SOLUTION BRIEF

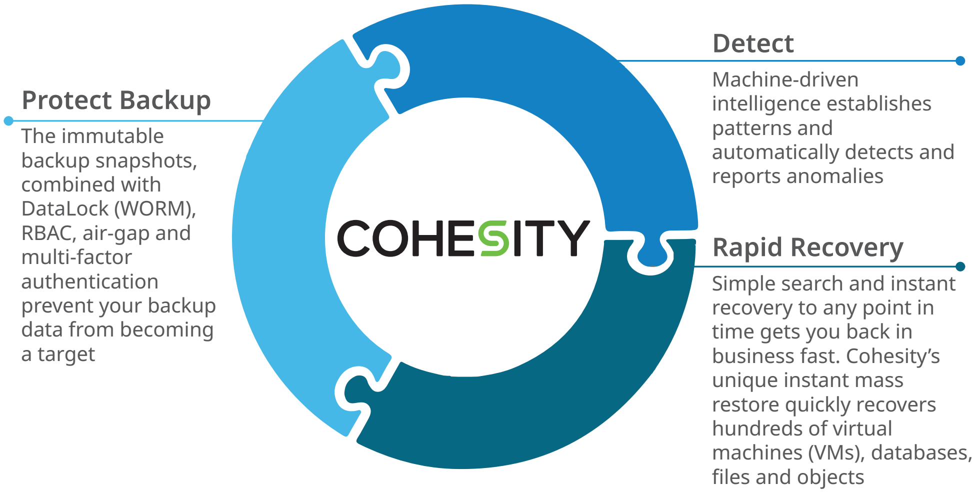
Counter Ransomware Attacks with Cohesity

Key Benefits

- Protect backup with immutable snapshots
- 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. As reported by Cybersecurity Ventures, it expects global cybercrime costs to reach $10.5 trillion USD annually by 2025, and a business will fall victim to a ransomware attack every 11 seconds by 2021[1]. Awareness of this digital extortion scheme is rising, yet more sophisticated and focused attacks that now increasingly target backup data and infrastructure continue 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, end-to-end 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 Backup
The immutable backup snapshots, combined with DataLock (WORM), RBAC, air-gap and multi-factor authentication prevent your backup data from becoming a target

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

Rapid Recovery
Simple search and instant recovery to any point in time gets you back in business fast. Cohesity’s unique instant mass restore quickly recovers hundreds of virtual machines (VMs), databases, files and objects

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

[1] Cybersecurity Ventures: Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2021 To 2025 (January 8, 2021)

Protect Backup Data

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 with its completely new, purpose-built file system—the Cohesity SpanFS™—uniquely offers multi-layered protection against a ransomware attack. Among other things, Cohesity delivers the highest level of protection against ransomware attacks because at the foundation it is an immutable file system with read-only state snapshots.

- The immutable file system can take very frequent, unlimited read-only state snapshots and store them with extremely low overhead. The original backup job is kept in an immutable state and is never made accessible, to be mounted by an external system. The only way to mount the backup in read-write mode is to clone that original backup, which is done automatically by the system. Although ransomware may be able to delete files in the mounted (read-write) backup, it cannot affect the immutable snapshot.
- Cohesity SpanFS, the file system, allows you to have a very large number of Views and clone these Views instantly with almost zero-cost in terms of storage utilization.

Preventing unauthorized access to sensitive data is at the heart of Cohesity's protection vision. That's why Cohesity innovation around ransomware prevention extends beyond immutable file system to include:

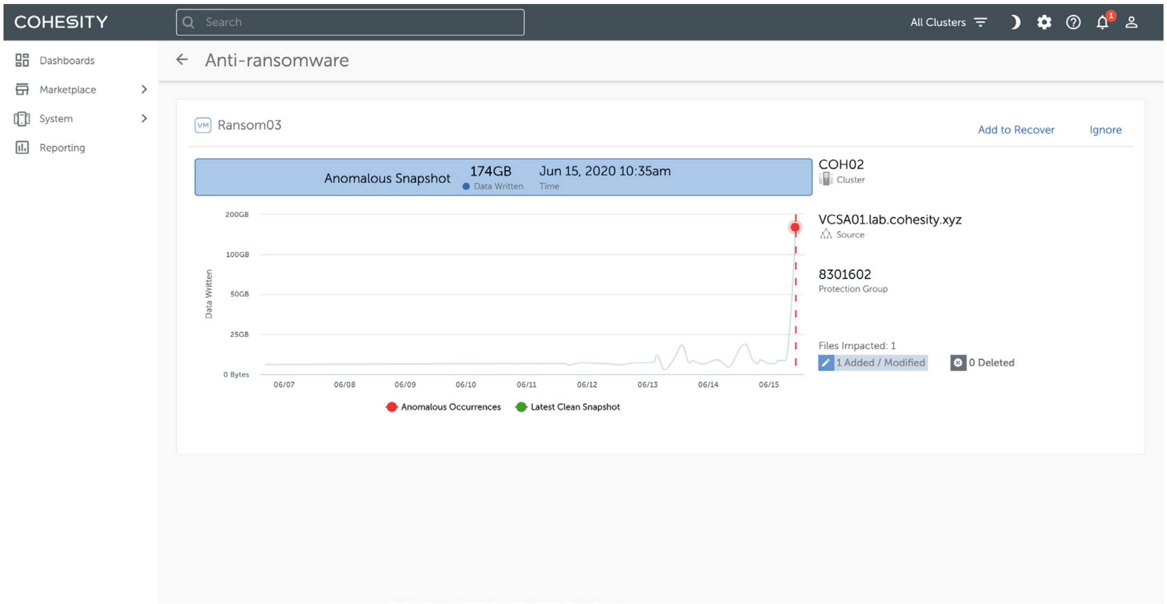
- **DataLock** – WORM capability for backup enables the role-based creation and application of a Datalock policy to selected backup snaps. The security officer role in your organization can use this feature to store snaps in WORM format. The time-bound setting enforcing spans cannot be deleted, even by the administrator or security officer role, providing an extra layer of protection against ransomware attacks.
- Air-gap – Cohesity offers multiple, policy-based methods to isolate your mission-critical data. Based on your organizations unique requirements, you can either replicate or archive data to an external cloud-based target, to another physical location or tape it out to an offsite storage location, like Iron Mountain. The policy-based data replication or archival offers lower RTO and RPO, and flexibility to only maintain network connectivity to another location during the data transfer.
- **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.

Cohesity Helios, a multicloud data management platform delivers a unique combination of an immutable file system with DataLock capabilities, plus policy-based air-gap and MFA to prevent backup data from becoming part of a ransomware attack.

Detect Intruders

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 very 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.

Rapid Recovery

Attacks 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. Cohesity Helios' machine-drive assistance recommends a clean copy of data to perform restore. Alternately, you can leverage the platform's Google-like, 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 gives deep visibility into the health and recoverability status of protected snapshots. CyberScan shows each snapshot's vulnerability index and actionable recommendation to address any software vulnerabilities. This helps you to cleanly and predictably recover from a ransomware attack.

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.

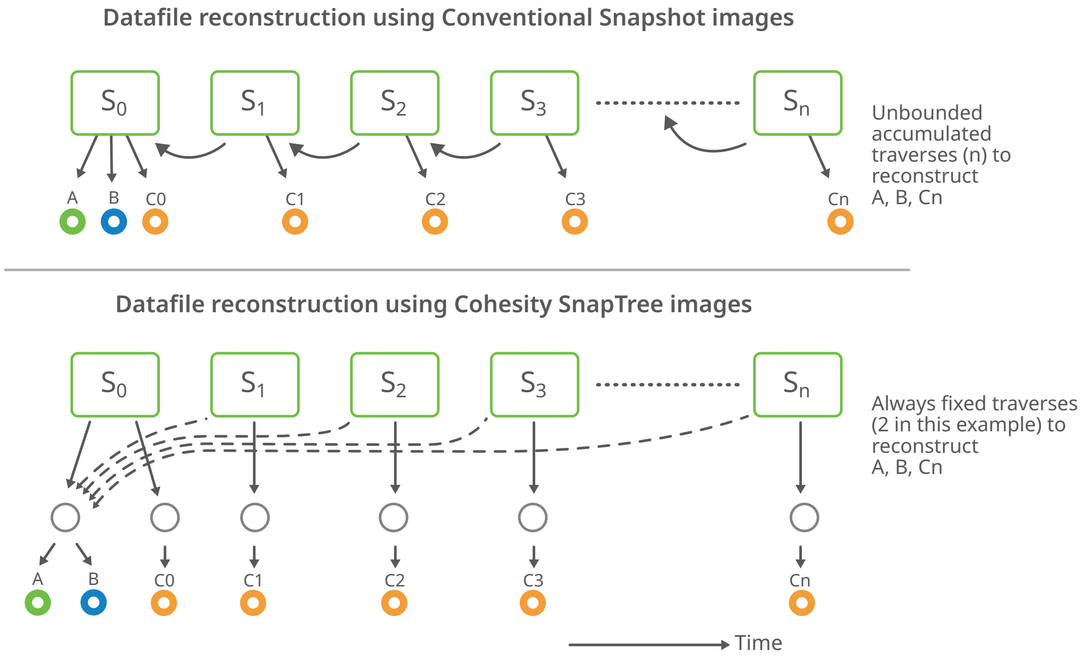

Datafile reconstruction using Conventional Snapshot images
S_0
S_1
S_2
S_3
S_n
A
B
C0
C1
C2
C3
Cn
Unbounded accumulated traverses (n) to reconstruct A, B, Cn
Datafile reconstruction using Cohesity SnapTree images
S_0
S_1
S_2
S_3
S_n
A
B
C0
C1
C2
C3
Cn
Always fixed traverses (2 in this example) to reconstruct 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, isolates, detects, and most importantly, rapidly recovers to reduce downtime and ensure business continuity.

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

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.com | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110

3000015-007-EN 2-2021