COHESITY

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 and integrate with security operations
- Reduce downtime with reliable and rapid recovery

Enterprise Strategy Group found that 79% of organizations have been struck by ransomware, 56% have paid the ransom and only 14% recovered all their data. And ransomware shows no signs of abating. 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, data security and 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.

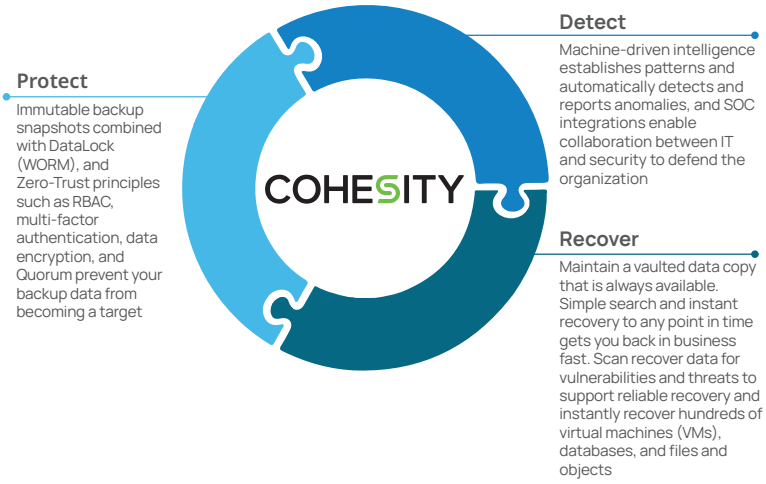

Figure 1: Cohesity delivers comprehensive capabilities to protect, detect and recover from a ransomware attack

[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.

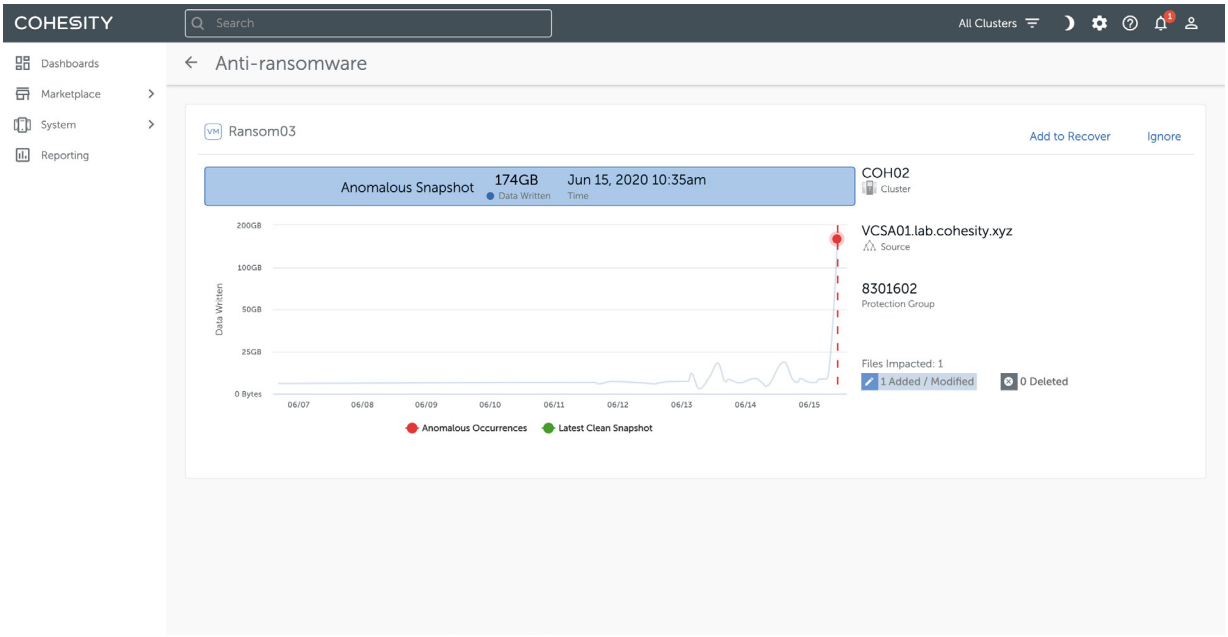

Figure 2: With Cohesity Helios, organizations detect ransomware intrusions

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. Plus with the monitoring of user activity organizations can identify when data usage indicates unauthorized data access and use that could lead to data exfiltration.

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 gathers log data for file-level anomalies within unstructured files and object data. Organizations can review 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 software vulnerability or exposure 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. And organizations can scan snapshots for threats that could reinfect systems after their restoration. Leveraging ML driven threat intelligence, snapshots can be scanned for the latest indicators of compromise (IOCs) that threat actors leverage to gain access to systems, escalate privileges and exfiltrate and encrypt data. To support privacy and industry regulations, organizations need to understand data exposure. Leveraging data classification, organizations can quickly access private and sensitive data that may have been exfiltrated.

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.

COHESITY

Counter Ransomware Attacks with Cohesity

Backup is your first and 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.

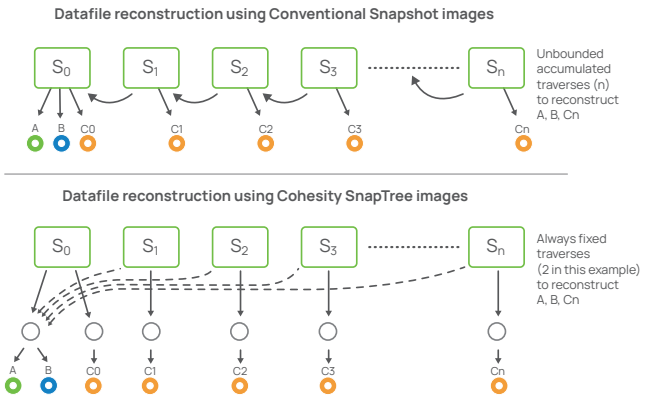

Figure 3: Cohesity patented SnapTree technology delivers unlimited snaps with no overhead, supporting instant recovery at scale

To learn more, visit www.cohesity.com/solutions/ransomware

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

3000015-010-EN 3-2024