COHESITY

# Cohesity Data Cloud (SaaS) Security Brief for NetBackup

*Information Security Measures in Cohesity-managed Data Cloud Services*

*Version 1.0*

October 2025

**ABSTRACT**

*Cohesity Data Cloud is designed, developed, and operated with security as a core tenet. Get an overview of the information security measures in Cohesity-managed Data Cloud Services.*

# Table of Contents

# Figures

# About Cohesity Data Cloud and Helios

Today’s organizations are overwhelmed by the exponential growth in the amount of data they collect, secure, manage, and store. As an organization, you should be able to focus on using your data without worrying about deploying additional hardware in your data center.

We designed Cohesity Data Cloud Software as a Service (SaaS), a modern data and security platform designed for today's multi-cloud environments, to provide enterprise-ready data protection and management capabilities such as backup and recovery, file and object services, cyber vaulting, threat intelligence, data classification, disaster recovery, and more, wherever you need them.

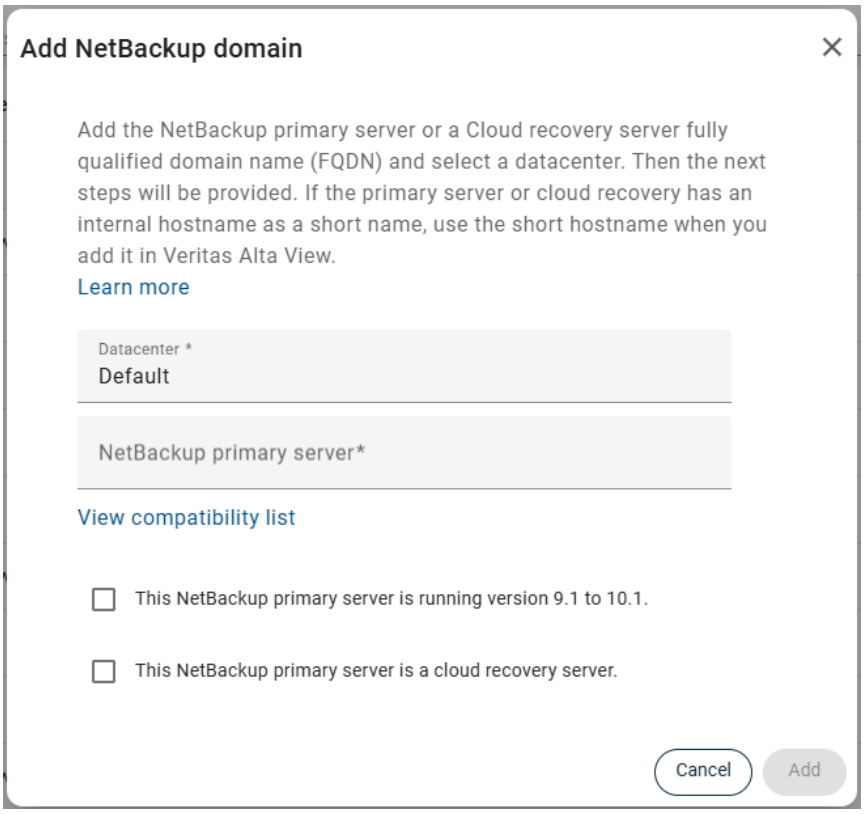
Cohesity’s Data Cloud management service platform, also known as Helios, provides you with a single management user– interface that enables you to manage your data globally, wherever it resides: on-premises, at the edge, and in the cloud.

# Connection from NetBackup to Helios

NetBackup primary servers connect to Helios and IT Analytics endpoints to send metadata such as policy and job details, and also to get API calls from Helios to perform management tasks such as changing policies.

The NetBackup primary server uses two means of communication: data collector and NetBackup WebSocket client. A data collector and NetBackup WebSocket are installed on the primary server. NetBackup primary server initiates the connections to Helios and IT Analytics on port 443 (HTTPS).

Figure 1: Add a NetBackup Primary Server Dialog Box



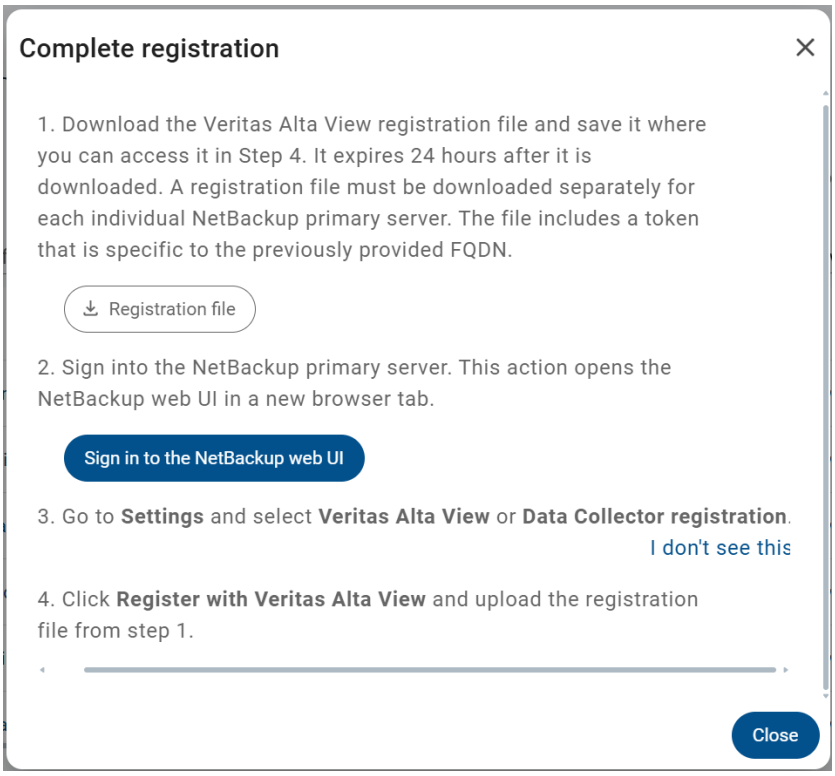

The data collector sends data to IT Analytics which is used by Helios, and the NetBackup WebSocket client sends data directly to Helios.

Connecting a primary server to Helios requires a registration file to be downloaded from Helios. This registration process sets up a secure means of bi-directional communication between NetBackup and Helios.

The registration file is customized for each NetBackup primary server; it includes an API key and the public certificate from Helios. The API key is unique to each NetBackup primary server and used by Helios to authenticate connections and requests. The public certificate is used to ensure that NetBackup can only connect to the Helios endpoint and none other.

The registration file must be installed on the specified primary server within 24 hours after it has been downloaded (see Figure 2). A NetBackup administrator user is authorized to install the registration file on the primary server. After the registration file is installed, the primary server will complete the registration process with Helios.

Figure 2: Complete Registration




Mutually, NetBackup creates an API key for Helios automatically as part of registration, enabling bi-directional authorization. API keys are fully manageable and available to rotate.

As a final part of the registration process, the data collector consumes the registration file which has the information needed to connect the primary server to IT Analytics. JSON web tokens are used for communication between the data collector and the NetBackup primary server.

## Connection Details

All communication between the primary server and Helios is secured with TLS 1.2 using the most secure cipher suites.  The API key and token used for authorizing the connection are stored in encrypted format on the primary server.

The primary server needs to connect two endpoints on port 443:

- Helios: https://helios.cohesity.com
- IT Analytics agent: https://helios-itaanalyticsagent.cohesity.com

Use of a proxy is supported between NetBackup and Helios. Proxy configuration is supported for NetBackup versions 10.1.1 and newer. The data collector only collects information necessary for operational capability and does not read backups or collect backup content data such as filenames or user information.

# 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.

Note: Helios does not access the backup data, only the metadata and configuration details are accessed from NetBackup domains.

## Metadata Collection

In every data center solution, the security of the data and metadata being managed is critical. In Cohesity's products and services, security is central in every phase of data management. When a customer uses Helios for managing NetBackup, it *only* collects metadata. See (NEED LINK FOR METADATA GUIDE)

> **IMPORTANT**: The Helios management service does *not* collect customer data from the data sources that the customer manages.

## Data Isolation

Each Helios tenant's metadata is logically segregated and isolated from the other tenants. Every Helios customer is provided with a secure environment, where the boundaries are controlled to only allow the appropriate communication and keep undesired traffic out. Each customer is provisioned as a tenant within Helios, which is the management plane and hosted in AWS, and within IT Analytics the reporting database is hosted in Oracle Cloud Infrastructure. Helios uses AWS Web Application Firewall. IT Analytics uses Oracle's Web Application Firewall (WAF). Proxies are also supported.

## Data-at-Rest Encryption

All customer data is encrypted at rest using AES-256-GCM, and the encryption keys are managed in a key management system (KMS). Helios relies on AWS KMS for key management.

For more information, see Cohesity product documentation.

Encryption of data-at-rest within IT Analytics is done with Oracle using transparent data encryption (TDE).

### Data-in-Transit Encryption

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

- Transmitting metadata and configuration data from the primary server to Helios.
- Data transferring from IT Analytics to Helios.
- Replicating data between remote offices, from one NetBackup domain to another.
- Transmitting data to the public cloud.

Data that is transmitted to a NetBackup primary server, as well as data being transmitted from a NetBackup primary server to an External Target, is encrypted for security.

### Data Deletion

Helios stores metadata about the NetBackup environment. Data purges from the NetBackup application within Helios happen periodically every seven days for job data; however, the data related to a specific domain can be deleted manually within Helios. Data purges within IT Analytics are configurable for several objects, but jobs data is stored indefinitely for compliance reporting reasons. If a customer de-provisions, the Helios data is removed within 30 days. Transient metadata is deleted as it is deleted within NetBackup.

### Secure Communication

Cohesity Data Cloud secures data in transit through secure, modern encryption protocols Transport layer security (TLS1.2) and Mutual Transport Layer Security (mTLS) with only FIPS-approved cipher suites protection throughout the Cohesity Cloud Service, employing these methods:

- Cohesity NetBackup primary server to Data Cloud Management Service: TLS 1.2

Inter-microservice communication in the Helios management service is managed via a service mesh (a dedicated infrastructure layer for facilitating service-to-service communications). Each microservice is assigned a specific service account and a corresponding IAM role. Also, there is no direct access to Cloud Vault.

### Vulnerability Scanning

Cohesity conducts regular vulnerability scanning using internal and third-party assessment of security, with penetration testing in preproduction and production. These periodic tests help ensure that Helios remains secure.

Cohesity uses standard industry processes and tools for assessment and notification of external threats and software vulnerabilities discovered by other trusted security sources.

## User Auditing

All end-user logins, in-application activity and API client activity are audited. Additionally, per data handling guidelines, all Cohesity access to production resources (Support, Provisioning & Management, Security Operations Center) is also fully audited.

## Data Resiliency and Availability

Helios as the management service is built on the Cohesity Data Cloud platform, which maintains an availability of 99.9% (‘*three 9’s*’).

# Secure Platform Architecture and Deployment

Cohesity takes the security of our customers' data very seriously. Cohesity Data Cloud is designed, developed, and operated with security as a core tenet guiding our approach. What's more, the Data Cloud architecture is modular, enabling a fast, scalable solution while remaining secure, available, and flexible. Cohesity implements security controls with a defense-in-depth approach across each module, while the communication between modules is secured across the Data Cloud service.

## Secure Modular Architecture

The Data Cloud platform delivers a centralized Management Service (Helios) developed, maintained, and managed by Cohesity. Cohesity's infrastructure for this application is based on a major public cloud's industry-leading architecture and framework. The Management Service is behind a DMZ (or 'demilitarized zone,' a physical or logical subnetwork that adds a layer of security). All user access requests terminate at the DMZ. The Management Service is hosted on AWS and is developed and managed by Cohesity.

# Identity and Access Management (IAM)

Identity and access management is a critical security aspect for any service. Cohesity Data Cloud SaaS platform implements strong IAM controls to manage access, authentication and authorization, and auditing across the service. The central mechanism for controlling access to the service and the data you're managing are user access rules which are built around user *personas* that reflect the different types of users on the service.

## RBAC

Role-based access control (RBAC) is built into each tenant, with zero trust between tenants, delivering a separation of duties within the product. The standard roles within Helios are specific to the functions available within the product.

## Password Policy

These restrictions apply to all local users:

- Minimum of 12 characters in length
- Must include at least three of the following four types of characters:
  - Alphabetic character
  - Numbers (0-9)
  - Special characters (!"#$%&'()*+,-./:;< = > ?@[\]^_`{|}~)

## Multifactor Authentication (MFA)

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.

## Firewall Profiles

Cohesity allows users to configure firewall profiles to restrict the incoming traffic on a Cohesity cloud service. Ensure that port 443 is open for the following FQDNs:

- Helios: https://helios.cohesity.com
- IT Analytics agent: https://helios-itaanalyticsagent.cohesity.com

## Multi-Person Authorization

The admin can further control the key operations via the multi-person authorization approval process. Multi-person authorization ensures that a second authorized user approves actions before they are performed.

For more information, see Cohesity product documentation.

# Cohesity Access

Cohesity maintains a highly restrictive approach to internal access. Access is based on a strict need-to-know basis related to the job responsibility for managing and maintaining the system. Cohesity adheres to the principles of least privilege and separation of duties and applies to internal access and authorization controls.

Before a user can log in to a particular role, they must meet established qualification criteria and obtain documented management approval beforehand in every case. A unique user ID and multifactor authentication are required for all Cohesity users.

For more information, see Cohesity product documentation.

# Security Management

Cohesity implements an Information Security Management System (ISMS) that establishes policies and controls designed to meet the security objectives of our organization. Our ISMS aligns with ISO 27001:2022, SOC2 Type II and the NIST CyberSecurity Framework to protect the organization, its personnel, and information assets.

- Policies are reviewed at least annually by the Information Security Committee and updated as appropriate.
- Annual update training is mandatory for all employees, which includes information security training.

New Cohesity employees are required to undergo background checks, sign a non-disclosure policy, and are required to review and acknowledge their receipt of relevant policies.

## Secure Software Development Life Cycle

Cohesity embeds security into every phase of the software development life cycle. Cohesity's secure development lifecycle delivers secure products (including all cloud-based images) to customers and eliminates any security vulnerabilities throughout the life cycle of the product.

For more details, please refer to both the Cohesity Trust site and Cohesity product documentation.

Cohesity Cloud Operations team sends Upgrade notifications ahead of time via the status.cohesity.com portal.

## Monitoring and Alerting

Cohesity provides one-stop-shop reporting on Data Cloud and implements continuous monitoring for both the security and availability of the service.

- Monitoring is considered a function of every service, with key performance indicators and metrics built in from the start.
- Dashboards and metrics are tracked by the monitoring and response teams.
- Alerts are designed in the development process. Alerts are reviewed by the cloud operations team and the development teams to ensure the thresholds are set and monitored while deploying to production.
- Aggregated view of your Cohesity deployment regardless of the use case, workload, or deployment type (on-premises, consumed as a Cohesity-hosted service, or a combination).

For more information, see Cohesity product documentation.

# Incident Response

Cohesity implements a security incident response program designed to detect, respond to, and recover from security incidents and events quickly and effectively.

- Security events and other IT-related problems are reported to the Information Security office. Issues are tracked and monitored until resolved.
- On-call response teams manage security and availability events through regularly tested response playbooks and procedures.

For more information, see Cohesity Support.

# Infrastructure Attack Defenses

Cohesity has several measures in place to address distributed denial of service (DDOS), intrusion, and malware attacks. These safeguards are built into the monitoring infrastructure that Cohesity has implemented to manage the Data Cloud environment. Firewalls monitor connections constantly and detect anomalies. As Cohesity identifies anomalies, the connection is blocked to evaluate the connection in the Data Cloud environment. Cohesity monitors the servers, containers, and infrastructure for vulnerabilities and addresses them regularly.

# Compliance and Certifications

As mentioned earlier, Cohesity takes the security of our customers' information very seriously. Cohesity recognizes the criticality of complying with standards and protecting the confidentiality, integrity, and availability of information assets. Cohesity maintains the following third-party assessments and assurances to validate the security posture of our products and services against industry standards.

- ISO 27001:2022.
- SOC 2 Type II.
- Cohesity holds a FIPS 140-2 Level 1 validation (AES 256-bit encryption).
- Cohesity performs regular penetration tests by qualified third-party assessors.

# Your Feedback

Was this document helpful? Send us your feedback!

# About the Authors

Karthick Radhakrishnan is Director, Technical Solution Engineering. In his role, Karthick focuses on managing Cohesity DataProtect and Security solutions.

Other major contributors included:

- Jason Hayes, Director of Information Security
- Ravishankar Murugan, Director of Cloud Operations
- Tim Robbins, General Counsel/VP of Legal
- Raj Dutt, Sr. Director, Product Marketing
- Luke Walker, Product Management

# Document Version History

| VERSION | DATE | DOCUMENT HISTORY |
|---|---|---|
| 1.0 | October 2025 | 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 42 of the Fortune 100.

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