COHESITY

Version 1.4

March 2024

Cohesity Data Cloud (SaaS) and Cloud Services Security Brief

Information Security Measures in Cohesity-managed Data Cloud Services

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 platform 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. Cohesity Cloud Services analyzes backup data, metadata, and system configurations to proactively assess IT needs and automatically manage infrastructure resources. Additionally, Data Cloud is capable of delivering capabilities through the Cohesity Marketplace. These include file auditing and compliance anti-virus defenses, and other services provided both by third-party partners and Cohesity.

The Cohesity Data Cloud SaaS platform consists of three fundamental components:

- **Management Service**. The Management Service, also known as Helios provides centralized management of the Data Service, whether it is customer-managed (data centers, edge, and public cloud) or Cohesity-managed. A Cohesity-supplied agent deployed in your Data Service infrastructure communicates with the Cohesity-hosted Data Cloud Management Service (hereafter referred to as "Management Service"). This enables Cohesity to retrieve telemetry information and lets you manage all your data sources centrally, from a single pane of glass. The Management Service is hosted on AWS and is developed and managed by Cohesity.
- **Data Service**. The Cohesity-managed Data Cloud Data Service (hereafter referred to as "Data Service") allows customers to store their data in Cohesity's cloud infrastructure, providing customers a data storage service without the infrastructure hassle. Alternatively, customers can choose to continue to store their data on customer-managed Data Service infrastructure that they manage and host themselves (e.g. on-premises or in your public/private cloud), and thus use only Management Services.
- **SaaS Connector**. A SaaS Connector is a compute instance running in a customer environment (on-premises or cloud) used for the Cohesity-managed Data Service, as illustrated in Figure 2 below. The Connector is deployed on a vCenter or ESXi host in a customer data center and establishes a secure channel for connecting on-premises data sources with Cohesity Data Cloud, thus enabling different use cases such as backup-as-a-service. Upon successful configuration, the SaaS connector is provisioned with TLS private keys and certificates, the private keys are always encrypted at rest and protected using Cohesity proprietary encryption techniques.

To register on-premises or cloud-based data sources with Cohesity DataProtect as a Service, you need to use a SaaS Connection to establish connectivity between your source and the service. A SaaS Connection consists of one or more SaaS Connectors, which are VMs that act as data movers between your data sources and Cohesity DataProtect as a Service.

To create a SaaS Connection, you deploy one or more SaaS Connector VMs depending on the data source that you want to protect. To learn how to deploy the SaaS Connector, see Cohesity product documentation.

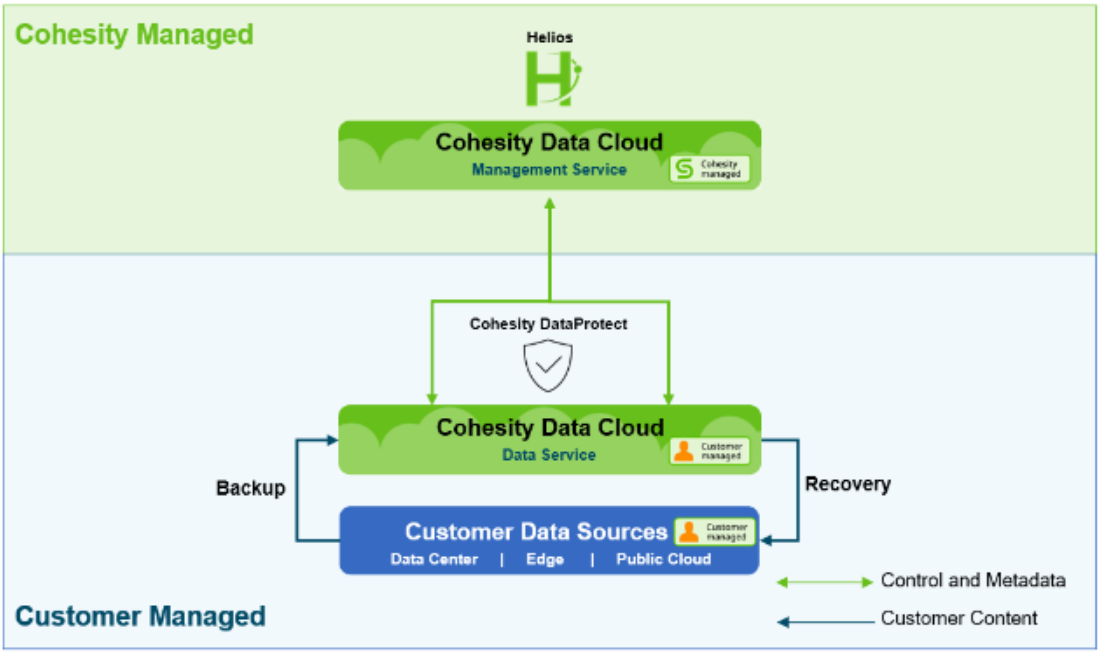
NOTE: You do not need a SaaS connector to use Management Service. A SaaS Connector is required only to use Data Service with sources in your data center.

NOTE: While the Management Service runs centrally in a single AWS region, the Data Service is available in multiple cloud regions.

The primary models to consume the value of the Cohesity-managed Data Cloud platform are:

- **Data Cloud for Customer-managed Infrastructure**. The customer uses Data Cloud to manage their Data Service infrastructure (across data centers, the edge, and the cloud), which they own, host, maintain, and operate themselves. In this model, the Management Service is managed by Cohesity, and the Data Service — on-prem Cohesity DataProtect — is managed by the customer.

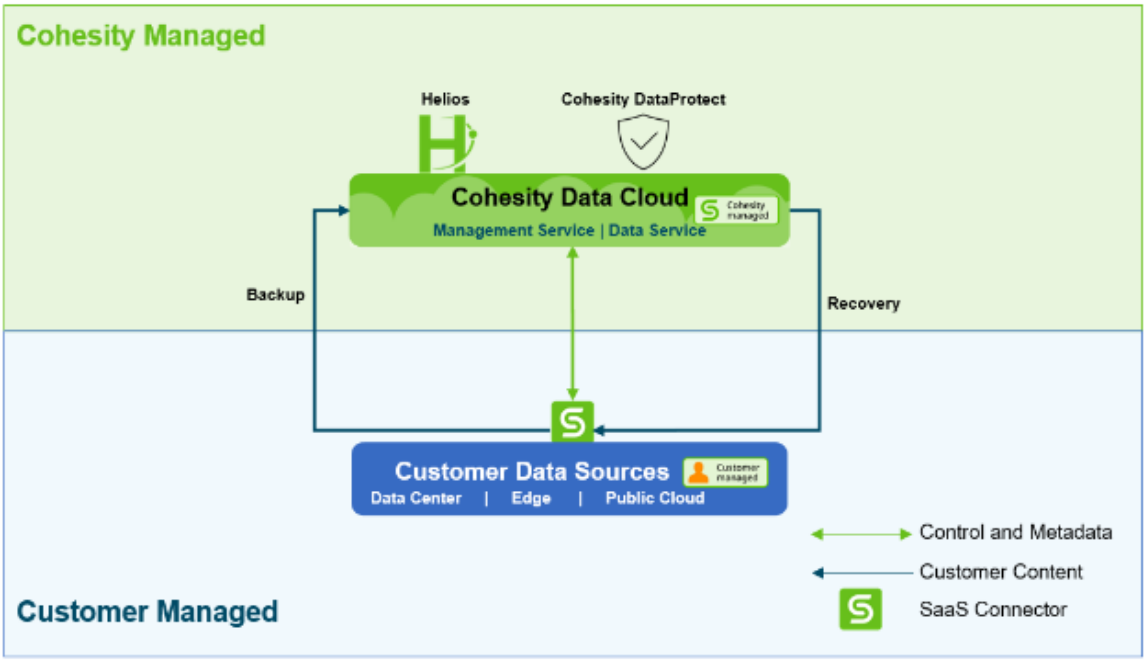
  Figure 1: Data Cloud for Customer-managed Infrastructure



- **Data Cloud for Cohesity-managed DataProtect as a Service**. In this software-as-a-service (SaaS) model, customers choose to store their data in the Cohesity-managed Data Service on AWS or Azure instead of hosting and operating their own Data Service infrastructure.

  For more details on supported workloads and cloud regions, See Cohesity product documentation.

Figure 2: Data Cloud for Cohesity-managed DataProtect as a Service

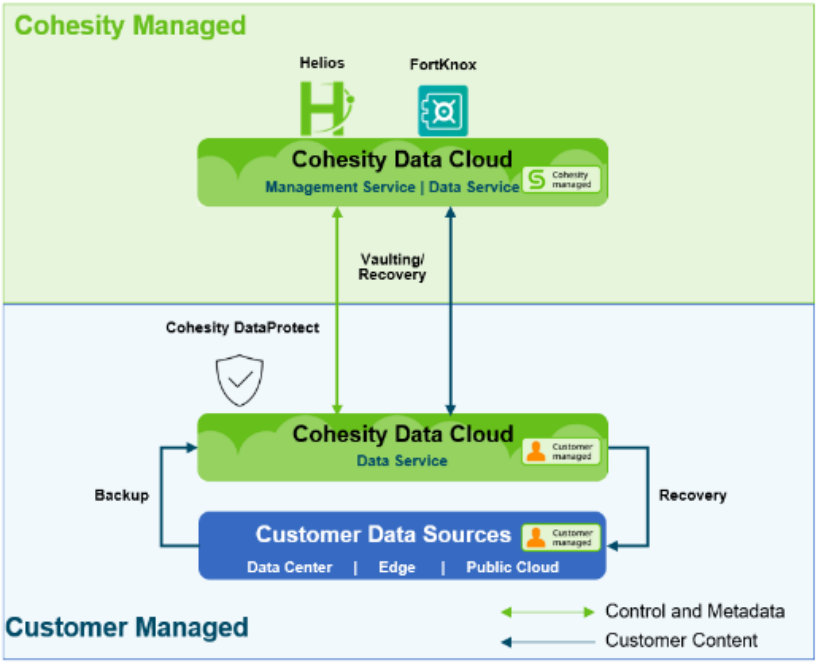


Cohesity FortKnox

Overview similar to DataHawk given below:

Cyber Vaulting and Recovery as a Service. In this software-as-a-service (SaaS) data isolation and recovery solution, customers choose to vault their data in the Cohesity-managed Cloud Vault instead of hosting and operating their own vaulting service infrastructure. A SaaS solution, Cohesity 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.

Figure 3: Data Cloud for Cohesity-managed Cyber Vaulting as a Service



In all three cases, you interact with Helios to configure the environment and set your data management policies. But as you might imagine, these three different models have implications on where data and metadata are stored and what data crosses traditional security parameters.

For more information, see Cohesity FortKnox.

Cohesity Data Hawk

To ensure the quality and security of organizational data, there is a need for robust data security and management solutions that span the breadth and depth of the data and enforce protection and security policies across this data footprint.

Cohesity **DataHawk** lends the capabilities that organizations require to secure data across on-prem data sources. DataHawk provides actionable insights that improve your cyber resiliency. DataHawk is an all-in-one solution that includes:

- **Cyber vaulting** - Cohesity FortKnox helps isolate away from cybercriminals and provides an off-site recovery copy.
- **Threat intelligence** - simplifies scanning for ransomware with 1-click scanning and automated threat feeds to stay up to date with the latest threats.
- **Data classification** - uses AI/ML to improve accuracy in finding sensitive data such as PII to help assess the impact of an attack and reduce time chasing false positives.
- **User behavior analysis** - provides log-based search and queries on user file activities that can cause signal tampering, exfiltration, or other risky behaviors.

For more information, see Cohesity DataHawk.

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 the 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). Cohesity Data Cloud Services comprising of FortKnox), DataHawk, and SiteContinuity are SaaS offerings, 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 and follows these best practices:

- 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.
- For customers who opt to use the Cohesity-managed Data Service, the management and data services are *delivered* together as a SaaS service but are *deployed* in unique public cloud (AWS, Azure) accounts to achieve segregation and secure access.

> **NOTE:** For information on securing the customer-managed Data Service, see the Cohesity Security Hardening Guide.

- For customers who opt to use the FortKnox Cohesity-managed data isolation and recovery service, the management and vaulting service are *delivered* together as a SaaS service but are *deployed* in unique public cloud (AWS, Azure) accounts to achieve segregation and secure access.
- Communication between the services running in public cloud accounts takes place through AWS/Azure private link, and all internal transport takes place through the AWS & Azure cloud back-end infrastructure.

Multi-Tenancy for Tenant Isolation

The Cohesity-managed Data Service is a highly scalable multi-tenant service wherein each tenant is implemented as an organization. Organizations are logically segregated via an *Organization ID* that uniquely associates all an organization's resources. Resources, such as users, data, policies, etc. are restricted to the Organization to which they belong.

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.

You can use Cohesity DataProtect as a Service to store your backups on the Cohesity-managed SaaS platform in Amazon Web Services (AWS) or Microsoft Azure.

For Amazon Web Services Cloud

Before you can register an AWS source, you'll need to configure your account's IAM role permissions for Cohesity DataProtect as a Service. To do so, you can execute **Cohesity's Cloud Formation Template** (CFT), a JSON file you can download from Cohesity DataProtect as a Service as you register.

When you execute the CFT, it creates an IAM role, and the policies based on the AWS services (EC2 instances and/or RDS databases) you select during AWS source registration. By default, the CFT-created role will be able to access all IAM roles and KMS keys in your account, but you can optionally restrict the permissions to specific IAM roles and KMS resources in the Parameters section when executing the CFT.

For more information, see Cohesity product documentation.

For Microsoft Azure Cloud

Before you register your Azure sources with Cohesity DataProtect as a Service, check the Azure requirements and then register Azure as a data source in Cohesity DataProtect as a Service.

For more information, see Cohesity product documentation.

Organization Access

Cohesity Data Cloud gives customers a broad set of controls to manage user accounts and their assigned access in accordance with strong security standards and their own security policy which includes RBAC, multifactor authentication, and Quorum policies.

RBAC

In every tenant Organization, an admin user manages the other users in that Organization. Organization admins can add and manage users through role-based access controls (RBAC). Applying principles of least privilege and separation of duties is simple with fine-grained control over standard and custom-defined roles.

Multifactor Authentication (MFA)

Multi-factor Authentication (MFA) provides a two-step verification method to authenticate and access Helios. Administrators can select one or both of the following authentication methods:

- **Authenticator App**: Cohesity recommends you install a Time-based One-Time Password (TOTP) authenticator app such as Okta Verify, Google Authenticator, Microsoft Authenticator, Duo Mobile, etc., on your device and enter the verification code generated by the app.
- **Email**: Users must enter the verification code sent to their email address.

Tenant admins can also integrate Cohesity Data Cloud with their existing Single Sign-On (SSO) Identity Provider using SAML or OpenID Connect. This enables each Organization to apply its specific controls for password policy, multi-factor authentication, and other controls through the upstream Identity Provider.

For more information, see Cohesity product documentation.

Firewall Profiles

Cohesity allows users to configure firewall profiles to restrict the incoming traffic on a Cohesity cloud service. Ensure that the ports listed in the Amazon Web Services (AWS) section in the Firewall Ports topic are open to allow communication between the Cohesity SaaS Connector(s) and Cloud environment.

For more information, see Cohesity product documentation.

Quorum

The tenant admin can further control the key operations via the Quorum approval process. FortKnox tightly integrates the quorum approval process into the recovery workflow where every recovery request to the original or an alternate location requires a Quorum group approval, thus safeguarding the vault data from unauthorized access or tampering.

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 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.

Secure Data Management

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.

In Cohesity's Data Cloud SaaS platform, the customer data and metadata are secured by different services based on the use case:

- **Data Cloud for Customer-managed Infrastructure.** When a customer uses the management Service, it collects the following metadata (and *only* the metadata):
  - For interactive management, information about:
    - Objects discovered from various registered sources, including External and Replication Targets.
    - License data on purchased SKUs.
    - Protection Group and Protection Run details.
    - Activity on the dashboard and by users and groups.
  - For advanced analytics, information about:
    - Alerts
    - Cluster config and status
    - Firmware information
    - A time capsule of the various cluster services
    - Audit logs
    - Statistics on capacity, performance, and more
    - Cohesity Platform system settings
    - Rest API outputs
    - Debug logs
    - Linux command outputs

  > **IMPORTANT**: The Management Service does *not* collect customer data from the data sources that the customer manages.

- **Data Cloud for Cohesity-managed Data Service**. When a customer signs up to use Cohesity DataProtect delivered as a service, Data Cloud backs up customer data from both on-premises and cloud-based sources to a Cohesity-managed cloud. Therefore, it collects both customer data *and* the metadata related to that data.
- **Data Cloud for Cohesity-managed Cyber Vaulting and Recovery Service (FortKnox)**. When a customer signs up to use Cohesity FortKnox, you get the management interface to vault your backed-up data to the Cohesity-managed immutable cloud vaults. A cloud vault is a destination where you can backup your Cohesity cluster data and retrieve it to the original or a new location. Once it is created, the data from the cluster is sent to the cloud vault.

  For more information, see Create Cloud Vault. Data Cloud coordinates the access to the cloud vault to minimize security exposure. It also ensures that any request to access cloud vault is from an

authorized Cohesity on-prem cluster and in non-violating user-defined vault specific vaulting window. Further, Data Cloud grants restricted privileges to the Cohesity cluster to be able to access Cloud Vault via short-lived-token-based authenticated APIs to prevent exfiltration attacks. It just collects metadata similar to **Data Cloud for Customer-managed Infrastructure.** For more details, see Cohesity product documentation.

Cohesity FortKnox allows you to recover workloads such as virtual machines and databases.For more information on workflows that are supported for each workload, see Supported Workflows.

Data Isolation

For the Management Service, each tenant Organization's data and metadata are logically segregated and isolated from the other tenant Organizations.

For the *Cohesity-managed Data Service*, unique AWS S3 buckets/Azure blob storage are allocated to each tenant Organization, ensuring that customer content is never shared or accessed across Organizations.

For FortKnox Cohesity-managed Data Isolation and Recovery Service, unique AWS S3 buckets/Azure blob storage are allocated to each customer, ensuring that customer content is never shared or accessed across different customers.

NOTE: Multi-tenancy is not supported with FortKnox.

Data-at-Rest Encryption

All customer data (whether it is metadata for the Management Service or metadata and data in the Data Service) is encrypted at rest using AES-256-GCM, and the encryption keys are managed in a key management system (KMS).

While the Management Service relies on AWS KMS for key management, the Data Service has two secure options for managing encryption keys:

- A built-in Cohesity-managed KMS.
- Customer-managed keys via AWS KMS.

For more information, see Cohesity product documentation.

Data Resiliency and Availability

In addition to offering customers centralized control of their self-managed Cohesity Data Service infrastructure, the Management Service orchestrates the deployment and management of the Cohesity-managed Data Service. Management Service is built on the Cohesity Data Cloud platform, which maintains an availability of 99.9% ('*three 9's*').

Amazon Web Services Cloud

In the Cohesity-managed Data Service, the data is stored in customer-unique S3 buckets in a customer-defined region. Data Service compute nodes are stateless with data stored in S3 (with '*eleven 9's* of durability'). AWS stores multiple copies of data for S3, making it a highly reliable storage service. For S3, the objects are automatically stored across multiple devices spanning a minimum of three Availability Zones, each separated by miles across an AWS Region. For more details, see Amazon S3 FAQs.

Each data plane region (aka provisioned region) creates a dedicated and secure tenant on the data plane cluster. The S3 bucket assigned to the tenant for that region can be observed in the "information" display for each listed Region in the CCS portal for a specific customer tenant. As customers do not manage the data plane clusters, they cannot see the external target configurations for the S3 buckets, however, each tenant does operate in a dedicated Storage Domain/Cloud Storage Domain which can only be strictly assigned to a single customer/tenant at a time in the Cohesity architecture. The Cloud Storage Domain is backed by a dedicated S3 bucket (external target) on the data plane cluster - all this is managed and secured by Cohesity Cloud Operations.

NOTE: If the SaaS connector loses direct connectivity to the S3 bucket in the CCS data plane, the SaaS connector will enter an unhealthy state and backup/recovery will error on the SaaS connector. The SaaS connector will constantly attempt to reconnect to the S3 bucket and data plane cluster to resolve the connectivity issue.

For Cohesity-managed Data Service, in the event of a disaster scenario, the Management Service can recreate the Data Service using the data in the S3 storage. The Data Service is deployed in a virtual private cloud (VPC) within private subnets. No public IP address is exposed on the Data Service. All communication between the Data Service and the SaaS Connectors it uses to connect to data center sources is secured through certificate authentication and is mediated by the front-end load balancer.

The FortKnox Cohesity-managed Cyber Vaulting and Recovery Service is built on the Cohesity Data Cloud platform, it maintains an availability of 99.9% ('*three 9's*'). In FortKnox, data is stored in a Cohesity-managed WORM (write-once-read-many) AWS S3 bucket created in a customer-defined region. AWS stores multiple copies of data for S3, making it a highly reliable storage service. For S3, the objects are automatically stored across multiple devices spanning a minimum of three Availability Zones, each separated by miles across an AWS Region. For more details, see Amazon S3 FAQs. All communications between the Cohesity cluster and Cloud Vault are secured by an encryption key management system coordinated by Data Cloud.

NOTE: The Data Service does not replicate the tenant backup data to a different region as a native part of the service offering. This is because AWS S3 is already highly available storage with high resilience. However, if you still prefer to replicate your backups from the Data Service, contact your Cohesity representative to discuss replication strategies.

Microsoft Azure Cloud

In the Cohesity-managed Data Service, the data is stored in customer-unique Azure Blob storage in a customer-defined region. Data Service compute nodes are stateless with data stored in Azure blob (with '*twelve 9's* of durability'). For Azure blob storage, the objects are automatically stored across multiple devices spanning a minimum of three Availability Zones, each separated by miles across an Azure Region. For more details, see Azure blob Storage FAQs.

Each data plane region (aka provisioned region) creates a dedicated and secure tenant on the data plane cluster. The Azure blob assigned to the tenant for that region can be observed in the "information" display for each listed Region in the CCS portal for a specific customer tenant. As customers do not manage the data plane clusters, they cannot see the external target configurations for the Azure blob, however, each tenant does operate in a dedicated Storage Domain/Cloud Storage Domain which can only be strictly assigned to a single customer/tenant at a time in the Cohesity architecture. The Cloud Storage Domain is backed by a dedicated Azure blob storage (external target) on the data plane cluster - all this is managed and secured by Cohesity Cloud Operations.

Secure Communication

Cohesity Data Cloud secures data in transit through secure, modern encryption protocols Transport layer security (TLS 1.3/TLS1.2) and Mutual Transport Layer Security (mTLS) with only FIPS-approved cipher suites protection throughout the Cohesity Cloud Service, employing these methods:

- Cohesity Agent (on clusters) to Data Cloud Management Service: Mutual Transport Layer Security (mTLS)
- SaaS Connector to Data Cloud Management Service: https
- SaaS Connector to Data Cloud Data Service in the selected region: mTLS
- Data Cloud Data Service to Data Cloud Management Service: mTLS (over a private link on the AWS & Azure backbone)
- DMZ to Data Cloud Management Service: mTLS (over a private link on the AWS & Azure backbone)
- Communication between Data Cloud Service to the cloud storage: mTLS (over a private link on the AWS & Azure backbone)
- Inter-service communication in Data Cloud Management Service: https
- Cohesity cluster to Data Cloud Management Service: mTLS
- Cohesity cluster to Cloud Vault: HTTPS using short lived tokens (Writes only during vaulting window)

Inter-microservice communication in the 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 the Cloud Vault.

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 align with ISO 27001:2022 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 information security training is required for all employees.

Background checks are performed on new Cohesity employees, who are also 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.

SaaS connectors are upgraded as a part of the service upgrade and the 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.

Manage the Support Channel

The Cohesity Support Channel is a secure, simple, and effective way for Cohesity employees to provide on-demand assistance to customers. Cohesity recommends that you enable the Support Channel for SaaS Connector when you need assistance from Cohesity employees.

For more information, see Cohesity product documentation.

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. If Cohesity DataProtect as a Service detects an anomaly during a protection run of your data, it triggers the critical alert, **DataIngestAnomalyAlert.** Using the alert information, you can investigate the anomaly and decide on the next course of action.

For more information, see Cohesity product documentation.

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.

Sagar Sethi is a Staff Technical Solution Engineer at Cohesity. In his role, he focuses on various aspects of Data Security to secure Cohesity product design & 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
- Subash Babu, Staff Technology Editor
- Luke Walker, Product Management

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.4	Mar 2024	Security assessment updates
1.3	July 2023	• Branding Updates • Minor Technical Updates
1.2	May 2022	FortKnox updates
1.1	May 2021	Minor updates
1.0	Nov 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 42 of the Fortune 100.

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