COHESITY

Leading the next era of data security and management

At a Glance

Founded: 2013

CEO & President: Sanjay Poonen

Founder & CTPO: Mohit Aron

HQ: San Jose, California

Key funding partners:
Sequoia Capital, AWS, DFJ Growth Fund, Cisco Investments, HPE, Google Ventures and SoftBank

Representative Directors & Advisors:

- Guarav Garg,
  Founding Partner of Wing Ventures
- Kevin Mandia,
  CEO of Mandiant
- Jonathan Chadwick,
  former VMware CFO
- Bill Coughran,
  former Google SVP Research, Sequoia Capital
- Carl Eschenbach,
  former VMware President & COO, Sequoia Capital
- Robin Matlock,
  former VMware CMO
- Janesh Moorjani,
  CFO at Elastic
- Vikas J. Parekh,
  Managing Partner at SoftBank Vision Fund

Cohesity Security Council:

- Kevin Mandia,
  CEO of Mandiant
- Kelly Bissell,
  CVP Microsoft Security Services
- Laura Barrowman,
  CIO, Credit Suisse
- Alex Stamos, *Former CSO, Facebook and Yahoo*
- Jason Chan, *Former VP Info Security, Netflix*
- Marianne Bailey, *Former NSA Exec and DOD CIO/CISO*
- Sheila Jordan, *Chief Digital Technology Officer, Honeywell*

Solving today's data challenges

Your data is a uniquely valuable resource, but ensuring your business can use it to best advantage has become too complex and risky. Ransomware attacks a business nearly every second of every day. And fragmented, single-purpose tools - even newer SaaS-based versions - are increasing the attack surface as well as cost and complexity. They treat data security and management as separate worlds. Cohesity is different.

Cohesity has adapted the software design principles of cloud hyperscalers - such as Google and AWS that manage the world's consumer data - and is bringing scale, simplicity, and security to enterprise-class data security and management. The result is the Cohesity Data Cloud.

Comprehensive multicloud solution

The Cohesity Data Cloud offers five key capabilities that work individually or together in a single, easy to manage environment that spans across the multicloud:

Data protection

Ensure your data is immutably preserved, and instantly available in the event of a ransomware attack.

Data access

Eliminate wasteful copies, and manage files and objects efficiently at scale

Data security

Increase resilience to cyber threats through cyber vaulting, threat intelligence and scanning, data classification, and two-way integration with your Security Operations Center.

Data insight

Search, classify and analyze data globally across your entire estate to provide business value, or identify sensitive data for compliance.

Data mobility

Safely and efficiently move data anywhere across a hybrid multicloud landscape to reduce cost and increase flexibility.

Market leadership

3X Leader in Magic Quadrant for Enterprise Backup and Recovery Software Solutions

First Time Out Visionary in Magic Quadrant for Distributed File Systems and Object Storage

4X Named to Forbes Cloud 100

Leaders in GigaOm Radar for Hybrid Cloud Protection, Unstructured Data Management and Enterprise Scale-Out File Systems

4X Data Center Backup and Recovery Solutions

2X Distributed File Systems and Object Storage

6X Winners Northface Customer Service Awards

85+ average NPS score

Customers

Why Cohesity?

Simplicity at scale

Our hyperscaler design supports multiple use cases that previously required separate solutions, enabling you to collapse silos, reduce complexity and cost, and control everything from a single UI.

Zero Trust Security

Our platform is built on the principles of least privilege and segregation of duties, and integrates with your existing security operations to provide a holistic approach to data protection and resilience.

Powered by AI insights

Built-in intelligence enables IT to accomplish more with their existing resources, improve efficiency, and avoid issues before they become serious by proactively monitoring and predicting behavior.

Third-party extensibility

Our API-first design allows developers and third parties to add value to your data through apps and services that can uniquely run in the same environment as the managed data rather than in a separate system.

Satisfied customers

We have enjoyed a high (85+) Net Promoter Score – a rare achievement that must be continuously earned and requires us to maintain the highest standards of customer obsession.

Our customers also enjoy complete flexibility in how they manage and license the Cohesity solution: a SaaS service managed by Cohesity, self-managed with a software subscription, or partner-managed through a service provider — or any combination.

Learn more at www.cohesity.com

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, DataHawk, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

*Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solutions, Michael Hoeck, Nik Simpson, Jerry Rozeman, Jason Donham, 28 July 2022. *Magic Quadrant for Distributed File Systems and Object Storage, Julia Palmer, Jerry Rozeman, Chandra Mukhyala, Jeff Vogel, 19 Oct 2022.*

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Cohesity.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

*The GARTNER PEER INSIGHTS Logo is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences and do not represent the views of Gartner and its affiliates.

*"Radar for Hybrid Cloud Data Protection for the Enterprise", Enrico Signoretti, Arjan Timmerman. GigaOm, June 14, 2021.

Defend Against Ransomware and Insider Threats With Data Isolation

Key Benefits

- Strengthen data security strategy
- Keep data safe from both cyber and internal threats
- Meet SLAs and reduce business risk
- Reduce downtime with instant recovery at scale

Enterprises will experience a ransomware attack every two seconds by 2031, according to a recent Cybersecurity Ventures survey, for more than $265 billion in cost damages. Concurrently, more than 34% of businesses globally will face an insider attack, an increase of 47% in the past two years, reports Tech Jury. The growing number and severity of cyberattacks and insider threats have organizations looking to fortify their IT systems and data, many following the NIST Cybersecurity Framework guidance to adopt a multi-layered defense strategy.

Organizations investing in Cohesity next-gen data management have a head start. Cohesity is purpose-built with defense-in-depth capabilities that include:

- **Immutable snapshots** – A gold copy of backup data never exposed nor mounted externally
- **DataLock** - A time-bound, WORM lock on the backup snapshot that can't be modified
- **Encryption** – Data encrypted at-rest and in-flight
- **Role-based access control (RBAC)** – Granular admin and user access can be implemented on least privilege and need to know principles
- **No back door** – Support account enablement by authorized customer users only
- **Secure SSH access** – A secure access path over an unsecured network
- **Data isolation** – Isolation of data to keep it safe from cyber and internal threats

Data isolation is not a replacement for existing backup and recovery or disaster recovery (DR) solutions, but rather a way of providing an extra layer of protection. The purpose: to strengthen the overall data security strategy.

Modern Data Isolation With Cohesity

As defined by NIST, air gapping requires organizations to keep at least one copy of their data physically and electronically isolated for extra security. While highly secure, this approach does not support the RTO and RPO goals of modern organizations. As a result, data isolation has emerged as an alternative to better support modern RTO and RPO requirements; backup data is stored in the cloud or another location with a temporary and highly secure connection. This provides a tamper-resistant environment protecting against ransomware and insider threats and supporting the organization's SLAs.

With Cohesity, enterprises never compromise SLAs or risk tolerance and have maximum choice and flexibility in isolating and protecting their organizations' data from bad actors. Cohesity supports flexible deployment with isolation to:

- **Cohesity FortKnox** – A SaaS data isolation and recovery solution that improves cyber resiliency with an immutable copy of data in a Cohesity-managed cloud vault via a virtual air-gap. The solutionprovides ransomware detection, quorum and zero-trust features to keep your data safe. Coupled with physical separation, network and management isolation, FortKnox provides the ultimate in protection and ease-of-use needed against ransomware and other cybersecurity threats.
- **Remote Cohesity cluster** – Customers can replicate from one immutable Cohesity cluster to another remote cluster, running either on premises or as virtual clusters in a public cloud. Compared to the legacy data isolation approach that requires shipping tapes off-site, this data isolation method lowers RTOs and RPOs as data on the remote cluster is readily available.
- **NAS target** – Cohesity archives data to a NAS external storage target that supports WORM for isolating data with lower RTOs and RPOs.
- **Cloud** – To take advantage of the public cloud's scale and elasticity, organizations have been leveraging cloud as one of the modern ways to achieve data isolation. Cohesity supports archiving to the cloud to achieve data isolation, and immutability, lower RTOs and RPOs, and lower TCO.
- **Tape (air gap)** – Cohesity enables the archiving of data to tape from backup so IT can send the tapes to off-site storage, ensuring access only through physical engagement.

Optimal Risk-SLA Rewards With Isolation to a Cohesity Cluster

Cohesity customers not only gain data resilience but meet demanding business SLAs while lowering risk by replicating their backup data to a remote Cohesity cluster. In alignment with the NIST Cybersecurity Framework's defense-in-depth model, Cohesity empowers teams to replicate data to another immutable Cohesity cluster at an isolated site which provides modern data vaulting, residing on an isolated network and supporting WORM.

Figure 1 shows the flexibility in Fort Knox deployment, with the ability to restore to multiple destinations for disaster recovery. Only the enterprise administrator opens and closes the necessary ports only during data transfer to keep data secure.

By replicating to an isolated Cohesity cluster, organizations modernize their data centers and achieve stronger cyber defense, faster recoveries—with instant recovery at scale—and shorter RTOs/RPOs while reducing network bandwidth requirements. Defend your business against increasing ransomware and insider threats by fortifying your IT systems with air-gap protection from Cohesity.

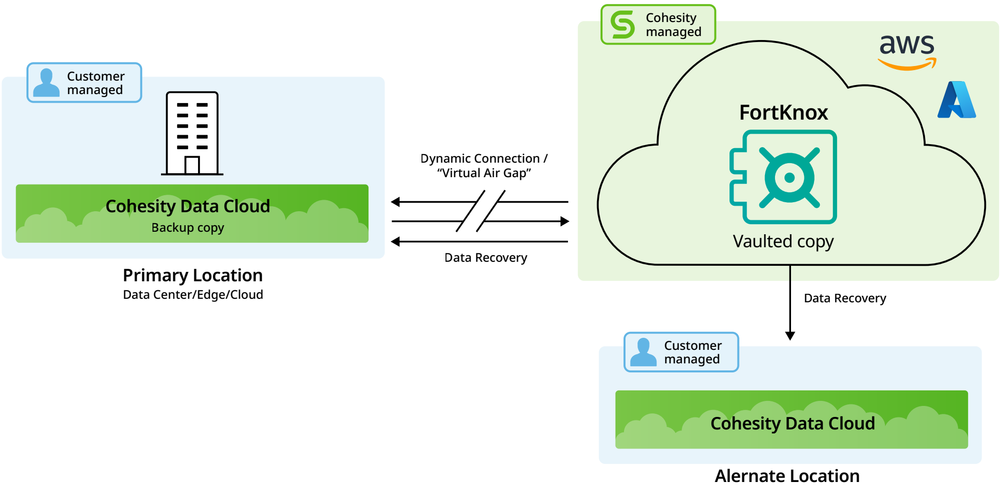


Figure 1: Cohesity FortKnox boosts cyber resilience with data recovery back to the source or to an alternate location.

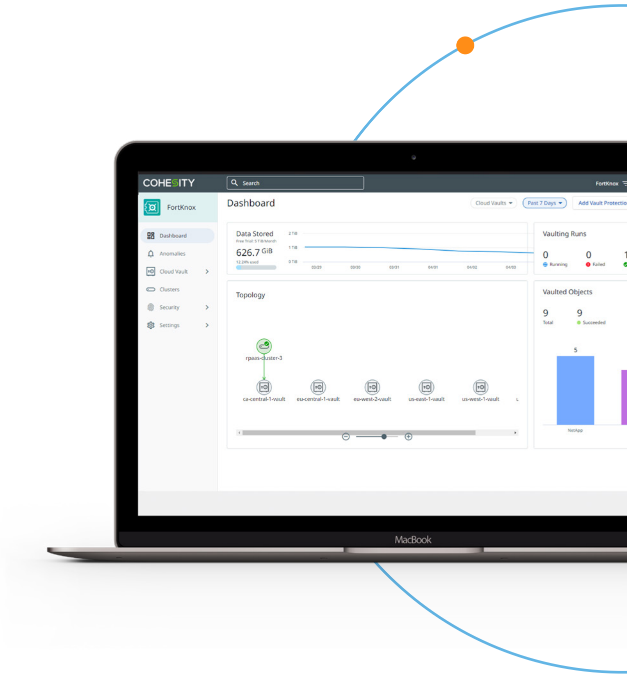
Learn more at www.cohesity.com

COHESITY

Cohesity FortKnox

Data Isolation and Recovery 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. This reality has forced organizations to rethink their approaches to the 3-2-1 strategy of backing up data—three copies of data, on two different media, with one of them in an off-site environment. Although a traditional air gap model where data is stored on magnetic tapes and moved off-site for data isolation ensures data security in the face of increasing ransomware attacks, it impedes rapid recovery which prevents teams from achieving stringent service-level agreements (SLAs). To stay competitive while protecting data, enterprises are embracing a modern 3-2-1 strategy that includes a virtual air gap with physical and network isolation and provides both secure and highly available data.



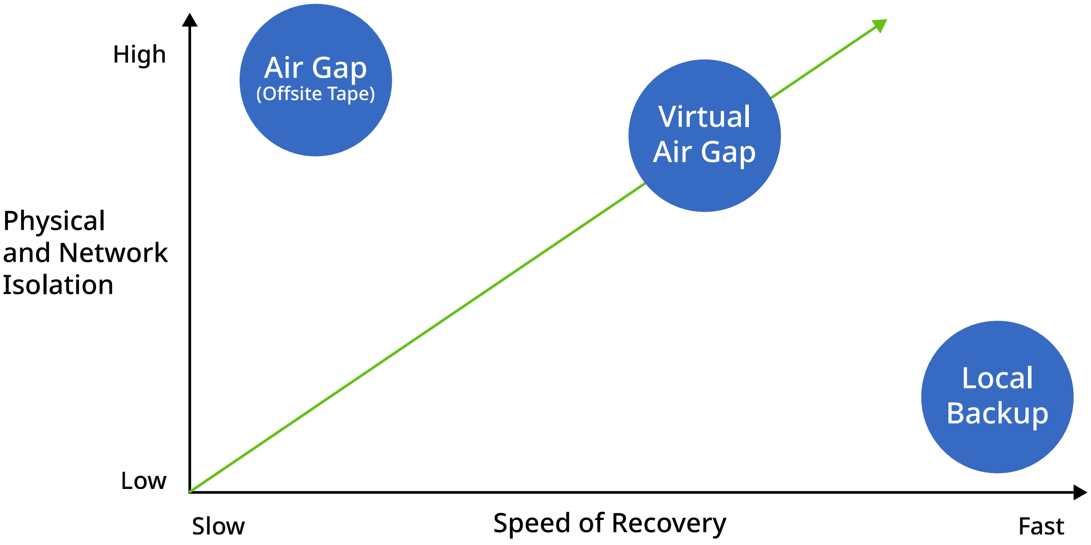


Figure 1: Modern data isolation via virtual air gap balances security and agility

Modern Air Gap for the Cloud Era

Cohesity FortKnox powers a modern 3-2-1 strategy for the cloud era that effectively balances organizations' security and agility priorities. A SaaS data isolation 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. FortKnox dramatically simplifies operations and lowers costs, eliminating the complexity and resource requirements of internally managed isolation solutions. FortKnox is a cloud service empowering organizations to prepare for and recover quickly and confidently from attacks with granular recovery back to the source or an alternate location, including the public cloud.

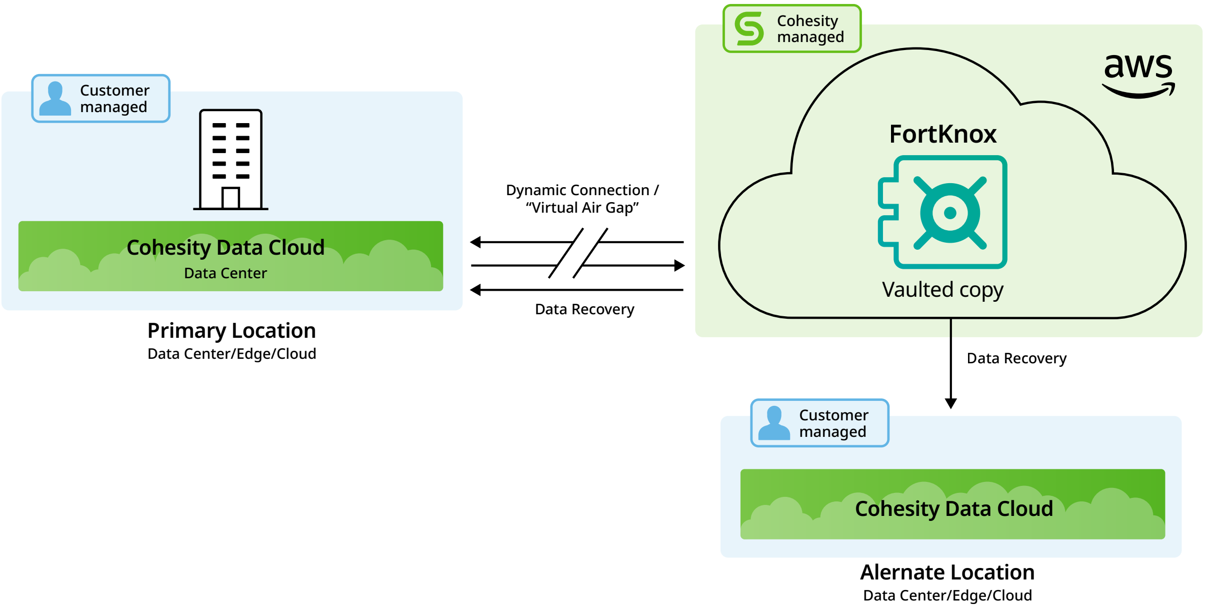


Figure 2: Cohesity FortKnox boosts cyber resilience with data recovery back to the source or to an alternate location

Key Benefits

Managing data vaults on-premises or in the cloud can be complicated and costly for internal teams, particularly as they encounter skills gaps and ever-more destructive ransomware that deletes backups and steals data. FortKnox overcomes these obstacles with a new data isolation technique that improves data resiliency amid rising ransomware attacks.

Additional Protection Layer Safeguards Data and Reputations

FortKnox is an integral part of the multilayered Cohesity Threat Defense architecture built on the notion of least privilege and segregation of duties with granular Zero Trust security principles. It keeps bad actors at bay with advanced access controls and early threat detection capabilities. FortKnox stores an immutable copy of data in a Cohesity-managed cloud vault via a configurable transfer window or virtual air gap and that copy of data is further protected with safeguards. These include role-based access (RBAC), encryption, multi-factor authentication (MFA), a WORM lock policy and a quorum rule that requires at least two employees to approve any critical actions, protecting data from unauthorized access or tampering. FortKnox allows for the management of global data vaults through a single UI and also automatically scans for cybercrimes by monitoring anomalous snapshots.

As-a-Service Consumption Dramatically Simplifies Operations and Lowers Costs

In a pay-as-you-grow service that keeps costs down, FortKnox empowers organizations to simply connect, vault, and recover data. No need to worry about deploying and maintaining "DIY" data vaults or the associated cloud storage or egress costs, as they are covered in the FortKnox subscription. When teams need to safely deposit data to the cloud vault or recover it quickly, Cohesity establishes a temporary and highly secure network connection that limits access to the isolated data by cybercriminals and unauthorized insiders while supporting business SLAs. Teams can leverage FortKnox data vaulting and recovery with customizable protection policies. Not only does FortKnox minimize enterprise attack surfaces, it also reduces the likelihood of a data breach.

Cohesity also provides customers greater flexibility to address varied RTO and budget requirements by providing a choice of FortKnox storage tier options—a warm storage tier for immediate data recoveries, suitable for ransomware protection use cases, as well as a more cost-effective cold storage tier with RTOs of up to 12 hours, suitable for compliance use cases.

Rapid Recovery Saves Time and Improves Business Continuity

FortKnox delivers fast, granular recovery of data back to the source or an alternate location, enabling enterprises to be more agile. Preferred recovery sites may be onsite, a public cloud (e.g., Amazon Web Services, Microsoft Azure, Google Cloud Platform), or an edge location. Since FortKnox prevents vaulted data from being modified, organizations with compromised or lost production data can be confident knowing that they can easily identify and recover an untainted copy of data. In contrast to legacy backup and air gap solutions, FortKnox simplifies the recovery of specific files and objects quickly—without having to restore whole data volumes.

Specifications

Virtual Air Gap	• Configurable transfer window, outside of which vault is locked from writing into/read access • Vaulted data copy isolated from customer environment with physical, network and management isolation, aka virtual air gap • Isolation from customer's own AWS cloud instance
Immutability	• Irrevocable DataLock (WORM) using AWS Object Lock • Read-only snapshots prevents intentional or unintentional modifications or deletions of vault data
Data Security	• Data-at-rest and data-In-flight Encryption • Flexible Cohesity or customer-managed KMS • Quorum controlled recoveries to minimize data exfiltration vectors
Access Control	• Multi-factor authentication • Granular role-based access control • Quorum for critical actions including recoveries • Short-lived token based authentication to access vault • Authenticated API call-based access over HTTPS • Access limited to authorized Cohesity clusters only
Ransomware Detection	• Machine learning-based anomaly detection and reporting
Rapid Recovery	• Machine driven recommendation of clean snapshot for faster incident response • Quick, granular recovery back to source or alternate location to meet stringent SLAs
As a Service Consumption	• SaaS solution that's as simple as connect, vault and recover • Data vaulting and recovery with customizable protection policies • Pay as you go consumption model based on back-end TB (BETB) usage • No cloud storage or egress costs
Flexible Storage Classes	• Warm Storage Tier on Amazon S3 IA (Infrequent Access) for recovery that starts immediately upon customer initiation, and a minimum 30-day retention period. • Cold Storage Tier on Amazon S3 Glacier FR* (Flexible Retrieval) for recovery that starts 4 hours after customer initiation, and a minimum retention period of 90 days or longer.
Single Pane of Management	• View and manage global data vaults with centralized dashboard • Simplified administration with SLA-based policies

*Available in early 2023

Simplify and modernize data isolation and recovery with Cohesity FortKnox.
Visit the free trial to get access to FortKnox.

COHESITY

COHESITY

SOLUTION BRIEF

Cohesity DataHawk

Threat protection and data intelligence for cyber recovery

Key Benefits

- Identify emerging ransomware attacks
- Detect risky user behaviors
- Ensure recovery data is malware free
- Get simple and cost effective data isolation
- Leverage and amplify existing security controls

Ransomware and cyberattacks continue to increase in frequency and severity as threat actors and nation-states attack organizations for monetary and political gains. Recovery is key as cyber defenses are never 100% reliable. Advanced data security and management solutions provide additional security and recovery to help organizations withstand and recover from cyber incidents, including ransomware, destructive cyberattacks, insider threats, natural disasters, and system failures.

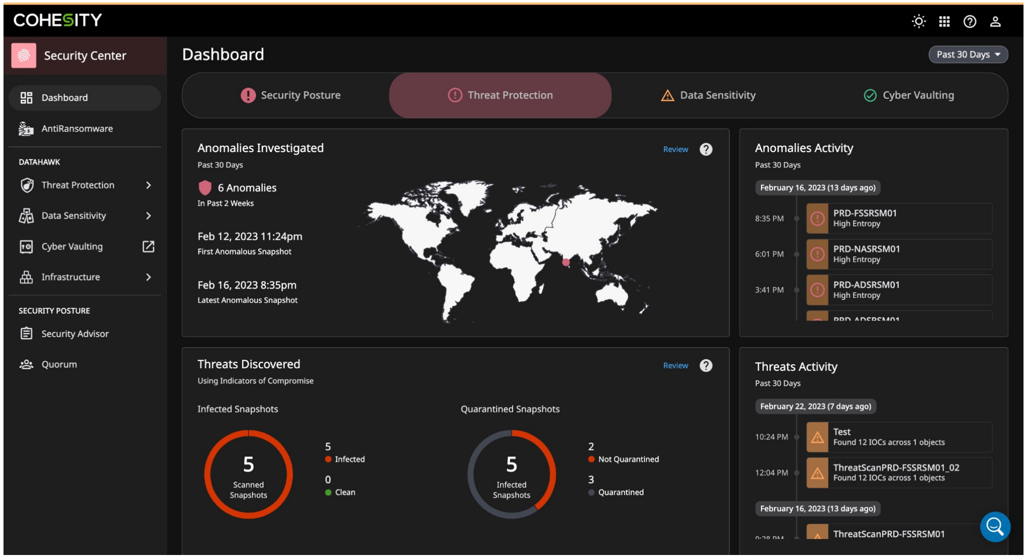
Along with immutability, Zero Trust principles, and instant recovery of data and processes, organizations need solutions that can detect cyber threats, provide impact analysis of sensitive data exposure, securely isolate data, and seamlessly integrate with security operations. As a result, organizations should consider modernizing security and resiliency with a cloud-based service to:

- Leverage AI/ML for threat detection and to ensure clean data recovery
- Use ML/NLP to identify sensitive data exposure from cyber incidents
- Take advantage of cyber vaulting to securely isolate data from threats
- Integrate with security operations to amplify cyber defenses and response

Improve Recovery for Cyber Resilience

Cohesity DataHawk provides multiple cloud service offerings that deliver comprehensive data security and recovery capabilities to withstand and recover from cyber incidents. DataHawk works with Cohesity DataProtect to extend the security and threat detection of the Cohesity data protection platform.

DataHawk leverages AI/ML to detect user and data anomalies that could indicate an emerging attack, utilizes threat intelligence to ensure recovery data is malware-free, and, with data classification, enables organizations to determine the exposure of sensitive and private information when an



Anomalies Investigated
Past 30 Days
6 Anomalies
In Past 2 Weeks
Feb 12, 2023 11:24pm
First Anomalous Snapshot
Feb 16, 2023 8:35pm
Latest Anomalous Snapshot

Anomalies Activity
Past 30 Days
February 16, 2023 (13 days ago)
8:35 PM PRD-FSSRSM01 High Entropy
6:01 PM PRD-NASRSM01 High Entropy
3:41 PM PRD-ADSRSM01 High Entropy
PRD-ADSRSM01

Threats Discovered
Using Indicators of Compromise
Infected Snapshots: 5 Scanned Snapshots — 5 Infected, 0 Clean
Quarantined Snapshots: 5 Infected Snapshots — 2 Not Quarantined, 3 Quarantined

Threats Activity
Past 30 Days
February 22, 2023 (7 days ago)
10:24 PM Test — Found 12 IOCs across 1 objects
12:04 PM ThreatScanPRD-FSSRSM01_02 — Found 12 IOCs across 1 objects
February 16, 2023 (13 days ago)
ThreatScanPRD-FSSRSM01

Figure 1: Identify Potential Data Exfiltration with Behavior Analytics

attack occurs. DataHawk provides an additional layer of security for recovery data with point-and-click data isolation and integrates with your security operations and existing incident response and remediation processes.

Bolster Your Data Security Defenses, Accelerate Recovery

Consolidate security intelligence and command

The Cohesity security center provides an integrated dashboard to monitor security alerts, threats, sensitive data exposure, data isolation status, and the security posture of the Cohesity platform. The security center provides drill down and control to all DataHawk capabilities to manage platform health and threats—and control security settings and schedules.

Improve threat protection

Ransomware and other attacks use deceptive tactics to cloak malware. Cohesity Threat Hunting helps you find elusive threats using AI/ML-driven threat detection that identifies the latest variants of ransomware and other cyberattacks. Our extensive library of over 117K behavioral patterns is updated frequently with the latest threats. For finding specific threats, organizations can create and import custom or existing YARA rules.

Understand attack impact

Use ML/NLP to determine if sensitive data has been exposed and ensure appropriate remediation and compliance processes. Support global deployments with 200+ prepackaged and customizable patterns.

Layer security with data isolation

Evade threats and meet modern recovery goals with award-winning cyber vaulting to support best practices and emerging requirements for enhanced security. Maintain data immutably in the cloud behind a virtual air gap with physical separation, and network and operational isolation. Recover data quickly and easily in case of an outage or disaster.

Improve detection and response with SOC integrations

Integrate data anomaly detection with your security operations center (SOC) to amplify and support existing incident triage, response, and remediation processes.

Services for Security and Recovery

Threat intelligence and scanning

Improve data security with one-click threat detection and scanning, utilizing AI/ML-driven threat detection, with over 100K threat rules updated daily.

Intelligent data classification

Get data discovery and classification powered by BigID using ML/NLP- based pattern matching to identify sensitive and regulated data. Users can leverage over 200 patterns to automatically or proactively discover and classify personal, health, and financial data when a breach occurs.

Cohesity FortKnox

Get the benefit of data isolation service with management, network, and location isolation, supported by immutability, Zero Trust principles, and quorum while delivering simple, flexible and granular recovery.

Related Products/Features

Cohesity DataProtect – Comprehensive backup and recovery for traditional and modern workloads is built on a secure and scalable multicloud platform—and provides instant recovery at scale and across environments.

Cohesity SmartFiles – A software-defined, unified file and object solution designed for the hybrid cloud that allows enterprises to securely and efficiently govern data at scale. SmartFiles consolidates data silos to a converged target and securely manages capacity-centric unstructured content such as digital libraries, archives, rich media, video surveillance, big data, and backup data sets.

A Proven Platform for Data Security and Management

Thousands of customers already enjoy the simplicity and proven value of the Cohesity Data Cloud platform. No matter where you are in your data security and management journey, we offer a full suite of services consolidated on one multicloud data platform: data security and protection, backup and recovery, disaster recovery, file and object services, dev/test, data compliance, and analytics.

Learn more at www.cohesity.com/products/datahawk.

COHESITY

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

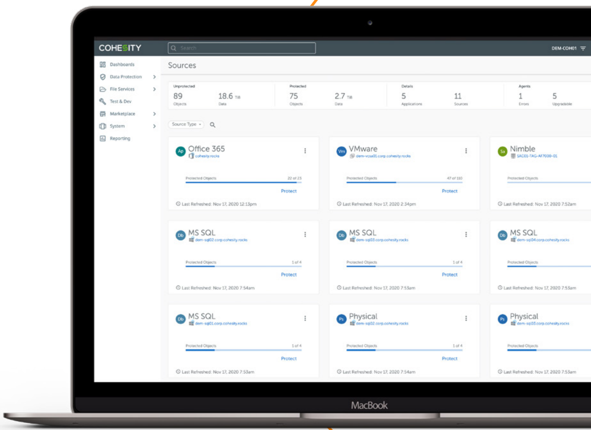
DATASHEET

Cohesity DataProtect

Available as a Service or Self-managed Software

Cohesity DataProtect is a high-performance, secure backup and recovery solution. Designed to safeguard your data against sophisticated cyber threats, it offers the most comprehensive policy-based protection for your cloud-native, SaaS, and traditional data sources.

DataProtect converges multiple-point products into a single software that can be deployed on-premises or consumed as a service (BaaS).



Sources

Unprotected: 89 Objects, 18.6 TiB Data
Protected: 75 Objects, 2.7 TiB Data
Details: 5 Applications, 11 Sources
Agents: 1 Errors, 5 Upgradable

Office 365 — cohesity.rocks — Protected Objects 22 of 23 — Protect — Last Refreshed: Nov 17, 2020 12:13pm

VMware — dem-vcsa01.corp.cohesity.rocks — Protected Objects 47 of 110 — Protect — Last Refreshed: Nov 17, 2020 2:34pm

Nimble — SAC01-TAG-AF7000-01 — Protected Objects — Last Refreshed: Nov 17, 2020 7:52am

MS SQL — dem-sql02.corp.cohesity.rocks — Protected Objects 1 of 4 — Protect — Last Refreshed: Nov 17, 2020 7:54am

MS SQL — dem-sql03.corp.cohesity.rocks — Protected Objects 1 of 4 — Protect — Last Refreshed: Nov 17, 2020 7:53am

MS SQL — dem-sql04.corp.cohesity.rocks — Protected Objects — Last Refreshed: Nov 17, 2020 7:53am

MS SQL — dem-sql01.corp.cohesity.rocks — Protected Objects 1 of 4 — Protect — Last Refreshed: Nov 17, 2020 7:53am

Physical — dem-sql02.corp.cohesity.rocks — Protected Objects 1 of 4 — Protect — Last Refreshed: Nov 17, 2020 7:54am

Physical — dem-sql03.corp.cohesity.rocks — Protected Objects — Last Refreshed: Nov 17, 2020 7:53am

Multi-layered Protection for Enterprise Applications

Designed on zero-trust principles, Cohesity DataProtect secures your enterprise data across a broad set of sources - virtual and physical servers, traditional and containerized applications, databases, NAS, and SaaS workloads.

A combination of immutability, WORM, data encryption framework, multifactor authentication, and granular role-based access control helps to stop unauthorized applications and bad actors from modifying or deleting your data.

Lightning Fast Recovery

The solution features near-zero recovery point objectives (RPOs) and near-instant recovery time objectives (RTOs) to meet business service-level agreements (SLAs). With Cohesity Helios' unified control plane quickly search and recover data on any Cohesity cluster, located anywhere. DataProtect uniquely reduces downtime by instantly mass restoring any number of virtual machines (VMs), large volume of unstructured data, and any size Oracle database, to any point in time, and reduces data protection costs by 70% or more.

Freedom of Backup as a Service (BaaS)

Take advantage of the public cloud's elasticity and economics with DataProtect delivered as a service. Choose an OpEx spend model and eliminate the need for on-premises hardware. The SaaS option allows you to easily configure your backup jobs and, within minutes, start protecting your mission-critical data and applications without needing any hardware on-premises.

Hosted in AWS and Microsoft Azure, Cohesity BaaS offers flexibility and choice to meet your business requirements.

Specifications

	Self-managed	Cohesity-managed BaaS
Protected Workloads	• Hypervisors: VMware vSphere (5.5 and later), Microsoft Hyper-V (2019, 2016, 2012 R2), Nutanix AHV and RHeV • Kubernetes-based data and application state • Cloud: AWS EC2, Azure VM, and Google Compute • Physical: Windows, Linux (RHEL, CentOS, OEL, Debian, Ubuntu), AIX (7.x), and Solaris • Enterprise Databases: Oracle (11g R2, 12c), Oracle RAC and Microsoft SQL (2008 or later), SAP Oracle, SAP HANA, SAP Sybase ASE, SAP MS SQL, Sybase IQ, IBM DB2 LUW, Sybase ASE • Modern Databases: MongoDB with CDP, Hive, Hbase, Cassandra, CouchbaseDB, MySQL Enterprise Commercial Edition • Cloud-native Databases: AWS RDS, AWS Aurora, CockroachDB • Applications: MS Exchange (2010 SP3 or later), MSFT Active Directory, Microsoft 365 (Exchange Online, SharePoint Online, OneDrive, Teams, Groups), SalesForce (SFDC), and SAP HANA • Primary storage: Pure FlashArray, HPE Nimble and Cisco Hyperflex • NAS: Pure FlashBlade, NetApp, Isilon, IBM GPFS, Google EFS, Elastifile, and generic solutions	• Hypervisors: VMware vSphere (5.5 and later) and Microsoft Hyper-V (2019, 2016, 2012 R2) • Cloud: AWS EC2 • Physical: Windows and Linux (RHEL, CentOS, OEL, Debian, Ubuntu), AIX (7.x) • Enterprise Databases: Oracle (11g R2, 12c) and Microsoft SQL (2008 or later) • Cloud-native Databases: AWS RDS • SaaS Applications: Microsoft 365 (Exchange Online, SharePoint Online, OneDrive and Teams) and Salesforce (EA) • Primary storage: AWS S3 (EA) • NAS: NetApp, Isilon and generic solutions
Recovery Level	• Instant mass restore • Granular recovery of files, folders, and objects • Volume recovery	• VMDK recovery • Instant volume mounts • Instant restores of VMs
Ransomware Protection	• Immutable backups, DataLock (WORM), encryption, and RBAC • Machine learning-based anomaly detection • Rapid recovery at scale	
Long-Term Archival	• Public cloud infrastructure, S3 and NFS compatible devices • Tape support using QStar archive manager	
Global Search	• Global actionable search • Automated global indexing • Wildcard searches for any VM, file, or object on the platform	
Flexible Deployment	• Software-defined solution for on-premises, public cloud, backup as a service, and edge sites	
Public Cloud Integration	• Multiple cloud solutions including long-term retention, disaster recovery, dev/test and native cloud backup • Cohesity CloudSpin	• Cohesity Cloud Snapshot Manager • Cohesity CloudArchive (unlimited) • Cohesity CloudArchive Direct
Global Management and Access Control	• Cohesity Helios control plane • Multi-cluster single sign-on • Role-based access control	• Multi-factor authentication • Multi-cluster dashboard

Specifications	
Machine-Drive Recommendation	• Clean recovery point • Proactive system wellness • Capacity prediction • What-if analysis • Performance balancing • Support automation
Capacity Optimization	• Storage efficiency (EC, small file efficiency) • Global variable-length sliding-widow deduplication • Compression
Integration and Automation	• API-first architecture • OpenAPI standard • RESTful API • Python SDK • PowerShell Module • VMware vRealize (vRA/vRO) • VMware vCloud Director (vCD) • ServiceNow • Ansible
Security	• Software-defined AES-256, FIPS 140-2 compliant encryption of data in flight and at rest

Simplify and modernize your backup and recovery infrastructure with Cohesity DataProtect.
Learn more at Cohesity.com/products/dataprotect.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

SOLUTION BRIEF

Cyber Resilience Security Framework – Going Beyond Zero Trust

Key Benefits

- Enable, build, and keep pace with critical Zero Trust cybersecurity
- Automated cybersecurity analytics for detection, response, & recovery of cybersecurity events
- Open API for 3rd party security tools and analytics, run cyber security apps directly on the platform
- Future proof; a purpose-built software-defined platform for multi-cloud hyper-scale deployments

Cyber resilience refers to an entity's ability to continuously deliver the intended outcomes, despite adverse cyber events. The concept essentially brings the areas of information security (and zero trust principles), business continuity, and organizational resilience together. A critical component to any security framework that aims to achieve a level of cyber resilience is ensuring that the security framework is aligned with Zero Trust principles of "never trust, always verify," which means that devices should not be trusted by default, even if they are connected to a managed corporate network such as the corporate LAN and even if they were previously verified. There are three key components in a zero trust architecture: user/application authentication, device authentication, and trust (don't trust). A cyber resilience security strategy and framework defines security throughout your IT systems and environments to prevent threat actors from accessing your most valuable resource: your data. One of the weakest links in many organizations' security strategy is how their data is organized, protected, and managed. It includes Zero Trust principles of "never trust, always verify" but does not stop there.

Many organizations still have unstructured data, with disparate policies that are inconsistently implemented. These conditions create an attractive attack surface with many attack vectors primed for exploitation by ransomware and cybersecurity criminals. These challenges are compounded with systems getting more distributed and complex with cloud, and more frequently, multicloud.

A successful cyber resilient security approach helps the government successfully keep data secure, detects and defends against cyber attacks, while also delivering on mission objectives. Government organizations are increasingly dependent on properly optimized, simplified, and protected data. A cyber resilient security framework that informs and delivers a security posture that enables the ability to continuously deliver the government's intended outcomes, despite adverse cyber events.

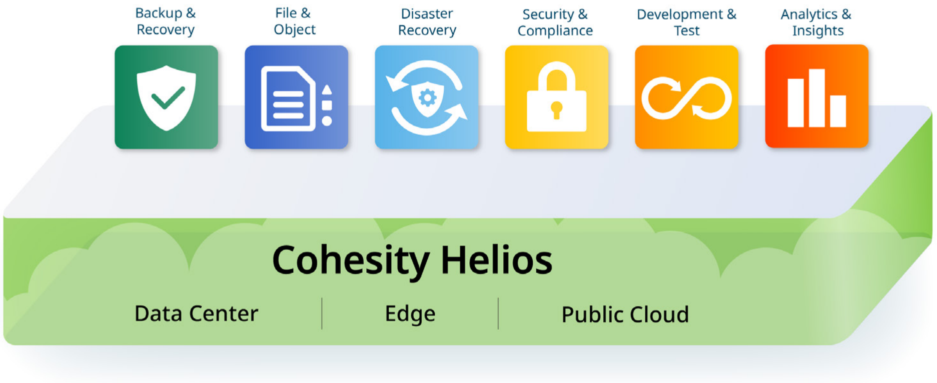


Figure 1. Cohesity Helios is your single data protection platform with reach into all topology areas enabling key critical cyber security functions in the most efficient and cost-effective way available in the industry.

This security approach must also be ready to perform at hyperscale, on-prem, and with multiple simultaneous private and public clouds. Cohesity DataProtect can do all of this for you and more, enabling your organization to achieve a level of cyber resilience by closing many security gaps including those driven by a Zero Trust strategy of systems access, while also keeping your data management operation tuned and automated. This protects the organization by reducing cyber risk, lowering costs, and driving operational efficiencies.

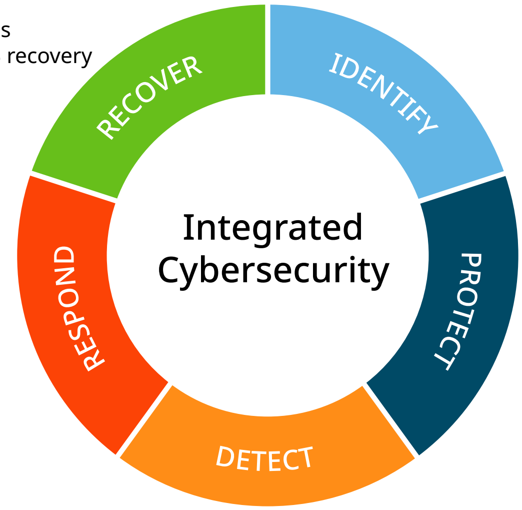
Cohesity Helios is a market-leading multicloud platform that dramatically simplifies how organizations protect and manage their data. Helios aligns and supports NIST, NSA, and DISA security frameworks by providing security capabilities for Data, Applications, Workloads, Devices, Visibility, Analytics, Automation, and Orchestration. Helios is purpose-built to run smart data analysis tools alongside your data at the edge, core, and cloud. These capabilities enable instant backup and recovery, automated disaster recovery orchestration, proactive machine learning-based anomaly detection, ransomware recovery, anti-virus, data classification, auto-indexing with full-text search, data deduplication and compression, quality of service management, data encryption in flight and at rest, immutable data stores, data replication, data storage, data cloning, data masking, and more.

Simultaneously designed to work at the edge, in your data center, and multicloud environments, and with additional onboard tools providing lightning-fast remediation of CMI spills, PHI and PII incidents, and similar events, Cohesity enables your agency to protect, detect and recover from cybersecurity attacks - recover fast and greatly reduce the impact of a ransomware attack. Cohesity capabilities offer a multilayered Cyber Resilience protection approach helping achieve a more comprehensive security posture that goes beyond a Zero Trust Framework.

Cohesity's Comprehensive Cybersecurity Framework

Recover
- Instant recovery at scale for VMs
- Non-disruptive instant large DB recovery
- Recover anywhere to any point
- Machine-driven clean snapshot recommendation

Identify
- Global visibility across environments
- Security advisor
- Cyber vulnerability scan



Respond
- Restore anywhere for forensics
- Built-in auditing and reporting
- Granular active directory comparison

Protect
- Immutable snapshots
- Immutable file system
- Encryption inflight and at rest
- WORM
- Test recoverability multi factor authorization
- Granular RBA
- No service backdoor
- Whitelisting

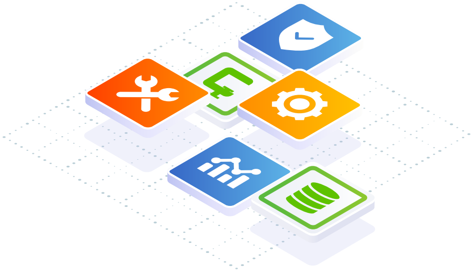
Detect
- Machine learning-based anomaly detection
- Deep visibility of affected objects and sources
- Realtime notifications and alerts

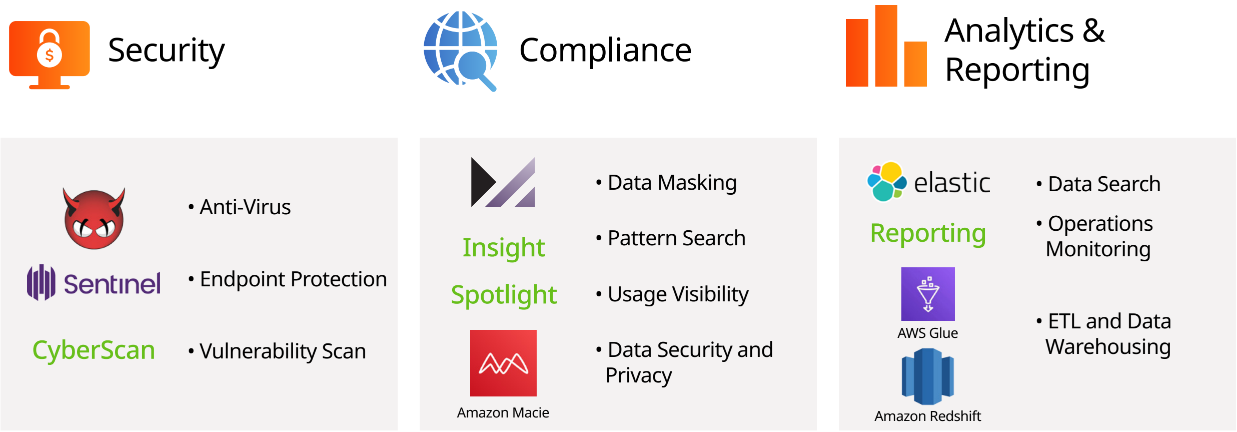
Figure 2. Cohesity's comprehensive cybersecurity framework supports NIST, NSA & DISA Zero Trust Architectures

Feature	Benefit	Description
Zero Trust Hardening	Highly secure – configure once, securely deploy across locations	Accelerating data mobilization, Cohesity can be securely configured and right-sized once then redeployed as the same secure environment anywhere from the cloud to on-prem or the edge reducing deployment time from weeks to hours
Automated Discovery, Baselining & Analytics	Automated the discovery and baseline production system data for Ransomware detection and remediation. Capture production environment elements for historical analysis.	Cohesity performs data analytics co-resident with data storage and can expand use cases enabling Federal organizations to keep pace with future Zero Trust cybersecurity challenges. This presents the most efficient analytics security, performance, business optimization, and operational efficiencies - Cohesity CDP (continuous data protection)
Future Security Capabilities	Cohesity Helios is an application framework and robust extensible API	Cohesity Helios provides an excellent method to quickly onboard new security capabilities to protect against emerging threats.
Improved data analytics and application mobility	Fast access to trends in data for better decision making	Cohesity empowers field-based teams to fully leverage the platform's compute capability to process data analytics in the field and make results readily available. Cohesity Marketplace apps enable rapid search, email forensics, e-discovery, tagging, and help streamline compliance. As a result, teams working with different applications across the many nodes and echelons of the tactical and higher-level networks are better informed.
Software-Defined	Consolidate multiple workloads onto a common data platform. Reduce cost and risk for on-prem and multi-cloud.	Cohesity's software-defined hyper-converged data management platform consolidates multiple point products and converges a range of data services, which helps to reduce that attack surface. The disaggregated architecture integrates easily with leading infrastructure as code and other 3rd party solutions. The net result is the ability to quickly scale up or scale down on demand achieving linear scale to performance objectives for a very broad set of DoD use cases, in additional cybersecurity Zero Trust Architecture.
Standards compliant	Government Certified solution for peace of mind	The joint solution features comprehensive technical controls and certifications: • FIPS 140-2 Level 2 Validated • TAA compliant • Federal Information Security Management Act (FISMA) Compliance | Authorities to Operate (ATOs) on DoD networks • WORM Compliant – SEC 17a-4f certification • Strong multi-factor, certificate (PIV/CAC)-based authentication • Common Criteria: EAL 2+ • SOC 2 Type 2 • (DoDIN) Approved Products List (APL) • Native cloud integrations with all leading FedRAMP clouds
Includes integrated vendor suites	Cohesity's hyperscale platform is architected to consolidate multiple point-product capabilities onto a common data platform.	3rd party capabilities can be integrated onto your Cohesity platform, which reduces costs and creates transformational efficiencies for the government; a highly functional data platform, Helios consolidates multiple data sets, data types, and workloads onto a common platform for more efficient cybersecurity work that can be done in one place.
SIEM Event data storage	Cohesity provides efficient and effective long-term storage of SEIM event data.	Cohesity integrates with leading SEIM vendors providing industry-leading dedupe and compression of log and event data to drive maximum capacity efficiency - lowering operating costs and streamlining Zero Trust and cybersecurity operations for other tools and platforms.
Low operational overhead		To accommodate the variable skills of federal operators, the solution can be pre-configured with the right data and simply stood up. As missions and requirements change, authorized personnel can easily and quickly modify automated policies.

Cohesity App Marketplace

Cohesity developed and third party





Security

- Anti-Virus
- Endpoint Protection
- Vulnerability Scan

Compliance

- Data Masking
- Pattern Search
- Usage Visibility
- Data Security and Privacy

Analytics & Reporting

- Data Search
- Operations Monitoring
- ETL and Data Warehousing

Figure 3. Run your favorite data analytics and security applications (such as Splunk, Tenable, ClamAV, and more) on the same Cohesity platform that stores, indexes, and backs up your data

Trusted Across the Government

USDA
U.S. AIR FORCE
DARPA
UNITED STATES COURTS

To learn more, visit www.cohesity.com/solutions/industry/government

COHESITY

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

SOLUTION BRIEF

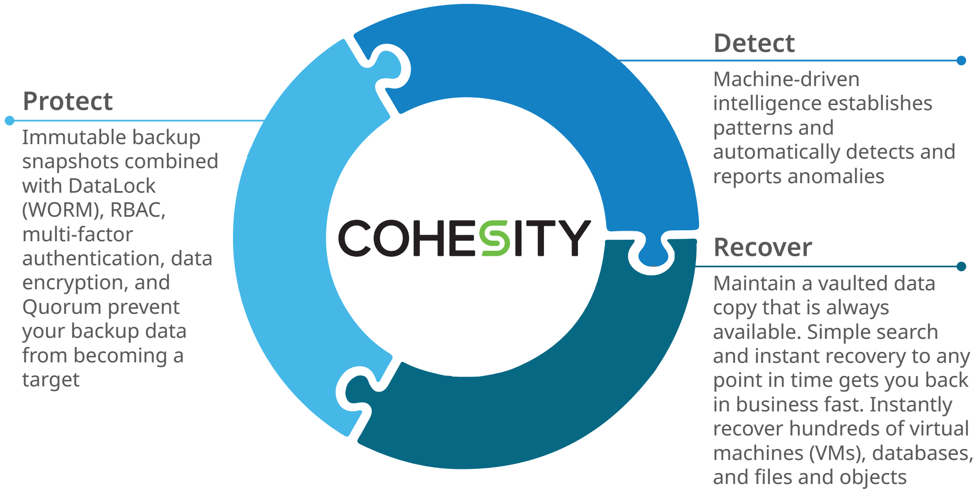
Counter Ransomware Attacks with Cohesity

Key Benefits

- Protect your data and business with a defense-in-depth architecture
- Quickly identify potential attacks with machine learning-based anomaly detection
- Reduce downtime with rapid recovery at scale

Data is a differentiator in the digital economy. That's why data has simultaneously become the most valuable and the most targeted business asset. Cybersecurity Ventures expects global cybercrime costs to reach $10.5 trillion USD annually by 2025 and that a business will fall victim to a ransomware attack every 2 seconds by 2031[1]. Even as awareness of digital extortion schemes is rising, more sophisticated and focused attacks increasingly target backup data and infrastructure continuing to threaten enterprises worldwide. For businesses that do become compromised, steep financial loss is often compounded by customer distrust, and in the case of healthcare, risk to human life.

Cohesity effectively counters ransomware attacks and helps your organization avoid paying ransom. Cohesity's comprehensive, next-gen data management solution features a multi-layered approach to protect backup data against ransomware, detect and rapidly recover from an attack. Cohesity's unique immutable architecture ensures that your backup data cannot be encrypted, modified or deleted. Using machine learning, it provides visibility and continuously monitors for any anomalies in your data. And if the worst happens, Cohesity helps to locate a clean copy of data across your global footprint, including public clouds, to instantly recover and reduce downtime.



Protect

Immutable backup snapshots combined with DataLock (WORM), RBAC, multi-factor authentication, data encryption, and Quorum prevent your backup data from becoming a target

Detect

Machine-driven intelligence establishes patterns and automatically detects and reports anomalies

Recover

Maintain a vaulted data copy that is always available. Simple search and instant recovery to any point in time gets you back in business fast. Instantly recover hundreds of virtual machines (VMs), databases, and files and objects

Figure 1: Cohesity delivers comprehensive capabilities to protect, detect and recover from a ransomware attack

[1] Cybersecurity Ventures: Top 6 Cybersecurity Predictions And Statistics For 2021 To 2025 (Dec. 30, 2021)

Protect

Sophisticated ransomware such as Locky and Crypto recently has been used to destroy shadow data copies and restore point data, making enterprise backup infrastructure a prime cyber-criminal target when it should be part of your organization’s defense. Cohesity stops intruders by preventing your backup from becoming an attack target.

Cohesity SpanFS™, a third-generation distributed filesystem—uniquely offers multi-layered protection against a ransomware attack. Among other things, Cohesity delivers the highest level of protection against ransomware attacks because immutability is at the foundation.

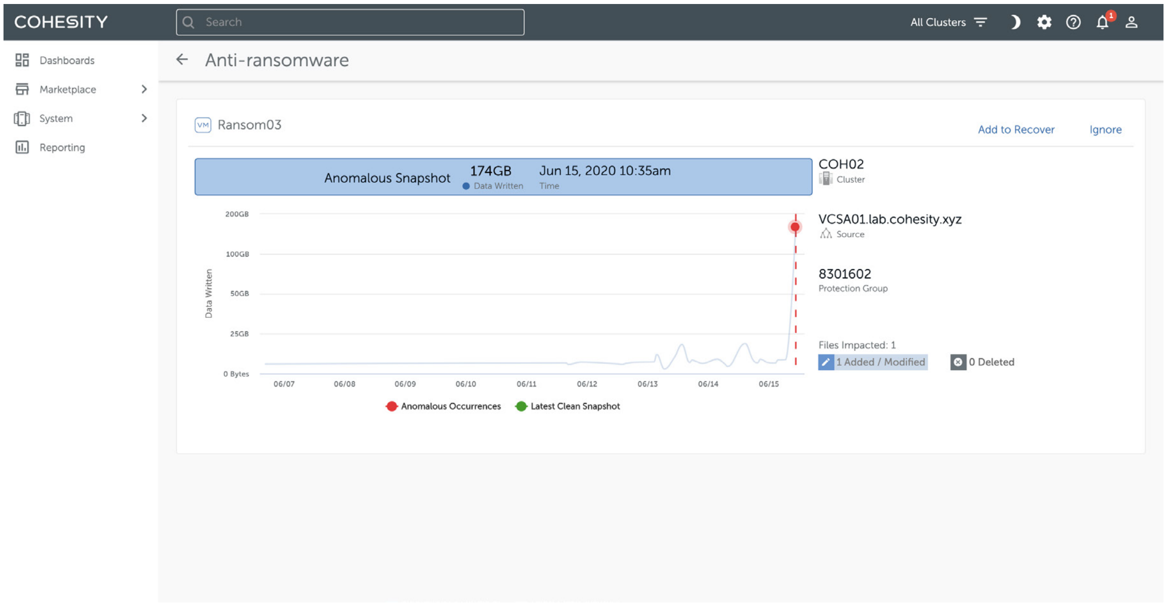
- **Immutable snapshots** – All backup snapshots, by default, are stored in an immutable state within Cohesity. The original snapshot (aka gold copy) is never mounted or exposed to any external system or application. The only way to write new data or mount the backup for recovery in read-write mode is to create a zero-cost clone of the original backup, which is done automatically by the system.
- **DataLock** – WORM capability for backup enables the role-based creation and application of a Datalock policy to selected backup snaps. The security officer role in your organization can use this feature to store snaps in WORM format. The time-bound setting enforcing spans cannot be deleted, even by the administrator or security officer role, providing an extra layer of protection against ransomware attacks.
- **Role-based access control (RBAC) –** To reduce the risk of unauthorized access to data and systems, Cohesity enables your IT staff to grant each person a minimum level of access to what is needed to do a particular job.
- **Multi-factor authentication (MFA)** – Should a criminal actor get access to your system password, that individual would not be able to access the Cohesity backup without passing an additional layer of security in the form of MFA or multi-step verification. Cohesity supports a variety of authentication and authorization capabilities, including strong Active Directory integration, MFA, access control lists, mixed-mode role-based access control (RBAC), and comprehensive system and product-level auditing.
- **Data encryption** – Cohesity features software-based FIPS-validated, AES-256 standard encryption for your data in flight and at rest. This cryptographic module validated by the United States National Institute of Standards and Technology (NIST) at the Federal Information Processing Standards (FIPS) 140-2 Level 1 standard is trusted worldwide.
- **Quorum** – To protect your data and systems from insider threats and stolen credentials, Cohesity requires any root-level or critical system change anyone in your organization wants to make be authorized by more than one person.

Cohesity Helios, a next-gen data management platform, delivers a unique combination of immutable backup snapshots, DataLock capabilities, RBAC, MFA, plus Quorum (aka the four-eye rule), to prevent backup data from becoming part of a ransomware attack.

Detect

As cyber criminals continue to strengthen and modify their approaches, Cohesity makes it easier for your organization to detect intrusions with a global, enterprise SaaS-based management solution. Cohesity customers have a single dashboard to see, manage, and take action fast on their data and applications globally. In the fight against ransomware, Cohesity Helios machine learning (ML) provides insights humans may miss because it automatically and continuously monitors and notifies you when an anomaly is detected.

The cutting-edge ML algorithms proactively assess your IT needs and automate infrastructure resources regularly. If your organization’s data change rate, including data ingest is out of the normal range—based on daily change rates on logical data, stored data after global deduplication, or historical data ingest—Cohesity Helios’ machine-driven anomaly detection sends a notification to your IT administrators. Instantly, IT is informed that data changes do not match normal patterns.



Ransom03

Anomalous Snapshot 174GB Data Written Jun 15, 2020 10:35am Time

COH02 Cluster

VCSA01.lab.cohesity.xyz Source

8301602 Protection Group

Files Impacted: 1

1 Added / Modified 0 Deleted

Figure 2: With Cohesity Helios, organizations detect ransomware intrusions

Because Helios machine-driven learning establishes patterns and automatically scans for data ingest/change rate anomalies, it flags a potential ransomware attack. Should an anomaly be detected, the platform simultaneously alerts both your enterprise IT team and Cohesity's support team, expediting remediation.

Besides monitoring backup data change rate to detect a potential ransomware attack, Cohesity uniquely detects and alerts for file-level anomalies within unstructured files and object data. This includes analyzing the frequency of files accessed, number of files being modified, added or deleted by a specific user or an application, and more to ensure, a ransomware attack is quickly detected.

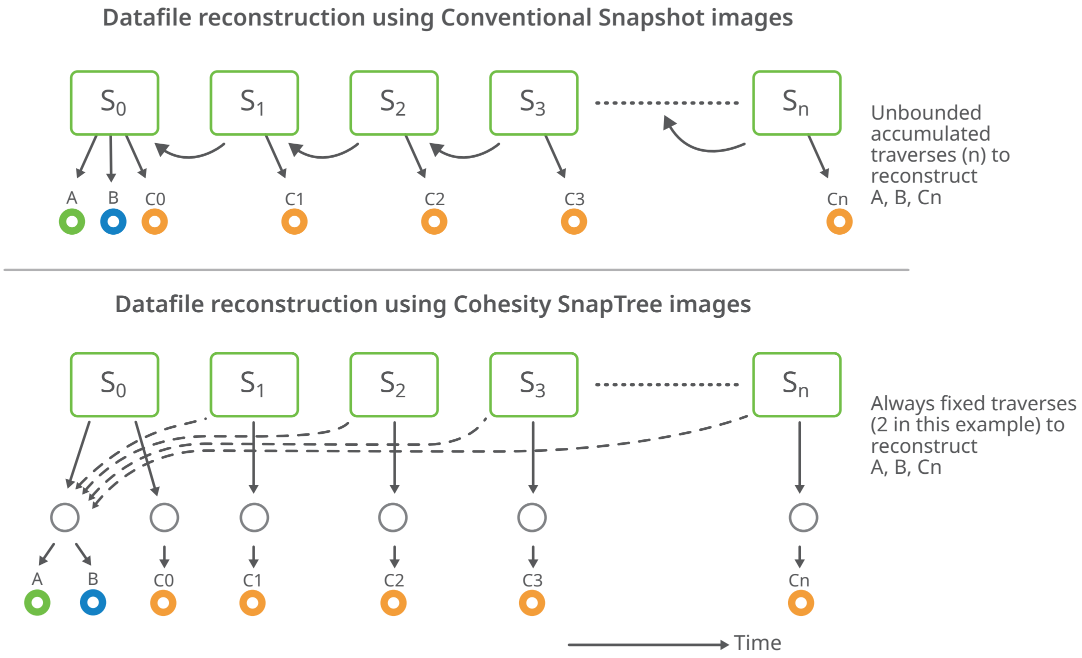
Recover

Cybersecurity threats, internal and external, do happen, and fast. That's why recovery has to be predictable and rapid. Cohesity speeds the process of getting back your ransomed enterprise data and applications—at scale. In addition to the immutable backups, Cohesity offers multiple policy-based methods to isolate your mission-critical data and have the last good copy secured. To meet your unique recovery and security requirements, you can isolate your data into the Cohesity-managed cloud vault - Cohesity FortKnox, replicate it to another immutable cluster, or tape it out to offsite storage, like Iron Mountain.

Cohesity Helios' machine-drive assistance helps accelerate the recovery by recommending a clean copy of data to restore. Alternately, you can leverage the platform's global search capabilities to quickly locate and access the data across environments.

To ensure a clean restore and avoid re-injecting a cyberthreat or software vulnerability into your production environment, Cohesity's CyberScan provides deep visibility into the health and recoverability status of protected snapshots. CyberScan shows each snapshot's vulnerability index and actionable recommendations to address software vulnerabilities. This helps you to cleanly and predictably recover from a ransomware attack.

With the combination of fully hydrated snapshots with Cohesity's proprietary SnapTree's B+Tree architecture, MegaFile, and instant mount, you can dramatically reduce your downtime by restoring hundreds of virtual machines (VMs), files, objects, and large databases instantly.


Datafile reconstruction using Conventional Snapshot images

S0
S1
S2
S3
Sn
A
B
C0
C1
C2
C3
Cn
Unbounded accumulated traverses (n) to reconstruct A, B, Cn

Datafile reconstruction using Cohesity SnapTree images

S0
S1
S2
S3
Sn
A
B
C0
C1
C2
C3
Cn
Always fixed traverses (2 in this example) to reconstruct A, B, Cn
Time

Figure 3: Cohesity patented SnapTree technology delivers unlimited snaps with no overhead, supporting instant recovery at scale

Counter Ransomware Attacks with Cohesity

Backup is your last line of defense against sophisticated and crippling ransomware attacks. Cohesity's comprehensive anti-ransomware solution protects, detects and most importantly, rapidly recovers what you need to reduce downtime and ensure business continuity.

Learn more at www.cohesity.com/solutions/ransomware

COHESITY

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.