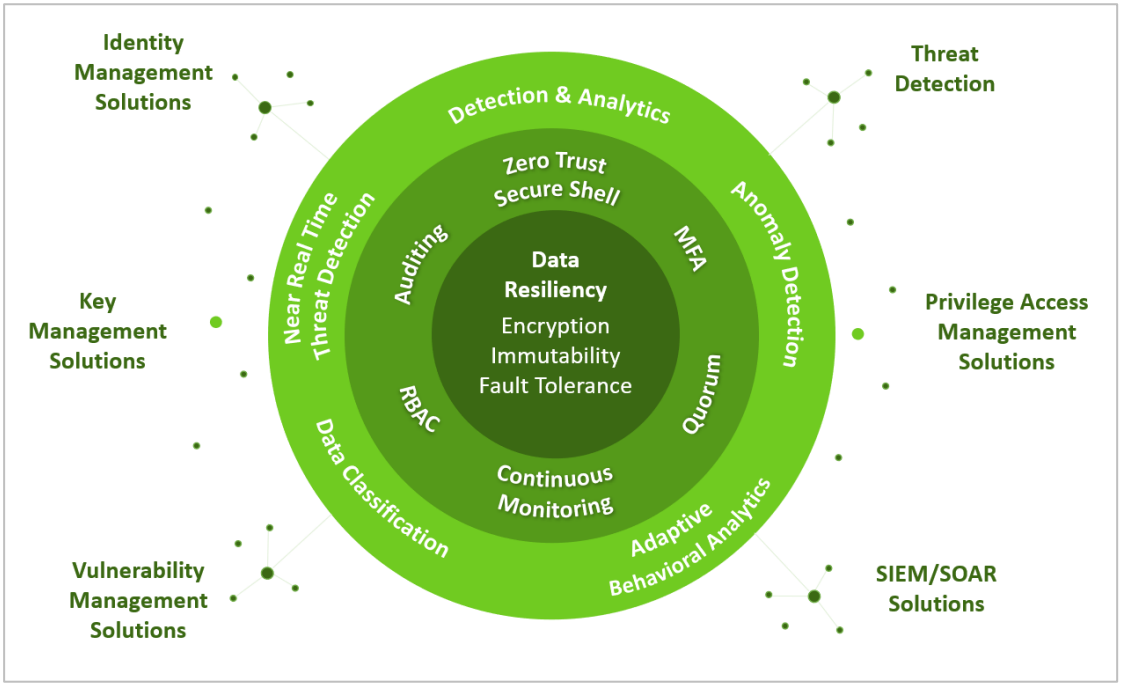
Secure By Design

Inspired by web-scale principles, Cohesity's security-first architecture, combined with secure software development and release practices, ensures enterprise-class security.

Cohesity Threat Defense Architecture

Protecting, detecting, and recovering from ransomware, data breaches or insider threats requires several key capabilities and functions. Cohesity's Threat Defense architecture is designed to help you combat threats against your data in the cluster by enabling you to achieve outcomes related to data protection, compliance, operational & Data resiliency, and defense against sophisticated attacks.

Figure 2: Threat Defense Architecture



Its safeguards include strong access controls to protect settings from unauthorized access or changes and to secure and ensure the confidentiality of the data, continuous monitoring with detection, and analytics to identify attacks and unusual activity.

Supporting these capabilities are integrations with leading security applications to automate incident response as well as to leverage existing enterprise security services such as key management, identity and access management, multifactor authentication, and threat and vulnerability scanning. These capabilities work in concert to provide a hardened data management platform that will prevent the ability of an attack to tamper with or destroy data and to help organizations better detect attacks against the data in progress.

The following provides a detailed review of the capabilities and functions that power the Cohesity Threat Defense Architecture. Each major component of the architecture is reviewed by category, which consists of:

- Data Resiliency: Encryption, Immutability, and Fault Tolerance
- Zero Trust: Multifactor authentication, Granular Role-based Access Controls, Quorum, Auditing, and Continuous monitoring
- Detection & Analytics: Near Real Time Threat Detection, Anomaly Detection with AI/ML capabilities, Data Classification, and Adaptive Behavioral Analytics
- Security Integrations: Identity Management, Threat Detection, Vulnerability Management, Key Management, Privilege Access Management, SIEM/SOAR solutions, and CyberArk PAM solution

Secure Data Placement

First and foremost, it is crucial to ensure that the data in the system is safe and consistent. Cohesity SpanFS™, our third-generation distributed file system, is built on several principles that ensure secure data placement, including:

- **No-overwrite Design**
  - SpanFS keeps the data secure by never overwriting data in place. It always writes data to an empty space. This helps to ensure that new changes never affect or overwrite existing content on the file system.
  - To ensure efficient recycling of deleted data throughout the system, the Data Cloud applies a garbage collection process to expired and deleted snapshots to reclaim space.
- **Immutable Backup**
  - The data backed up by Cohesity is stored on internal Cohesity Views that are inaccessible from outside the Cohesity cluster.
  - All backups are stored in a read-only state. Any incremental backups are written on clones, which are also marked read-only upon completion of each Protection Run. Once a backup copy is stored, the data in it cannot be modified.
  - Writes to internal Views during backup are only allowed via trusted internal services and authenticated APIs.
  - Cohesity Views include DataLock, Cohesity's Write Once Read Many (WORM) feature. If DataLock is enabled, the data cannot be deleted by anyone, including administrators, until the DataLock expires.
- **Integrity Checks**
  - Cohesity calculates the checksum of data before it is written to the disk.
  - The data is verified before serving each read.
  - Cohesity also has a scrubber process that periodically scans the data and verifies the checksum to validate it. This allows the system to catch any bit-rot. When Cohesity detects bit-rot, it fixes it using the redundant copy on the cluster.

Inter-node Communication

Node-to-node communication within a Cohesity cluster takes over an internal network that connects the nodes. This communication consists of two main workflows:

- **Introducing a new node to the cluster**—Node addition is configured and triggered by the cluster administrator. In the process, Cohesity automatically verifies that the node being added has:
  - Valid certificates.
  - Cohesity software installed on it.
- **Node-to-node communication between existing nodes**— Cohesity uses certificate-based authentication for communications between services within a Cohesity cluster. Each 7.1.1 cluster with Node-to-Node encryption enabled employs X509 certificates to both authenticate cross-service communication and encrypt user data exchanged between cluster nodes with TLS 1.3 & AES-256-GCM (Galois/Counter Mode).

  NOTE: From Cluster version 7.1.1 onwards, node-to-node encryption is enabled by default. However, if you are upgrading your existing earlier version to 7.1.1, you need to manually enable node-to-node encryption.

For more information, see Cohesity product documentation.

FortKnox: Cyber Vaulting as a Service

Data powering business operations is more valuable than ever. It is also more vulnerable than ever to cybersecurity threats, power outages, and natural disasters. To stay competitive while protecting their data, organizations are embracing a modern 3-2-1 strategy that includes a virtual air gap with physical and network isolation, which provides both security and high availability.

A SaaS-based cyber vaulting and recovery solution, FortKnox improves cyber resiliency with an immutable copy of data in a Cohesity-managed cloud vault via a virtual air gap. Organizations relying on FortKnox gain an additional layer of security against ransomware and other cybersecurity threats through physical, network, and operational isolation.

Cohesity FortKnox powers a modern 3-2-1 strategy for the cloud era that effectively balances organizations' security and agility priorities. For more details on how Cohesity keep its SaaS services secure, see Cohesity Cloud Services Security Brief guide.

Key Benefits:

- A SaaS-based, single-pane-of-glass model
- Simplifies operations and lowers costs.
- Eliminates the complexity and resource requirements of internally managed isolation solutions.
- Rapid recovery saves time and improves business continuity.
- Additional protection layer safeguards data and reputations such as MFA, granular role-based access control (RBAC), quorum for critical actions, and short-lived token-based authentication to access vault.

For more details on how Cohesity keep its SaaS services secure, see Cohesity Cloud Services Security Brief guide.

Use Cohesity Air-Gap Data Protection for Redundancy and Additional Protection

In some scenarios, your organization is required to make sure that at least one copy of your critical data is stored on a secure network that is isolated from other networks—a strategy known as 'air-gap data protection.' Cohesity provides two methods for implementing air-gap data protection, each with its own benefits and tradeoffs. The choice between the two depends on factors such as organizational policies, compliance requirements, TCO, existing infrastructure, future plans, etc.

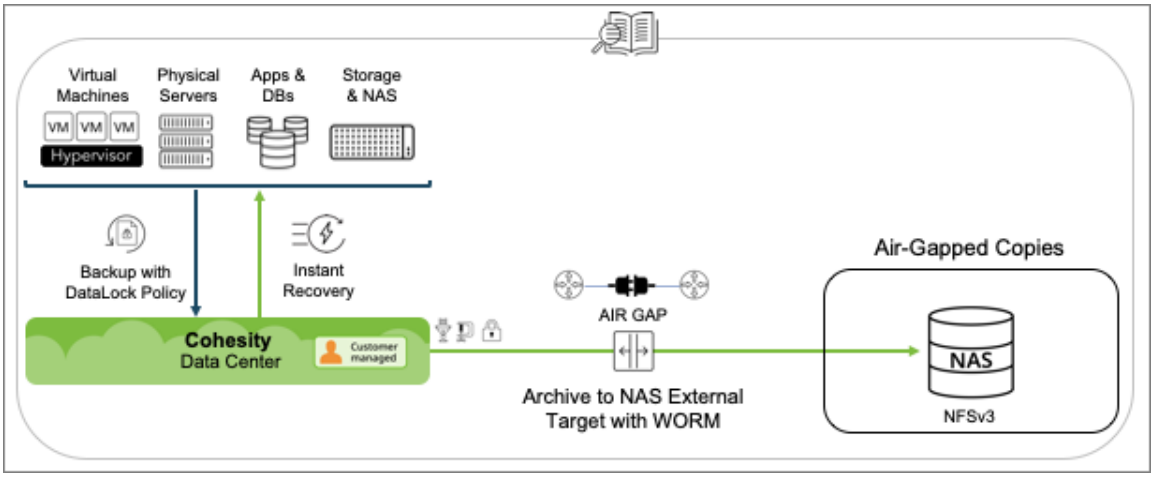
Understand and decide which method best suits your organization's needs:

- **Modern Air Gapping (Virtual)**. In addition to traditional air gapping (below), Cohesity also supports a more modern approach that enables air-gap data protection with lower Recovery Time Objectives (RTOs) and Recovery Point Objectives (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 on the target to keep the remote copy immutable.

  For example, if you wish to archive your data to AWS, you can enable VaultLock on Glacier in combination with DataLock on Cohesity. This prevents local and archived snapshots in Cohesity, as well as those in the cloud, from being deleted.

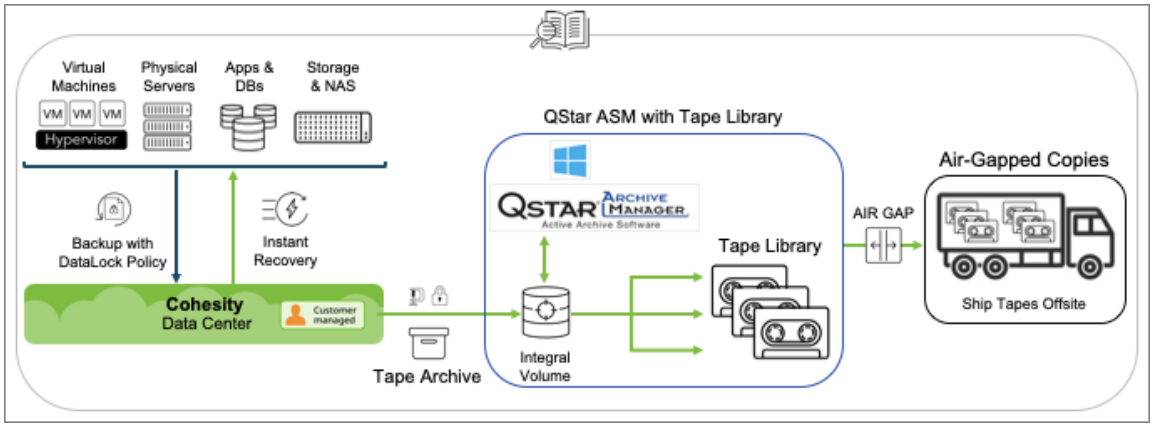
  Cohesity DataLock, Cohesity's implementation of WORM, ensures compliance; once it is set, it cannot be disabled, even by the administrator.

Figure 3: Archive to NAS External Target with WORM—Modern Air-gap Data Protection



- **Traditional Air Gapping (Physical)**. Tape out the data from your backup and, after every archive, send the tapes 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. Note, however, that the challenge with tape is that it leads to higher RTOs and missed RPOs.

Figure 4: Archive to Tape—Traditional Air-gap Data Protection



Secure Software Development and Release Practices

Cohesity reviews security at each phase of the software development life cycle. The goal of the Cohesity's secure product development life cycle is to deliver secure products to customers and contain security vulnerabilities throughout the life cycle of the product. To deliver on this goal, Cohesity practices:

- Security Training
- Security in Design
- Threat Model
- Vulnerability Management
  - Vulnerability Management Policy
  - Penetration Testing
  - Static Code and Binary Analysis
  - Dynamic Scanning
  - Third-party Component Security
  - Product infrastructure and Tool Support
- Secure Product Release

  Cohesity performs extensive feature testing, system testing, and release readiness testing against our releases, ensuring both the Cohesity application and the underlying OS are validated:
  - Feature Testing
    - Extensive unit and functional test coverage through automation
    - Functional regression through automation
    - Backwards Compatibility testing
    - Documentation development
  - System Testing
    - Customer centric scale
    - E2E workflow and integration tests
    - Performance, Scalability and Reliability tests
  - Release Readiness
    - Patch testing
    - Internal ToI
    - Security Vulnerability Testing
    - Ecosystem Testing
- Product Incident Response

  Vulnerability scanners run periodically to assess the state of the operating system, networking layer, and services running on the Cohesity cluster. Based on the scan results, unused ports and services are closed and kernel or system libraries are updated for known vulnerabilities. We run these scans weekly on our test beds and address the vulnerabilities within SLA.

  In addition to using third-party software to conduct security assessments, Cohesity has a dedicated in-house Security Team to assess and improve security in the product for each release. Some system

integrators are used to build integration plugins, but that code is also quality assurance tested and certified by our Engineering and QA teams. Also, third-party penetration tests are performed periodically.

- Vendor OS hardening details for CentOS
  - Cohesity Appliances (Physical and Virtual Editions, SaaS Connector) are shipped in a lockdown mode by default. Access to shell via SSH is disabled by default, and no direct access is provided to the underlying filesystem or data that resides upon it.
  - We regularly perform SCA (Software Composition Analysis via Twistlock & Snaky), vulnerability scans (Tenable) and SAST (Static analysis) & DAST (Dynamic Application Securitytesting) against our releases, followed by an annual penetration test performed by an external third-party. CIS Benchmarks are applied to Appliance images. Unused open ports and services are closed by default. Kernel and system libraries are updated regularly for known vulnerabilities through Cohesity updates (patch, unified release, or full release updates).
  - For vulnerability management, guidance is taken from ISO 27001:2013 Control A.12.6.1 and NIST's Cybersecurity framework Version 1.1 (Controls RA-1, RA-5, IP-12, CM-8, MI-3).
  - Hashes of software images are provided to customers with both SHA256/MD5 via downloads.cohesity.com
  - Support Access to SaaS Connectors is disabled by default, and we recommend it is only to be enabled when required during the course of a support case. Support Access cannot be enabled indefinitely and will automatically disable itself by a designated date as selected by the Customer.
  - The SaaS connector secures data in transit through secure, modern encryption protocols TLS 1.3 and mTLS with only FIPS approved cipher suites.

For more information, refer to Cohesity product documentation.

Secure Cluster Administration

Cohesity's cluster administration access is governed by multiple security layers. Cohesity enables you to apply the principle of least privilege by assigning fine-grained access, even to a single object on the Cohesity cluster.

Some of the features that ensure secure cluster administration include:

- Secure Base Operating System
- Authentication-server-based Single Sign-on (SSO)
- Certificate-based Authentication
- Granular Role-based Access Control (RBAC)
- User Audit Trail
- Secure Multi-tenant Design

Secure Base Operating System

Cohesity SpanOS is Security-Enhanced Linux (SELinux)-enabled with strict enforcement added. The following list of enforcements make the base OS secure:

- Cohesity grub is password protected and single user mode is disabled.
- Cohesity SpanOS has implemented many STIG controls as detailed in APSC-DV, RHEL, and SRG-APP.
- The cluster and Linux user account credentials are only stored as cryptographic representations, not in plaintext. These credentials have been protected with AES-256 encryption and/or salted hashing (SHA-512).
- Cohesity SpanOS uses Federal Information Processing Standards (FIPS)-approved cryptography algorithms for all handshake authentication and encryption.
- Cohesity SpanOS implements a default firewall rule that blocks non-essential protocols and ports.
- Cohesity SpanOS implements a secure shell with restricted command options to execute (iris_cli only) when logged in through SSH.

Authentication-server-based Single Sign-on

Single Sign-on is not only required to avoid password fatigue and simplicity but is also a crucial component of centralized credential and access control. Cohesity integrates with all major SSO services that support SAML & OpenID Connect protocol standards, including:

- Active Directory
- LDAP
- Azure Active Directory
- Okta

- Ping
- Duo
- Shibboleth

In Cohesity, you can enable multifactor authentication (MFA) workflows using the Single Sign-on workflows.

Certificate-based Authentication

If Cohesity is joined to an Active Directory domain, you can enable certificate-based authentication for Cohesity, requiring users to sign in using a digital certificate.

This acts as an additional layer of security, as users are required to be validated via certificate in addition to providing their login credentials.

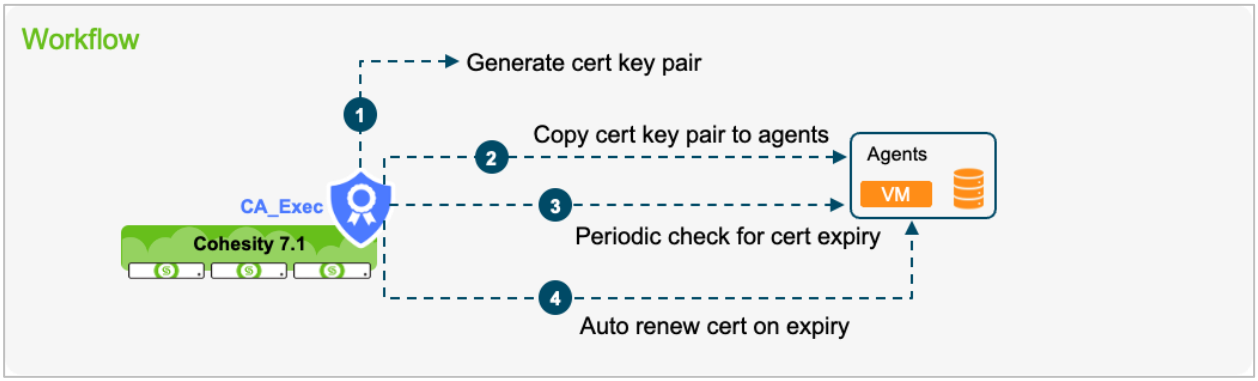
For more information, refer to Cohesity product documentation.

PKI Management

To eliminate risk of widespread certificate expiry issues, Cohesity has built PKI infrastructure for issuing agent certificates for cluster communication.

From cluster version 7.1 onwards, the Cohesity CA (ca_exec) service issues a unique CA cert/key for each cluster agent to cluster communication and replication communication.

With the Support of Intrinsic Automation—existing agents are automatically provisioned new certs from Cohesity CA.



For more information, refer to Cohesity product documentation.

Granular Role-based Access Control

Granular Role-based Access Control enables an organization to grant the least privileges to a user required to do their job, minimizing risk, and keeping areas outside their domain out of reach.

Granular RBAC consists of:

- **User roles—Standard and Custom**. Cohesity has two types of user roles that you can assign to specific users to control user access to the Cohesity cluster:
  - **Standard Roles**. Cohesity has six default system roles that act as templates based on different user privileges: Admin, Viewer, Operator, SMB security, Self-service Data Protection, and Data Security.
  - **Custom Roles**. Cohesity administrators can create custom roles by picking up individual privileges. Users who are assigned these roles will have only those privileges.
- **Ability to restrict user role to granular functionality**. You can restrict Cohesity user roles to specific workflows, thereby limiting what a user with a certain role can do on the cluster. For example, you can restrict specific users to assign the privileges for performing backups or just for monitoring activities.
- **Restrict user access to a specific object**. Based on individual adapter behavior, you can restrict users to have access only to specific objects. No other objects are visible to the user other than the objects that are assigned to it.

Multifactor Authentication

Multifactor authentication is an additional layer of security used to verify the identity of a user. With Cohesity, you can use native MFA or configure MFA with external MFA providers such as Ping, Duo, Okta, and more.

Native Multifactor Authentication

Data Cloud supports Multifactor authentication for local users. Administrators can enable MFA for all or specific local users. Administrators can select one or both of the following authentication methods:

- **Authenticator App**—Users must install a TOTP authenticator app such as Okta Verify on their device and enter the verification code generated by the app.
- **Email**—Users must enter the verification code sent to their email address.

After MFA is enabled, users can access the Cohesity GUI or Cohesity CLI by providing their local user password and the verification code generated by the authenticator app or received in their email. For more information, see multifactor authentication help.

Integration with External Multifactor Authentication Providers

Data Cloud supports authentication server-based single sign-on (SSO) with SAML v2 support & OpenID Connect. The idP/SSO providers support MFA for the users. Using this feature you can implement the MFA with external MFA systems, such as Supported vendors—Okta, Duo, Ping, and Microsoft Entra ID via SAML 2.0.

Cluster Session Management

Often admins leave the cluster session open which can lead to unauthorized cluster access and misuse. An attacker can gain access to the environment without requiring credentials which is a major security risk.

Cohesity supports multiple session timeout settings which enables you to define the session timeout of Cohesity interfaces like GUI, CLI, and SSH.

In the Account Session policy, you can define:

- **Maximum Absolute Timeout for UI and CLI**: The maximum time limit after which the user account will be logged out from Cohesity UI and Cohesity CLI, irrespective of the status of the session. The default value is set to 1440 minutes, i.e., 24 hours. Minimum value can be 1 hour, and the maximum can be up to 24 hours.
- **Inactivity Timeout for Cluster UI**: User account will be logged out from Cohesity dashboard if the session remains inactive for configure time limit. The default value is set to 30 minutes. The minimum value can be 1 minute, and the maximum value can be 12 hours.
- **Inactivity Timeout for SSH**: User cluster SSH session will be logged out if the session remains inactive for configure time limit. The default value is set to 5 minutes. The minimum value can be 1 minute, and the maximum value can be 24 hours.

You can configure the session timeout settings as per your organizational policy. For more information, see Configure Account Security Settings.

User Audit Trail

Cohesity maintains a user audit trail for all actions performed on the Cohesity cluster. These records provide proof of compliance and operational integrity. Audit trails can also identify areas of non-compliance by providing information for audit investigations. For more details, see Audit Logs.

No Service Back Doors

Unlike some legacy backup vendors, Cohesity doesn't have a concept of a default user used by the product support team. All access to Cohesity clusters is controlled and administered by the customer. At no point does Cohesity have access to a customer's data or cluster without the customer's expressed authorization.

Cohesity nodes are shipped in a lockdown mode by default. Access to the shell via ssh is disabled by default and can be controlled in accordance with your organizational security policies. Even the Cohesity Support team cannot access a cluster for troubleshooting until the cluster administrator disables lockdown mode. When the

cluster administrator does allow a Cohesity support engineer to access the cluster, the “support” user account has read-only privileges by default. Only the cluster administrator user can escalate the privileges.

> **NOTE**: Even when granted access by a cluster administrator, Cohesity Support only has temporary access to the customer’s cluster. Access will expire automatically or can be canceled at any time before expiration by the cluster administrator.

For more information, see the Security Hardening Guide.

By default, the Cohesity browser UI is the only way to interact with a Cohesity cluster. The admin user is required to change the default password at the first login to the cluster. The administrator can change the privilege credentials in the system.

Secure Multi-tenant Design

In today’s data-management sector, secure multi-tenancy is a crucial part of planning corporate IT infrastructure. With Cohesity, enterprises and service providers can create an *Organization* corresponding to each department or tenant on a Cohesity cluster.

In a Cohesity cluster that is configured for multiple tenant organizations, each tenant is implemented as an *Organization*. The Organization ID acts as the multi-tenancy identifier for each tenant. To tie all the resources assigned to the organization, organizations act as namespaces. Some resources—such as an Organization’s Administrator and Users, Views, VLANs, and Sources—are isolated per tenant, while other resources—such as Storage Domains and Protection Policies—can be dedicated or shared, depending on the specific tenant and service provider requirements of the deployment. The option to isolate a Storage Domain to a specific tenant is unique to Cohesity when compared to other aspiring multi-tenant systems.

With Cohesity multi-tenancy, you can securely share the same cluster across multiple tenants, including the use of tenant-isolated deduplication domains when required.

Split Key for IPMI Console Access

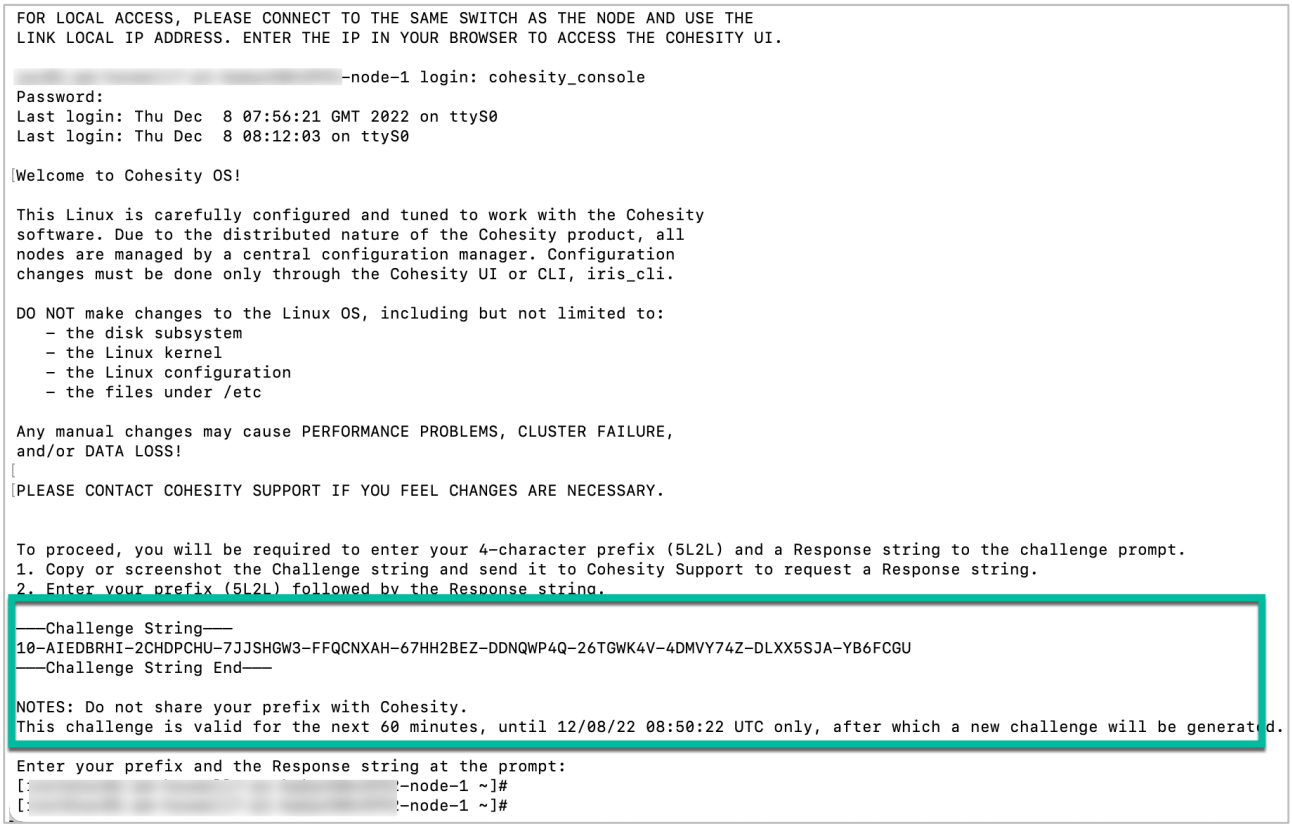
Introduced in Version 7.0, the Split Key for IPMI Console Access feature delivers an additional safeguard against malicious access to the Host OS by mandating a challenge-response system when a user attempts to access the console via IPMI, in addition to the existing username-password combination.

Split key can be enabled from iris_cli —

iris_cli cluster split-key-host-access enable=true

> **NOTE**: On upgrade from 6.8 or below to 7.2, Split key for IPMI console access can be enabled from **cluster UI under Access Management > SecureLogin > Split Key.**

The response code can only be generated by opening a support case with Cohesity SREs, who will be available 24x7 to service the response key within pre-defined SLAs. Refer for more details to generate the Challenge-response code to access the host OS on a node via IPMI.



Secure Shell

In order to access the cluster securely and comply the principle of least privileges, Cohesity offers the Secure Shell feature that restricts SSH access to the host operating system shell. This further tightens access to the Cohesity cluster while still providing users with the ability to execute CLI commands, run diagnostic tools, and access logs.

This secured shell can do the following:

- run `iris_cli` commands (provides options to run specific host-shell commands which are allowlisted). For more details, see Running Linux Commands using Cohesity CLI.
- view the logs (read only).

NOTE: If you need access to the host shell using SSH, contact Cohesity Support.

Secure Shell Prompt `

To identify whether you are running the secure shell, once you log into the shell using the support user account, the shell prompt displays the term "**restricted**," which suggests that you have logged into the Secure Shell of a Cohesity node.

For example:

```
~ % ssh support@10.x.x.x
support@10.x.x.x's password:

**********  Welcome to Cohesity **********

WARNING: Unauthorized access to this system is forbidden.
By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.

**************************************************
[support@restricted-node-1 ~]\>
```

See product documentation to Enable Host Shell access.

Quorum

In order to prevent unilateral administrative changes without a multi-approval level, Data Cloud has designed with a unique feature called “Quorum “to comply with the principle of Dual control.

Quorum approvals are an authorization model within Data Cloud that ensures that sensitive or privileged operations requested by a Helios user must be approved by a quorum of approvers before those operations are executed.

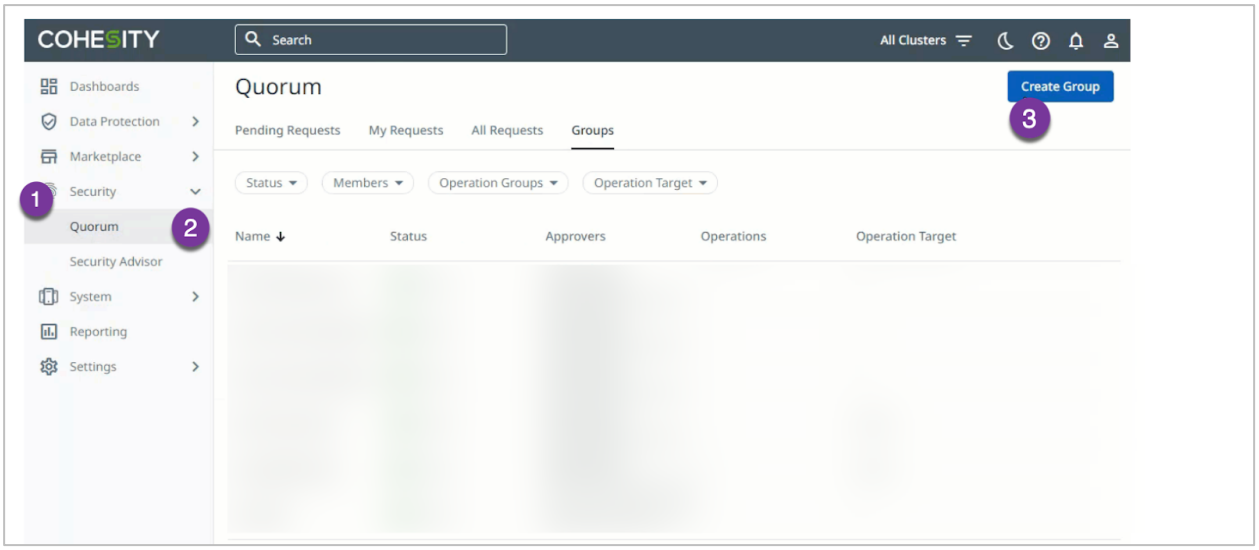
Quorum approvals help you eliminate the risks associated with unilateral admin tasks from highly-privileged administrator—specifically to prevent a rogue, poorly trained, or compromised administrator from performing sensitive or privileged operations on the Data Cloud without authorization or oversight.

From 6.8 release, any cluster-related operations that are quorum-protected in Helios cannot be initiated from the Data Cloud UI or CLI. Instead, customers need to initiate these operations from Helios, which goes through a Quorum approval process with at least two or more users to the quorum group and reviewed before execution.

In Helios, you can define a group of users called a quorum group who can decide to approve whether defined operations initiated by a Helios user are allowed to be executed or not.

Before you create a quorum group, ensure that you review the considerations and best practices for using quorum in Helios.

See How to create Quorum group and supported operations.



In Helios, when a user initiates a quorum-protected operation, an email notification is sent to all the approvers in the respective quorum group. The operation requires approvals from the quorum approvers to execute.

Quorum approvers can approve or decline the quorum requests from the pending request tab in the Quorum Dashboard. Once the quorum request is approved per the conditions defined in the quorum group configuration, the operations are executed immediately.

Continuous Security Monitoring

All logs (such as system processes, audit and security events (Authentication Events) generated on Data Cloud are stored in a centralized location as per retention period and can be integrated to External SIEM tools.

Cohesity has built-in integrations by which you can export the logs through RestAPI or by configuring syslog server. You can centrally manage these for advanced correlation and detection purposes.

Supported vendors —

- Cisco XDR
- Palo Alto Networks XSOAR
- Microsoft Sentinel
- Crowdstrike Falcon Logscale
- ServiceNow * (upcoming release)

Automate Incident Response

Data Cloud can be integrated with an external Security Orchestration, Automation and Response (SOAR) platform to carry out faster Incident response and help customers to improve the mean time to detect (MTTD) and mean time to recover (MTTR) values, integrate data security events, and automate data recovery workflows into security incident response playbooks to accelerate recovery in the aftermath of a ransomware attack, which brings efficiency to security and data operations.

Cohesity has partnered with leading SOAR technology vendors:

- Cisco SecureX Integration
- Palo Alto Networks Cortex XSOAR Integration

DataHawk

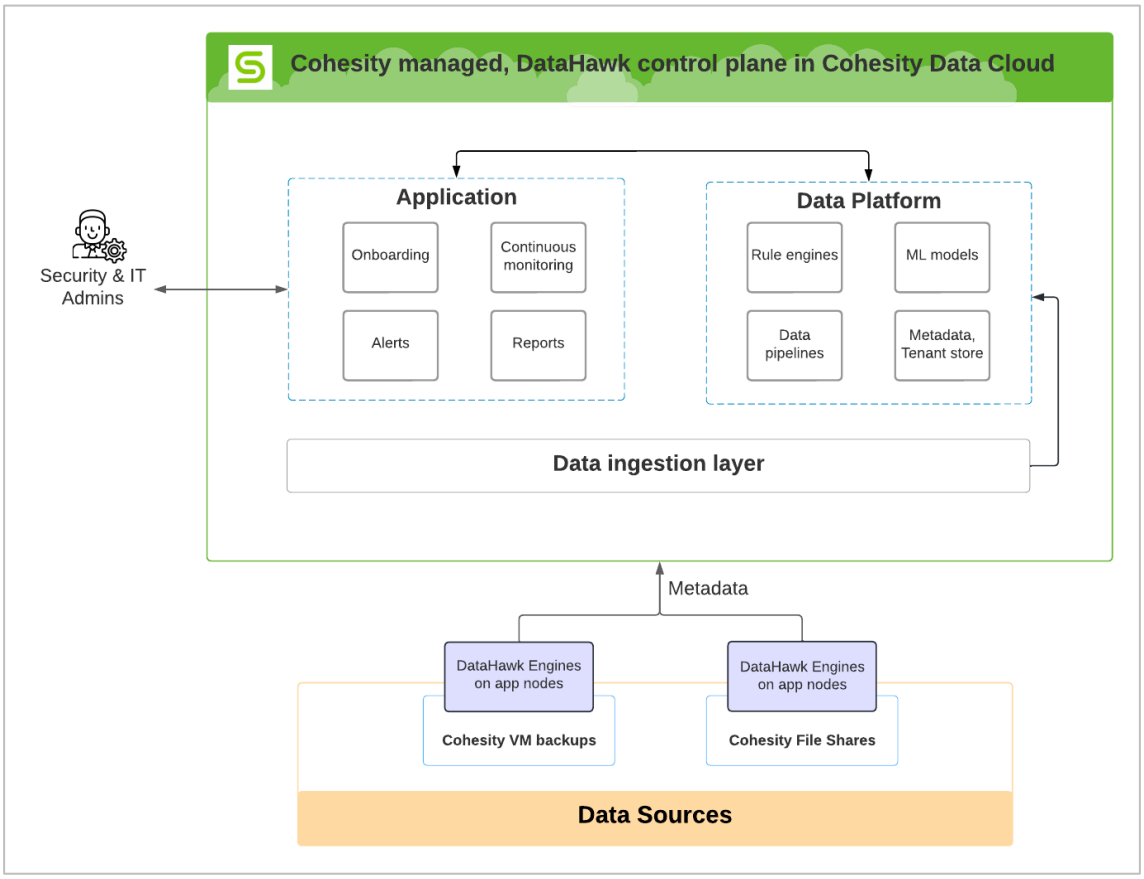
Today's companies and organizations are overwhelmed with the exponential growth in the data they collect, manage, and store. To ensure the quality and security of such data, organizations need robust data security and management solutions that help them understand the breadth and depth of data and enforce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

Cohesity DataHawk offered as a service on the Cohesity Data Cloud, 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, see Cohesity Product documentation.

Figure 5: DataHawk



Secure Data Management

Data handling is another important aspect of security. Cohesity encrypts data both at rest and in transit. This section outlines the security infrastructure in place to handle data at various touchpoints.

Data-at-Rest Encryption

Data-at-rest encryption refers to encryption employed as the data is written to a platform. Cohesity stores data in various locations and has different approaches for different platforms.

Data-at-Rest Encryption on Cohesity

The Cohesity file system provides full at-rest encryption based on the strong AES-256 CBC (Cipher Block Chaining) standard. Only 256-bit keys are used for encryption. The encryption architecture provides high security while maintaining the flexibility to optimally leverage the available hardware and software resources.

The built-in, software-based encryption is hardware-accelerated through the latest Intel processors that support the AES-NI instruction set. Thanks to hardware acceleration, the software-based encryption process has a minimal impact on performance.

All user data is encrypted before it is stored on any storage media. The data is decrypted after it is read from the storage media in memory. The storage media can be SSD, HDD, tape, and cloud storage.

There are three ways to obtain encryption keys:

- Cohesity's internal Key Manager
- External key manager systems (EKMs), including: Cohesity supports KMIP version 1.1 to 1.4, and the following KMIP-based KMS systems have been validated by the Cohesity cluster.

Table 1: KMIP-based KMS Systems

KMS	Documentation Reference
Hashicorp Vault	Hashicorp Vault - Key Management
SafeNet KeySecure	Integration Guide - Cohesity and SafeNet AT KeySecure for Government
Vormetric Data Security Manager	Use Vormetric DSM to Manage Cohesity Encryption Keys
Fortanix KMS	Use Fortanix Self-Defending KMS to Manage Cohesity Encryption Keys

KMS	Documentation Reference
CipherTrust Manager	CipherTrust Manager Documentation Portal
IBM Security Guardium Key Lifecycle Manager	IBM SGKLM Documentation
Hashicorp Enterprise Vault	Manage Cohesity Encryption Keys Using HashiCorp Vault 1.4

- Cloud-based key manager service:
  - AWS Key Management Service

    Keys can be rotated periodically. The default rotation is set to 90 days. Unlike legacy vendors, Cohesity allows customers, especially Managed Service Providers (MSPs), to use different encryption keys for tenants on the same cluster, therefore saving the cost of deploying a separate cluster for a security-conscious tenant.

    Cohesity supports KMIP compliant External KMS in Active/Passive mode to manage the cluster key encryption keys. You can add up to 4 key management services (KMS) servers and create a KMS cluster to ensure high availability of keys. For more information, see Add a Secondary External KMS and Create a KMS Cluster.

Add a Secondary External KMS

To ensure high availability of keys, Cohesity supports KMIP compliant External KMS in Active/Passive mode to manage the cluster key encryption keys. You can add up to 4 key management services (KMS) servers and create a KMS cluster to ensure high availability of keys. For more information, see Add a Secondary External KMS and Create a KMS Cluster.

Data-at-Rest Encryption in the Cloud

With Cohesity, you can use the cloud as another tier of storage (Cloud Tier) or to store copies for long-term retention (CloudArchive and CloudArchive Direct). Cohesity supports all the major cloud vendors, including AWS, Microsoft Azure, Google Cloud, Oracle Cloud, and any S3-compatible storage.

- To use your cloud vendor with Cohesity, you register the cloud storage as an External Target on the Cohesity cluster and provide the cloud storage access keys. The access keys are encrypted and stored on the Cohesity cluster using AES-256 encryption. You can update the access keys from the Cohesity dashboard or by using the Cohesity REST API.
- Though the access keys are specific to the cloud storage provider, Cohesity key storage security is the same regardless of the cloud provider. Cohesity is FIPS-certified and has an internal, software-based key management system (KMS) that stores the key-encryption key (KEK).
- CloudArchive uses its own encryption, independent of data at rest encryption.
- CloudArchive encryption is enabled by default but can be turned off. Cohesity recommends keeping it on.
- Both the data encryption key (DEK) and KEK are encrypted, distributed for resiliency across the cluster, and stored in SSD.
- The cluster creates a new DEK for each External Target. Cohesity provides two options:
  - Store the data, metadata, and encryption keys (DEK/KEK) in the External Target.
  - Store only the data and metadata, and not the encryption keys, in the External Target. This requires the encryption keys to be downloaded and stored outside the cluster. Without the downloaded keys, future CloudRetrieve operations will not be possible.

Data-in-Transit Encryption

In-transit data is any data that is being transmitted from one location to another. Examples include:

- Ingesting data on the Cohesity cluster from a primary site.
- Replicating data between remote offices, from one cluster to another.
- Transmitting data to the public cloud.

Data that is transmitted to a Cohesity cluster, as well as data being transmitted from a Cohesity cluster to an External Target, is encrypted for security.

Primary Site to a Cohesity Cluster

When Cohesity ingests data from primary storage, it first establishes a secure connection with the primary storage over HTTPS. It determines which data blocks have changed from the previous backup run by communicating with the primary storage over the secure connection and then transfers all the changed blocks over the HTTPS connection.

Backup Communication

There are three different ways in which Cohesity communicates to data sources, depending on the type of source being backed up. All three communications are secured to the maximum extent possible.

- **Agent-based backups**. Used by Cohesity DataProtect™ for built-in adapters.
  - Cohesity applies point-to-point encryption using TLS 1.2 encryption for all communications.
  - You can also enable custom certificate-based authentication to enhance security between agents and the Cohesity cluster.
  - Communication is always initiated by a Cohesity cluster. Hence, the agent cannot initiate any operation on the Cohesity cluster.
  - Cohesity has a provision to push backup agents from a central server as well.
- **Mount-based backups**. Used when native database tools are used for performing backups or Cohesity is used as a storage target for backups.
  - When the data is written to Cohesity as a NAS, it is protected through IP allowlists and protocol-level encryption (where available).
  - Only authorized hosts and users have access to the data.
  - For these use cases, the system is configured to take periodic snapshots (per best practices) to ensure there is always a read-only copy available if the data is deleted or modified for some reason. The NAS read/write View is only used for staging the data temporarily. As soon as the backup is complete, a clone is created and marked as immutable.
  - You can also extend the data protection using DataLock, Cohesity's WORM feature.
- **API-based backups**. Cohesity uses TLS 1.2 encryption for all communication for point-to-point encryption.

Restore/Clone Communication

There are three different ways in which Cohesity communicates with source depending upon the type of source data being restored. All three communication types are secured in the best possible way.

- **Copy-based Restores**
  - **API-based restores**. Cohesity uses TLS 1.2 encryption for all communication for point-to-point encryption.
  - **NBDSSL-based VMware restores**. You can use NBDSSL to restore VMware data. NBDSSL is a VMware variant that uses SSL to encrypt all data passed over the TCP connection. The NBDSSL transport method is built into the virtual disk library, so it is always available. This is one of the fastest ways to restore data back to VMware.
  - **Agent-based restores**
    - Cohesity uses TLS 1.2 encryption for all communication for point-to-point encryption. You can also enable custom certificate-based authentication to enhance security.
    - Communication is always initiated by the Cohesity cluster.
    - For all direct access from an agent to the cluster, say for Instant Volume Mount (IVM), read/write Views are sandboxed.

    - Even if the server on which the agent installed is compromised, it cannot perform any invasive activity on the original copy of the backed-up data or any other data on the cluster, as it is inaccessible.

- **Instant Restores and Clones**
    - Cohesity snapshots are immutable. For restore operations, snapshots are cloned. The snapshots are fully hydrated (that is, they contain all the pointers to changed and unchanged blocks).
    - All read/write operations to internal Views are sandboxed. For restore operations, the internal View is first cloned and then presented to the source as a drive (IVM) or as a share (SMB, NFS, etc.).
    - Note that cloning is extremely fast, as it relies only on metadata pointers and involves no data movement or copying).

Replication from One Cohesity Cluster to Another

A source cluster starts a replication session by initiating a handshake with the target cluster over an HTTPS connection. Upon receiving the handshake request, the target cluster obtains a session key from its local Key Management Server (KMS) and sends it to the source cluster over the HTTPS connection.

The source cluster stores the received session key in its local KMS and completes the handshake. At this point, both the source and the target clusters have the session key.

The source cluster uses the session key to encrypt the data and transfer it securely for that replication session.

Data Transfer to the Cloud

Cohesity establishes a connection to an External Target only when making REST API calls to perform an archive or recovery operation.

Cohesity does not include External Target access keys in the API request. The request is signed using the External Target's access key and the signature is sent using the Authorization request header.

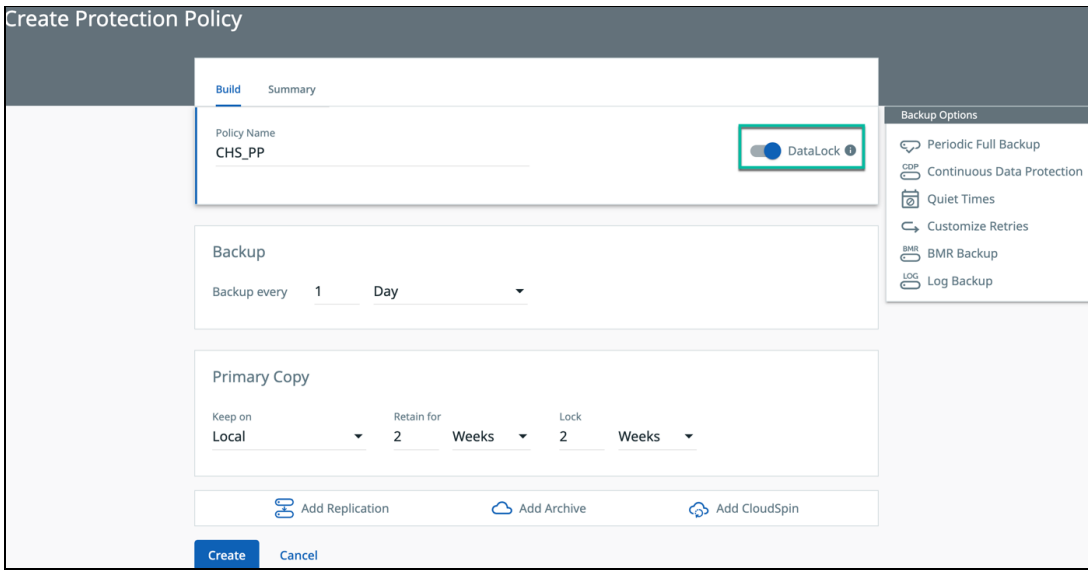
Cohesity uses TLS 1.2 to encrypt in-transit data. Currently, Cohesity uses mTLS (mutually authenticated TLS) for communication with agents, and can use TLS without mutual authentication with External Targets if they support and are configured to use TLS.

For Cloud Tier, encryption is always on and cannot be turned off.

DataLock

DataLock is the WORM time-bound feature that locks and retains files in a View for compliance and regulatory purposes. It ensures that your protected data, including local backups, archives, and replication, cannot be modified until the DataLock expires. Once applied, a DataLocked snapshot will be deleted only after its retention period expires.

A DataLock prevents all users, excluding those who have the Data Security role in Cohesity, from modifying or deleting any snapshots that were generated by a Protection Group. Only users with the authorized Cohesity Data Security role can add, modify, or remove a DataLock.



NOTE: Even a Cohesity cluster administrator cannot delete or modify WORM-protected data.

Legal Hold

Users who are assigned the Cohesity Data Security role can also put a Legal Hold on existing snapshots (Protection Runs), to preserve them for legal purposes. Once a Legal Hold is applied, the retention period is ignored, and the snapshot is preserved until the Legal Hold is removed. Legal Hold Snapshots can only be deleted by a user with the Data Security role.

NOTES:

- You can add a Legal Hold to both regular and DataLocked snapshots.
- You can add a Legal Hold to a Protection Run (snapshot) or to individual objects in a Protection Run.
- If you add a Legal Hold to a Protection Run, it applies to all the snapshot objects that were backed up by that Protection Run, and the Legal Hold is propagated to replicated and archived objects.
- If you add a Legal Hold only to selected objects in a Protection Run, the Legal Hold is propagated to archived objects, but not to the replicated objects. You must manage the Legal Hold on the remote replication cluster manually.
- A Legal Hold prevents snapshots from being deleted until the Legal Hold is removed.

Secure Network Communication

Network security plays a pivotal role in keeping an ecosystem secure. To give customers direct, granular control of a Cohesity cluster's connections to their networks, Cohesity provides IP allowlisting on different levels and the information you need to manage traffic across a cluster's ports.

IP Allowlist

Cohesity gives you the option to apply IP allowlists to individual Cohesity Views as well as to define a global allowlist for an entire cluster.

- **View Allowlist**. If a View has an allowlist, only the systems with IP addresses specified in the Subnets of the View's allowlist have privileges to access and mount the View.
- **Global Allowlist**. Cohesity supports a global allowlist that applies to all Views in the cluster that don't have their own allowlist.

If a View has its own allowlist, the View allowlist supersedes the global allowlist.

Ports

By default, all the ports on a Cohesity cluster are disabled except for some known ports. Preconfigured IP tables in the underlying OS allowlist the services that can access each other internally.

Cohesity sends the following types of traffic over the network:

- **IPMI traffic**. For admins to access nodes, typically for pre-boot BIOS access and post-boot console access.
- **Management traffic**
  - From nodes to external services such as Active Directory, DNS, NTP, and SNMP.

    NOTE: Protocols like SNMP are not enabled by default. They must be enabled by an administrator.
  - For administrators to access Cohesity.
- Backup and restore traffic for moving data between protected Sources and Cohesity.
- Replication traffic for replicating data from one cluster to another cluster.
- Data access traffic for accessing data on the cluster using protocols such as NFS, SMB, or S3.
- Archive and tiering traffic for moving data to External Targets such as cloud or tape storage.
- Support Channel traffic between nodes and Cohesity's Support servers. The Support Channel is optional and you can disable it for an isolated/dark site.
- Internal traffic between nodes in a cluster.

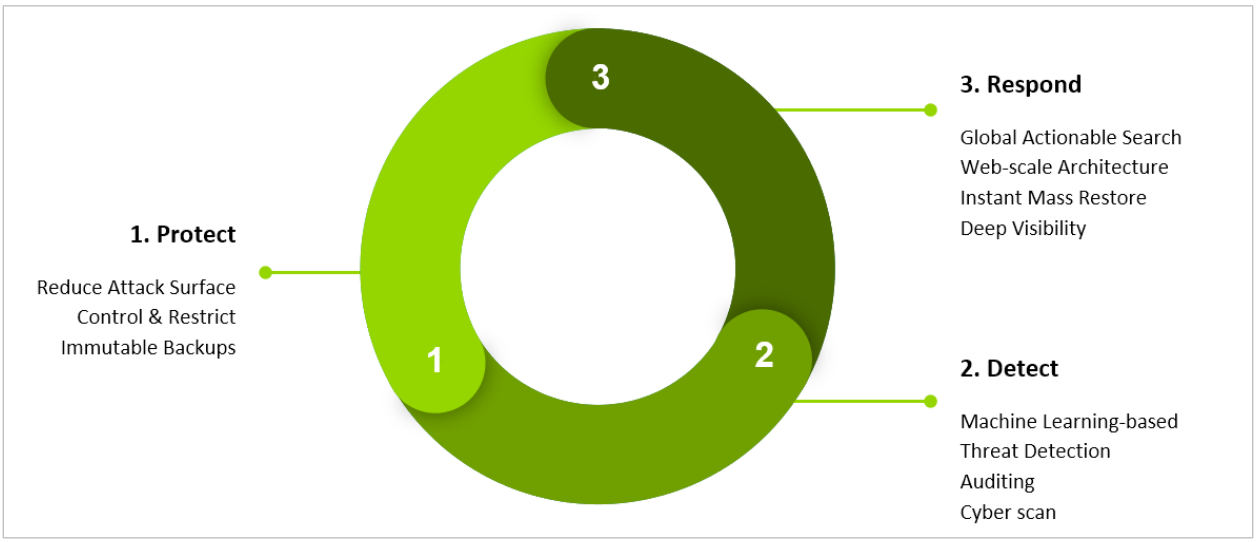
Cohesity Protects Against Ransomware

Cohesity offers a comprehensive solution against sophisticated ransomware attacks targeted at your backup and file-service data. Cohesity's Ransomware solution uses a three-pronged approach to first safeguard the Cohesity backup and file-service data. And then use this data to detect and respond to attacks on primary data:

- **Protect**. Protect the data against ransomware.
- **Detect**. Detect a ransomware attack on production infrastructure using backup data.
- **Respond**. Respond quickly in case of a ransomware attack on your primary data.

The same three principles are applied to both backup as well as file-service data, as outlined for each below. For more details, see Cohesity Ransomware Protection solution guide.

Figure 6: Cohesity Enables You to Protect, Detect, and Respond



Secure Backup Data

Backup is the last line of defense against ransomware attacks. However, sophisticated malware now is targeting backup data. Attackers gain access to legacy backup infrastructure through Windows- and Linux-based media and master servers. Cohesity's modern architecture helps protect backup data from becoming a ransomware target with these strategies:

- **Protect**. Guard your backup data.
- **Detect**. Cohesity uses machine learning-based detection to protect against potential attacks on your primary IT infrastructure.
- **Respond**. Cohesity provides rapid recovery using several advanced Cohesity technologies.

Together, these capabilities provide rapid recoveries and dramatically reduce downtime when your organization comes under attack.

- **Protect—Guard the Backup Data**. Cohesity backups are protected under our secure design principles. Two of the prominent defense mechanisms for your data are the reduction of attack vectors and making the data immutable.
  - **Reduce Attack Surface**. Cohesity helps reduce your data footprint and exposure by consolidating various backup components, disaster recovery, file services, object storage, dev/test, and analytics on one web-scale platform.
  - **Control and Restrict**. Cohesity provides a rich set of features that help organizations guard themselves against unauthorized access (the main source of malware and ransomware attacks).
    - Multifactor Authentication
    - Granular Role-based Access Control
    - No Service Backdoor
    - Secure API access
    - IP Allowlisting
    - Cluster Session Management
  - **Immutable Backups**
    - Cohesity backup snapshots are immutable and at no point are they exposed to any external clients. Only the backup service running on Cohesity can write to the file system by the means of authenticated APIs.
    - All read/write operations to internal Views are sandboxed. For restore operations, the internal View is first cloned and then presented as a drive (IVM) or share (SMB, NFS, etc.) to the source.
    - Backup and restore communications are secure.
- **Detect—Machine Learning-based Threat Detection**. Cohesity Helios, our SaaS-based global management solution, helps you detect anomalous patterns to identify and alert you to potential ransomware attacks on your primary IT infrastructure that might be in progress.

  When the rate of data change among primary files is out of the norm, Helios alerts not just the IT administrator but also Cohesity's Support team. Anomalies are detected when they reflect data changes that are larger than the normal patterns, including:
  - Daily change rate on logical data.
  - Daily change rate on stored data (after deduplication).
  - Patterns based on historical data ingest.
  - Entropy (randomness of data).

  In addition to monitoring backup data change rates to detect potential ransomware attacks, Cohesity's machine-learning algorithms also help locate a clean copy of the data that can be used for recovery.
- **Respond—Rapid Recovery from Attack**. In the event of an actual ransomware attack, you will need to restore your data from your backups. Cohesity provides you the ability to recover data from a previous

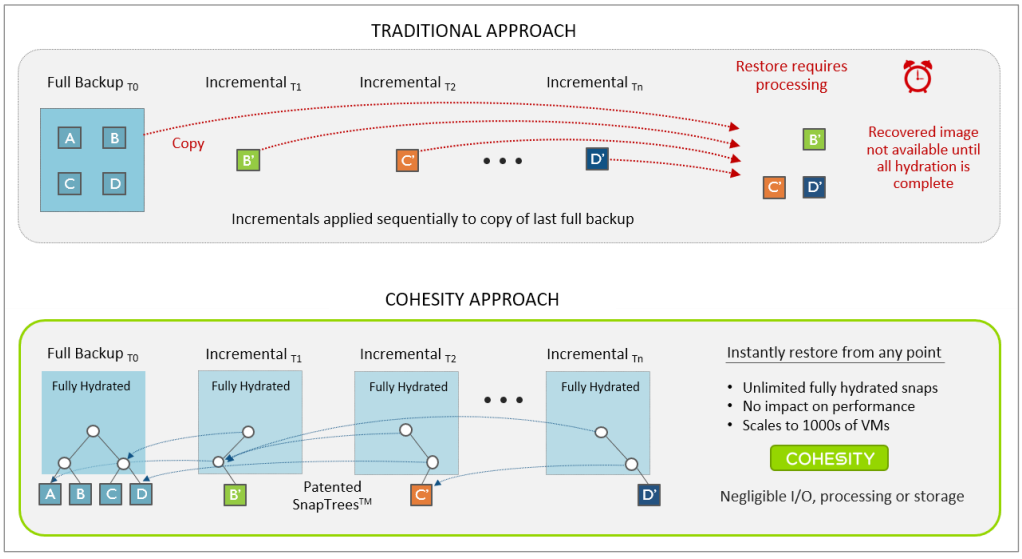
point in time, with reliability and in the most efficient manner possible, thereby reducing recovery times considerably, meeting much more aggressive Recovery Time Objectives.

The most important requirement after a ransomware attack is having the ability to quickly and cleanly recover data that has been compromised. Unlike other solutions, Cohesity helps you locate and delete infected files across your global data footprint, including in the public cloud, and then to take corrective action.

With these Cohesity capabilities, you can rapidly and cleanly restore your data at scale:

- **Unlimited Scalability**. A web-scale platform that allows IT administrators to grow their Cohesity cluster from three to an unlimited number of nodes with the ability to store unlimited snapshots and clones without affecting performance.
- **Global Actionable Search**. Unlike legacy solutions that rely on third-party search products, Cohesity's unique, Google-like global search capability allows you to locate data quickly and initiate the recovery process.
- **Deep Visibility**. Cohesity CyberScan gives you deep visibility into a backup snapshot's health and recoverability status. CyberScan shows each snapshot's vulnerability index to ensure that no cyber vulnerability is re-injected into the IT production environment as part of the restore process. This helps you recover from a clean copy of the data.
- **Instant Mass Restore**. With Cohesity's powerful instant mass restore technologies, IT administrators can recover hundreds of VMs instantly, at scale, to any point in time.
  - Cohesity's SpanFS™ file system is a patented B+ tree metadata structure and a Distributed Redirect-on-Write (D-ROW) implementation.

Figure 7: Cohesity SpanFS Enables Instant Mass Restore



- All snapshots on Cohesity are kept fully hydrated (that is, in the same format as in the original VM environment), so the system doesn't have to spend time and resources stitching backups.
- Because SpanFS is a distributed file system that can mount a clone of the backup data using the NFS or SMB protocol, data is instantly available while the recovery is happening in the background.

Cohesity SmartFiles Guard Against Ransomware

Cohesity SmartFiles is the industry's first software-defined, data-centric file and object solution for the enterprise and extends traditional NAS capabilities by integrating data and apps in a single platform.

In addition to the innovative integration, Cohesity SmartFiles employ a proactive 'protect, detect, and respond' approach:

- **Protect**. Cohesity has the ability to take a snapshot that acts as a point-in-time, read-only replica of the file system. If you enable DataLock, Cohesity's WORM feature, on a View, even super users cannot delete it. Cohesity employs anti-virus software that can help to detect some types of attacks. You can use IP allowlisting to restrict access to your NAS data to specific hosts. For SMB, Cohesity supports SMB signing and sealing, as well as Kerberos-based authentication.
- **Detect**. Cohesity helps you by analyzing the unstructured data residing on the Cohesity file shares and auditing the access patterns of the files. It then flags any anomalous access behavior. Some categories of ransomware change the entropy of the files by altering the file data or attributes. This activity can indicate a potential attack. Using Cohesity Helios anomaly detection feature, you can get an alert in case of any anomaly.
- **Respond**. Snapshots are read-only so they cannot be altered, and a file system can be reverted to a previous point in time using a snapshot.

Cohesity Protects Against Time-Based Attacks

The Cohesity Data Cloud is designed to operate in an environment where time can be reliably and securely established. The Cohesity Data Cloud supports Network Time Protocol (NTP) and implements several defense in depth techniques to ensure a) the platform can utilize trustworthy NTP sources in a secure manner, and b) there are checks and failsafe mechanisms in place if the NTP servers and their transmitted timestamps are compromised or the platform hardware fails. These techniques help prevent malicious manipulation of NTP and other time-based attacks that might enable premature removal of DataLock protection from backups snapshots and protected Views.

The Cohesity Data Cloud uses a layered defense to minimize time-based attacks that can be used to compromise data on the platform.

- **Time Synchronization**—A tiered architecture minimizes the likelihood of individual nodes within a cluster falling out-of-sync. The primary node in the cluster is responsible for syncing with configured external NTP sources. Secondary nodes in the clusters defer to the primary node as their authoritative source of time to minimize the risk of node time shifts within a cluster.
- **Secure NTP Communication**—The platform supports secure NTP to ensure it communicates securely with authenticated, trustworthy sources of time and that the communication between the platform and those sources are resistant to attacks, such as man-in-the-middle or spoofing.
- **Time Shift Resistance**—The platform includes logic to detect and resist large shifts in time based on timestamps being transmitted from configured NTP sources—this helps ensure that if a configured NTP server is compromised at the source, then the platform will not unconditionally reset its time based on whatever the NTP server is reporting.
  - The Cohesity cluster invalidates the NTP server if it detects a sufficiently large shift in time between the configured NTP source and the current system time (>10 seconds). Cohesity cluster dispatches an alert.
  - The Cohesity cluster applies slewing if the NTP-supplied time differs from cluster time. The cluster time cannot adjust forward (or slow down) by more than one second per 2,000 seconds. As a result, for a WORM retention time of 14 days (1.2 million seconds), the maximum amount of time by which the backup can expire prematurely is 10 minutes (600 seconds), which is immaterial.
  - The Cohesity cluster falls back to the in-built CMOS clock on the primary node, if all NTP servers are invalidated.
  - The cluster sets its time using the CMOS time on the primary node, if all the cluster nodes are power cycled at the same time.
- **Fallback to CMOS clock**—The platform will fallback to the CMOS clock to ensures a reliable source of time for the cluster when external sources of time are inaccessible or deemed unreliable. Cohesity cluster dispatches alerts when the NTP server is deemed unreliable, or a hardware issue may affect the reliability or accuracy of the local CMOS clock on the primary node in the cluster.

- **CMOS Clock Protection**—To protect operations following a cluster or node reboot from drift or latent errors in CMOS time, the cluster will periodically reset the CMOS time on all the nodes to match the cluster time.
  - Manually resetting CMOS time on a node cannot be performed without low-level access (e.g. root or BIOS-level). Root-level access to the platform can only be achieved using a different set of credentials from the cluster administrator and can be further protected with Multifactor Authentication.
  - In the rare event that the CMOS clock on the future primary node fails immediately leading up to the reboot, the cluster will use the CMOS clock on a different node to set the cluster time during reboot.

Secure App Ecosystem and Marketplace

Cohesity uniquely brings the compute to data to derive business insights by running Cohesity and third-party applications on Cohesity. You can obtain great value from your backup and unstructured data by using Cohesity's Marketplace apps, which cater to a number of use cases around data analytics, data security, and data management.

Athena, Cohesity's app platform, is a secure platform built on top of Kubernetes running on the Cohesity cluster. The security of the app ecosystem is of paramount importance and for that reason, Cohesity imposes rigorous qualifications before an app is added to the Cohesity Marketplace, and protects the whole app ecosystem with important guardrails:

- First things first, use of apps on a Cohesity cluster is disabled by default. Enabling the app ecosystem and instantiating any app is solely at the discretion of the customer.
- Cohesity has a process for vetting and onboarding any ISV vendors who want to publish an app to the Marketplace.
- Athena only runs apps that have been digitally signed by Cohesity. Hence, only the apps that are hosted on the Cohesity Marketplace are certified by Cohesity can run on the app platform.
- By default, each app runs under its own isolated network and cannot interact with other apps.
- All the microservices for an app run inside containers, and these containers communicate with each other via an internal container network. This network is not exposed outside the Cohesity cluster.
- An app cannot communicate over the Internet until you grant network access for it via Cohesity's firewall allowlisting.
- The app ecosystem is RBAC-aware. Resources that are accessible to the user on the Cohesity cluster are visible to the app that that user launches.
- Apps only have read/write access to their own internal storage and cannot access storage used by other apps or Cohesity services.
- Apps are required to pass thorough validation benchmarks, such as code reviews, vulnerability scans, and more before they are certified and onboarded.

Compliance Standards and Certifications

Cohesity employs security guidelines, standards, and specifications to ensure the safety and integrity of your data:

- **FIPS Compliance**. The Cohesity cluster is FIPS 140-2 certified. The encryption module has been validated on the Data Cloud with NIST for FIPS certification. The encryption module always operates in FIPS mode. You can find detailed information in the Cohesity FIPS 140-2 Non-proprietary Security Policy (PDF) on the NIST website.
- **Common Criteria (EAL2+ Certification)**. Common Criteria is an internationally recognized set of guidelines for evaluating IT security products. Common Criteria:
  - Is a catalog of criteria and a framework for organizing a subset of the criteria into security specifications.
  - Is a methodology for evaluating security features.
  - Can be applied to hardware, software, firmware, or a combination thereof.
  - Allows vendors to describe a product's security functionality with proof to support their claims.
  - Cohesity realizes the value of being a Common Criteria participant. To view the CC certificate, see MyCC.
- **WORM (Write Once Read Many SEC 17a-4(f) Certification)**. Long-term records retention is often mandated by regulations and compliance rules. For example:
  - In the financial services industry, SEC Rule 17a-4(f) specifies that “electronic records must be preserved exclusively in a non-rewritable and non-erasable format.”
  - Other industries must meet similar requirements when they store mission-critical information.

  Cohesity’s WORM technology, DataLock, addresses these requirements by providing immutable locking and secure data retention capabilities.

  Cohesity implements WORM as a DataLock for Views. Views with a DataLock are locked (read-only) for a user-specified duration. Any user who has access to the View can clone a copy of the View as a DataLock View and set the lock retention time. During that time period, even an admin user cannot delete the View or modify the expiration. Only users with Cohesity’s Data Security role can delete the View, extend the lock period (which cannot be reduced), add allowlisted IPs, change the QoS, and change the description of the View. After the lock period expires, the View can be deleted by any user who has permission to delete it. A replicated or archived DataLock View retains its DataLock properties. You can clone a DataLock View to a regular or DataLock View.

- **Department of Defense's Information Network Approved Product List (DODIN APL)**. Cohesity is DoDIN APL certified. To use Cohesity as per DoDIN APL requirements and recommendations, you need to enable DoD mode.

  As part of the DoDIN APL requirements, Cohesity provides the following security features:

  - Login banner support
  - Transfer audit logs to a Syslog server over a secure TLS connection.
  - Certificate mapping-based authentication support
  - Support to configure the banner on the Cohesity UI.
  - Server-side session management
  - Node-to-node traffic encryption

  For more information, see the online Help article Use Cohesity in DOD Mode.

- **Authorization to Operate (ATO)**. Cohesity offers the following ATO features:
  - ATO for highly classified US Department of Defense (DoD) agency networks.
  - DoD customers have created STIGs for Cohesity on DoD top-secret networks.
  - ATO for highly classified Department of Energy networks.
  - ATO for US Air Force networks that support mission-critical programs including Air Force GPS ground systems.
  - Supports the US intelligence community in many programs.

- **General Data Protection Regulation (GDPR)**. The GDPR is an EU regulation designed to strengthen data protection for residents of the EU. It became effective on May 25th, 2018 and applies to any company controlling or processing Personally Identifiable Information (PII) of EU residents, regardless of the location of the company. The GDPR imposes a broad set of legal, governance, and technical requirements on companies processing personal data. A subset of these requirements—those related to data protection and data management—are particularly relevant for storage platforms that are used to store personal data.

  Cohesity has a strong vision to enable our customers to be at the top of their GDPR compliance. The tools and product functionality that Cohesity provides as part of its vision fall into the following categories:

Table 2: Cohesity Functionality and Capabilities

FUNCTIONALITY	MANDATE	FEATURES OFFERED
Protect	• GDPR mandates data protection by design and by default, making privacy by design an express legal requirement.	• The encryption architecture, based on strong AES-256 Cipher Block Chaining standard and FIPS-certified, provides high end-to-end security while allowing optimal use of available resources.

FUNCTIONALITY	MANDATE	FEATURES OFFERED
	• Organizations should also be able to demonstrate transparency when validating compliance.	• Granular control through Role Based Access Control and strong Active Directory integration. • File- or view-level WORM provides immutable locking and secure data retention capabilities.
Minimize	• GDPR mandates data minimization as one of the main tenets to ensure that companies maintain reduced amounts of stored PII data. • Here, the PII needs to be kept only for the time period relating directly to the original intent of capturing the data.	• Cohesity's architecture inherently minimizes data copies, reduces attack footprint, and tracks copies through centralized data management. • Granular control over and automation of retention policies enables customers to keep PII only for intended periods. • Cohesity effectively relocates files to 'on-demand' to minimize spread of PII data.
Locate	• The GDPR mandates getting a 360-degree view of what PII is stored by an organization. In addition, the organization should be aware of: ○ What PII they store and why. ○ Where it comes from. ○ Where the data is stored, and the retention policy on the personal data. ○ Who has access to the data. The organization must also monitor the movement of the data.	• Scheduled update to data maps that delineate: ○ Location and Movement Tracking (source & destination) of PII. ○ Categories of PII stored. ○ File containing PII. ○ Retention policies of PII. ○ Access rights to PII. • Leverage Cohesity reports to complete Data Protection Impact Assessments (DPIAs), if needed.
Search	• The GDPR mandates that any EU resident can request visibility of PII from a company. • They can also request that the PII be deleted, modified, corrected, or exported.	• Search within unstructured data for multiple categories of PII. • Input PII patterns and their variations, and file types (txt, doc, pdf, xls, zip, jpeg) to scan using templates.

FUNCTIONALITY	MANDATE	FEATURES OFFERED
		• Inject custom code to run data processing jobs on stored data using in-place analytics tools. • Report search results in the txt file format or integrate with third-party data visualization and analytics tools.
Monitor	• The GDPR mandates companies to monitor and report security breaches. • Companies are obliged to communicate breaches to the relevant supervisory authorities, and to the affected individuals in certain cases. • Demonstrating appropriate reporting procedures after a breach is identified can validate compliance.	• Cohesity uses allowlists to prevent portability of PII. • When data is tiered, archived, or replicated to a non-Cohesity target, users receive notifications and warnings. • When data leaves the EU while still on Cohesity, users receive notifications. • Cohesity can export cluster- and system-level audit logs for additional analytics and breach detection.

- **Payment Card Industry Data Security Standard (PCI DSS)**. Cohesity adheres to the security benchmarks and requirements that are mandated by the PCI-DSS, including:
  - Authentication and access.
  - Logging and auditing.
  - Browser, plug-in and/or third-party software requirements.
  - Management systems and software.
  - Releases, patching, and updates.
  - Granular service controls.
  - Exposed protocols.
  - Monitoring, alerting, and calling home.
- **Secure Government Clouds**. Cohesity supports AWS GovCloud, Azure Government Cloud, and is working towards C2S support.
- **Trade Agreements Act (TAA).** All Cohesity appliances are compliant with the Trade Agreements Act (19 U.S.C. & 2501-2581) and ship from San Jose, CA.

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 Cohesity product design & solutions.

Karthick Radhakrishnan is Director, Technical Solution Engineering. In his role, Karthick focuses on DataProtection, Platform Security and leads the technical solutions team.

Other major contributors include:

- Sandler Rubin, Product Management
- Rob Young, Product Solutions
- Adaikkappan Arumugam, Director, Product Solutions
- Lintu Thomas, Engineering
- Raj Dutt, Marketing
- Subash Babu, Staff Technology Editor, TSE

Document Version History

VERSION	DATE	DOCUMENT HISTORY
7.2	Jun 2024	7.2 release updates
7.1	Apr 2024	Changing “Data-in-Flight” to “Data-in-Transit”
7.0	May 2023	DataHawk updates
6.0	Jan 2023	Updated with Cohesity 7.0 Features
5.0	Oct 2022	Updated latest Security Features
4.0	Jan 2022	Added “Cohesity protects against time-based attacks” section.
3.0	Nov 2021	Third release
2.0	April 2021	Second release
1.0	July 2020	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.