COHESITY

Cohesity FortKnox Cloud Service Security Brief

Information Security Measures in Cohesity-managed Cyber Vaulting and Recovery SaaS Offering

Version 1.2

September 2025

ABSTRACT

Cohesity FortKnox Cloud Service is designed, developed, and operated with security as a core tenet. This Security Brief gives you an overview of the information security measures in FortKnox.

.

Table of Contents

Figures

About Cohesity Cloud Services

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

We designed Cohesity Cloud Services, a modern data platform designed for today's multi-cloud environments, to provide enterprise-ready data management capabilities such as backup and recovery, cyber vaulting, threat intelligence, data classification, disaster recovery, and more, wherever you need them.

Cohesity's cloud service management platform Helios provides you with a single administrative 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.

Simplify your data security and management with Cohesity's SaaS offerings, which includes:

- **DataProtect Delivered as a Service**: Protect your critical SaaS, cloud-native, and on-premises data sources with Backup as a Service SaaS offering.
- **FortKnox** is a SaaS offering which vaults backed up data to the cloud. It sends a replica of the Cohesity backup data to an AWS-hosted storage target that has physical separation, network, and operational isolation from both the production and backup environments.
- **DataHawk** is a data governance and security service SaaS offering. It helps you protect your critical data against ransomware with threat intelligence and scanning and ML-powered data classification.
- **Site Continuity** helps enterprises automate their disaster recovery failover/failback orchestration. Customers can self-manage their DR or leverage Cohesity-managed disaster recovery as a service (DRaaS), all through a single, global UI.

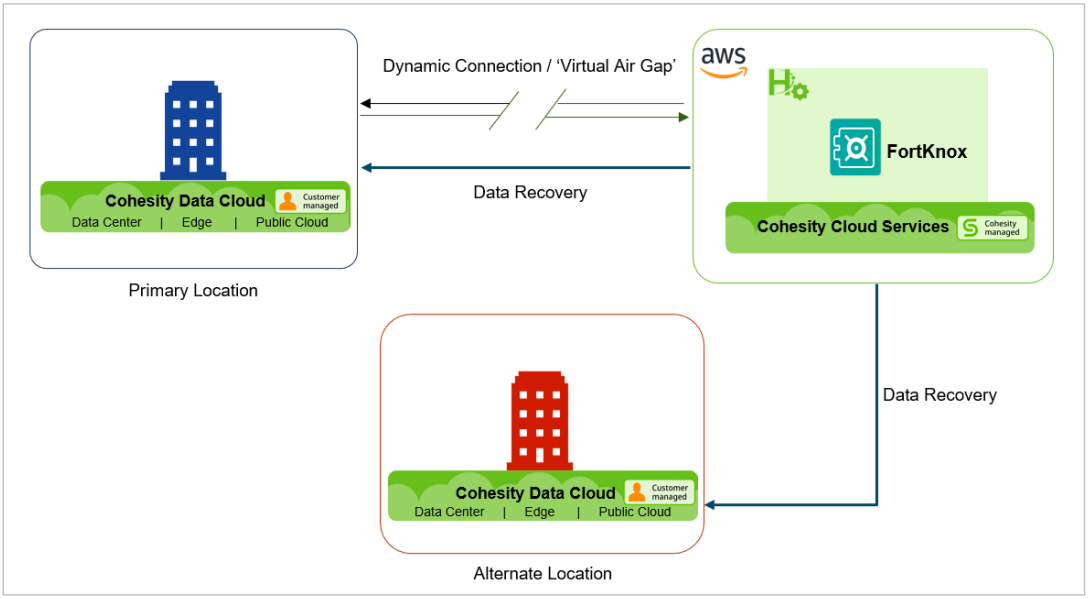
Let's get into more details on Cohesity cyber vaulting and recovery SaaS offering FortKnox.

Cohesity FortKnox

Cohesity FortKnox is **Cyber Vaulting and Recovery as a Service,** a Cohesity Cloud Services' offering to create a copy of your backup data in the Cohesity-managed cloud vault. FortKnox aims to secure and isolate the critical data from both the production and primary backup environment for improved security against ransomware attacks. FortKnox makes the customers confident about their data security in the cloud in case of ransomware attacks or other risks.

In case of a ransomware attack, customers have the option of recovering their vaulted data either using their original self-managed Cohesity cluster or, if the primary site is fully compromised by the attack and the original cluster is not accessible, by initiating recovery from a new cluster located at an alternate site.

Figure 1: Cohesity FortKnox

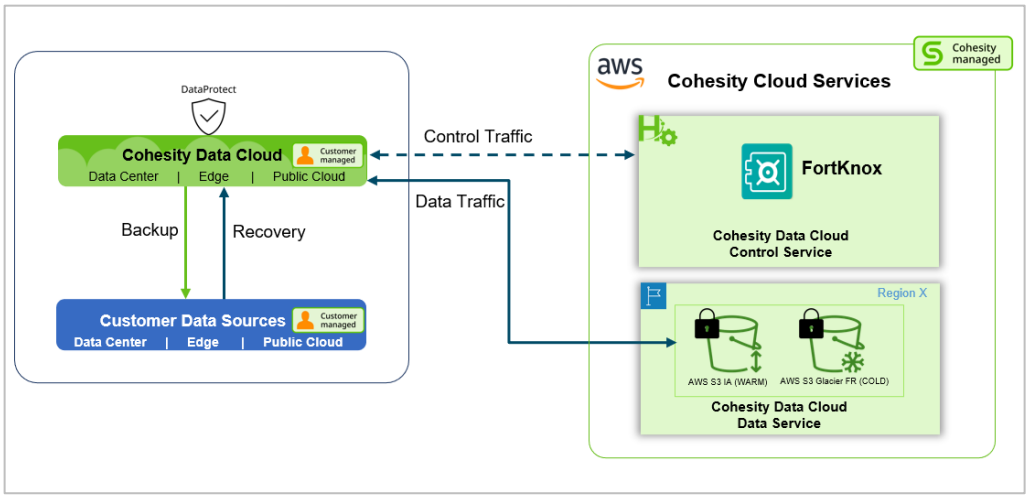


FortKnox consists of two fundamental components:

- **Cohesity Cluster**: Customer's primary workload protected using Cohesity's DataProtect offering to Cohesity cluster deployed physically at datacenter, as a virtual edition or in the cloud.
- **Cohesity's Cloud Service**: This comprises two smaller services:
  - **Data Cloud Control Service**: The Control service is a vital component in securing access to the cloud vault, specifically helpful in eliminating potential unauthorized access to data sitting in the cloud vault. The Control service enforces a set of security measures to ensure that requests to access the data in the cloud vault are only made by authorized Cohesity clusters during vault availability hours.
  - **Data Cloud Data Service:** The Cohesity-managed Data Service allows customers to vault their data in Cohesity's cloud infrastructure hosted on AWS, which provides customers a data storage service without any infrastructure hassles.

NOTE: Cohesity's Cloud Service FortKnox is available in multiple AWS regions.

Figure 2: FortKnox - Fundamental Components



Secure Platform Architecture and Deployment

We take the security of our customers' information very seriously. Cohesity FortKnox is designed, developed, and operated with security as the core tenet guiding our approach. What's more, the FortKnox architecture is simple and modular, enabling a scalable solution that remains secure, available, and flexible. We implement security controls with a defense-in-depth approach across each module, while the communication between modules is secured across the FortKnox Cloud Service.

Multi-Tenancy for Tenant Isolation

To manage multiple customers' data in FortKnox, the service is designed as a highly scalable multi-tenant service wherein each tenant (Customer Helios Account) is logically isolated from other tenants, via the implementation of Cohesity *Organization in Data Cloud Data Service* hosted on Cohesity-managed cloud accounts. Cohesity organizations are logically segregated via an *Organization ID* that uniquely identifies all of the Tenant's resources. Resources, such as cloud vaults, data, policies, users, etc. are restricted to the Organization to which they belong.

Tenant Data and Network Segregation

Cohesity assigns each FortKnox customer their own dedicated AWS S3 buckets, and it employs AWS IAM roles and policies to ensure that customer content is not shared or accessed across different customers.

FortKnox can also leverage AWS PrivateLink capabilities to provide private connectivity between virtual private clouds (VPCs), AWS services, and on-premises networks, without exposing network traffic to the public internet. Using AWS PrivateLink, the on-premises Cohesity cluster can communicate privately with FortKnox cloud vault for storing and retrieving vaulted data.

Data Isolation

With FortKnox, you can create an immutable and isolated copy of your data in the Cohesity-managed cloud vault, which is hosted in unique AWS S3 storage buckets allocated to each customer. Since the vaulted data is not being hosted in the same environment as your production or primary backup copy of data, your offsite data copy is virtually air-gapped. Moreover, as the customer does not need to use their own AWS login, the vault is isolated from their own AWS instance, which adds to an improved security posture.

Logical Data Network Separation

FortKnox implements logical network separation with the concept of vaulting window. Cohesity cloud vault is available for writes only during the defined vaulting window. The vaulting window is static, and customers get the flexibility to configure the vaulting window as per their business needs. This provides logical network separation to the cloud vault along with greater control to the customer over vault availability. When the vaulting window is not active, the Helios control service will not issue the necessary temporary credentials required by the Cohesity cluster for accessing the cloud vault, resulting in denied access to the vault.

Data Immutability

Cohesity cloud vault, by design, incorporates DataLock, a feature that enables the implementation of Write Once Read Many (WORM) functionality through the utilization of the AWS Object Lock feature. This integration allows for the application of immutability to the data stored within the cloud vault, designed to ensure that once data is written, it cannot be modified. The WORM capability serves as a key component of the overall data protection strategy of Cohesity cloud vault, providing an additional layer of security and compliance to the data stored within FortKnox.

AWS Object Lock offers two distinct modes of operation: Compliance Mode and Governance Mode. Compliance Mode is a more restrictive mode that prohibits any tampering by administrators, while Governance Mode allows for administrative adjustments to retention holds. In the context of Cohesity FortKnox, the Governance Mode lock is applied to the data stored within FortKnox.

NOTE: FortKnox is not available for Cohesity's service-providers (Multi-tenancy) deployments.

Secure Data Management

In a data vaulting solution, managing the security of the data and metadata, irrespective of whether it is in-transit or at-rest, is critical. In FortKnox, security is central in every phase of data management.

Encryption

With FortKnox, all customer data (metadata or data) is encrypted in-transit and at-rest using AES-256, and the encryption keys are managed in a key management system (KMS).

FortKnox has two secure options for managing encryption keys:

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

Encrypted KMS key is stored in the cloud vault along with data.

Secure Access to Cloud Vault

Cohesity cloud vault is designed with robust security measures to restrict access to the vaulted data at various levels. This includes both read and write access to the vault, which is restricted at the authentication layer.

Cohesity cluster gains access to the cloud vault by authenticating through the Control Service. Only the Cohesity cluster can initiate the process of vaulting data (Data Write) or recovering it (Data Read) from the cloud vault.

To read from or write to the Cloud Vault, the Cohesity cluster must first authenticate itself to the Control Service to obtain temporary security credentials. This ensures that any request to access the Cloud vault is authorized by the control service. The Cloud Service ensures that for write operations these temporary security credentials are granted within a defined vaulting window.

Cloud Service ensures that temporary security credentials are granted for write operation only during the defined vaulting window. This ensures that any request to access the Cloud Vault is authorized by the control service.

To prevent exfiltration attacks, the Control Service grants the Cohesity cluster restricted privileges to access the Cloud vault via short-lived, token-based authenticated APIs. For example, when recovering data, the Cohesity cluster is given only read access to the requested cloud vault data.

Direct access to the cloud vault outside the Cohesity managed environment is not permitted. As discussed in the previous section, only authorized Cohesity clusters are permitted to initiate read or write operations to the Cohesity cloud vault. There is no direct access provided to the customer or customer managed Cohesity cluster to the data residing in the cloud vault.

This means that any request outside the Cohesity managed environment to the control service, or outside authorized Cohesity cluster attempting to perform operations such as read, write, delete, or modify on the cloud vault (for instance: using AWS API calls), will be denied. Such access requests to the cloud vault must go through the authorization process via the Cohesity-managed control service. This is designed to prevent malicious actors or malware from accessing the data stored in the vault.

Data Resiliency and Availability

The FortKnox Cohesity-managed Cyber Vaulting and Recovery Service is built on the Cohesity Cloud Services Platform, which maintains an availability of 99.9% (‘*three 9s*’). 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 the Amazon S3 FAQs. All communications between the Cohesity cluster and cloud vault are secured by an encryption key management system coordinated by the control service.

NOTE: FortKnox Data Service does not replicate the tenant-vaulted data to a different region as a native part of the service offering. This is because AWS S3 is already a highly available storage with high resilience.

Secure Communication

Cohesity Cloud Services Platform secures data in transit through secure, modern encryption throughout the service, employing these methods:

- Cohesity cluster to Helios Management Service: Mutual Transport Layer Security (mTLS)
- Cohesity cluster to cloud vault: HTTPS using short-lived tokens (Writes only during the vaulting window)
- DMZ to Helios Management Service: mTLS (over a PrivateLink on the AWS backbone)
- Communication inside FortKnox Data Service: AWS Security Groups
- Inter-service communication in Helios Management Service: https

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.

Identity and Access Management (IAM)

Identity and access management is a critical security aspect for any service. Cohesity Cloud Services implements strong IAM controls to manage access, authentication & 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.

The two main types of users who access FortKnox service are:

- Organization (tenant) users
- Cohesity internal users (for managing and maintaining the service)

Organization Access

Cohesity FortKnox 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 (MFA), 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)

Tenant admins can also integrate Cohesity Helios with their existing SAML-based Single Sign-on (SSO). This enables each Organization to apply its specific controls for password policy, MFA, and other controls.

Quorum

The tenant admin can further control the Helios 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 read access.

Cohesity Access

Cohesity uses strict controls for internal access. Only the CloudOps team, which manages FortKnox's cloud infrastructure, is permitted access. Access follows least-privilege and separation-of-duties principles, with strong authorization requirements. When CloudOps requires access, it is **read-only** and requires unique user IDs, multifactor authentication, and quorum approval. For Cohesity-managed KMS keys, even the CloudOps super admin must go through quorum approval.
Importantly, having super admin access plus KMS and cloud infrastructure access is still not sufficient to restore data. The data is encrypted and stored in a proprietary Cohesity format.

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 and the NIST CyberSecurity Framework to protect the organization, its personnel, and information assets.

- Policies are reviewed at least on an annual basis 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 to customers and eliminates any security vulnerabilities throughout the life cycle of the product. To deliver on this goal, Cohesity practices:

- Security Training
- Security in Design
- Threat Model in Architecture
- Vulnerability Management
  - Vulnerability Management Policy
  - Penetration Testing
  - Static Code and Binary Analysis
  - Dynamic Scanning
  - Third-party Component Security
  - Support for Product Infrastructure and Tools
- Secure Product Release
- Product Incident Response

Monitoring and Alerting

Helios 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.

Incident Response

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

- 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.

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 we have implemented to manage the Helios environment. Firewalls monitor connections constantly and detect anomalies. As Cohesity identifies anomalies, the connection is blocked to evaluate the connection in the Helios environment. Cohesity monitors the servers, containers, and infrastructure for vulnerabilities and addresses them on a regular basis.

Compliance and Certifications

As mentioned earlier, Cohesity takes the security of our customers' information very seriously. We recognize the criticality of complying with standards and protecting 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.

- SOC 2 Type II
- Cohesity performs regular penetration tests by qualified third-party assessors.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

- Dayanand Sharma, Director of Product Management
- Dan Van Dyck, Staff 2 Software Engineer
- Patrick Ryan, VP of Assistant General Counsel
- Renee Jacowitz, Director of Legal-Technology Interlock
- Pamela Flemming, Directory of Information Security GRC
- Luke Walker, Lead Product Manager
- Subash Babu, Sr. Technology Editor

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.2	Sep 2025	Updated the “Cohesity Access” section.
1.1	July 2024	Republishing
1.0	Mar 2023	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.