Counter Ransomware Attacks with Cohesity

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 per Gartner, "Ransomware families have grown by more than 700% in the last few years"[1], and recovering data from ransomware attacks is expected to cost organizations $11 billion this year[2]. 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 prevent, detect, and respond to a ransomware attack. Cohesity capabilities stop your backup from becoming an attack target. Using machine learning, it provides visibility and continuously monitors for any anomalies in your data. And if the worst happens, Cohesity helps to locate and then deletes infected data across your global footprint, including public clouds, to instantly bring back your data and apps, ensuring business continuity.

KEY BENEFITS

- *Prevent backups from becoming an attack target*
- *Quickly detect anomalies with continuous machine-driven monitoring of primary sources*
- *Recover fast with instant mass restore—on-premises and across multi-clouds*

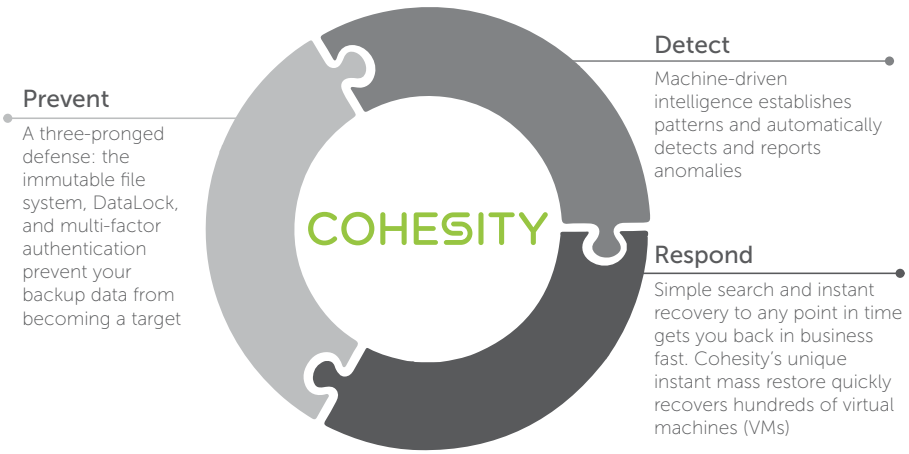

Figure 1: *Cohesity delivers comprehensive capabilities to protect, detect, and respond to ransomware attacks*

1. *Gartner. https://www.gartner.com/smarterwithgartner/protect-your-organization-from-cyber-and-ransomware-attacks/*
2. *Cybersecurity Ventures. https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion*

Prevent Attacks

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 following Cohesity DataPlatform® and Cohesity DataProtect® capabilities enhance protection:

- 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 policies –** WORM-like capabilities for backup enable 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.

- **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 is the only platform delivering a unique combination of an immutable file system with DataLock capabilities, plus 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. Enterprises using **Cohesity Helios®** have a single dashboard to see, manage, and take action fast on their data and applications globally. In the fight against ransomware, Helios machine learning (ML) provides insights humans may miss because it automatically and continuously monitors and notifies you when an anomaly is detected.

Helios 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—Helios machine-driven anomaly detection sends a notification to your IT administrators. Instantly, IT is informed that data changes do not match normal patterns.

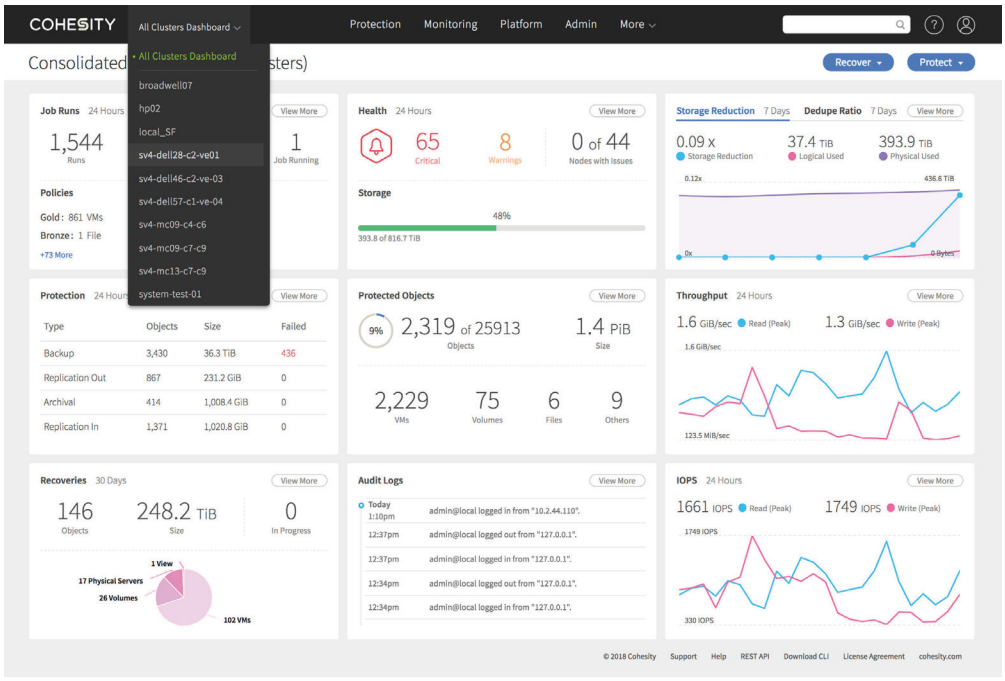

Figure 2: *With Cohesity Helios, organizations detect ransomware intrusions*

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, Helios 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.

Respond Fast

Attacks do happen, and fast. That's why recovery has to be rapid, too. Cohesity speeds the process of getting you back ransomed enterprise data and applications—at scale. Only Cohesity locates and deletes infected files across your global data footprint—including public clouds such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform—and instantly brings back all of your apps and data with unique instant mass restore capabilities. Cohesity searches through Helios and allows you to take corrective action to ensure smooth business continuity.

The scalable DataPlatform stores backup data at the retention rates your organization sets—weeks, months, and years—close to production for fast recovery. Your IT teams can leverage the platform's Google-like, global search capabilities then to quickly locate the data and infected files before taking appropriate corrective actions. This includes finding a malicious file across not just one, but all of your workloads, and deleting it for quick, targeted cleansing. Beyond accelerated response, another benefit of Cohesity's instant mass restore differentiation is to roll back any number of VMs to any previous point in time to ensure business continuity. Cohesity can recover individual virtual machines (VMs), restore files to source VMs, and recover individual application objects.

To speed ransomware recovery, Cohesity simply performs a rapid restore of the latest healthy snapshot. Uniquely Cohesity can instantly restore hundreds VMs to any point in time. Cohesity instant mass restore powers on within minutes because patented Cohesity SnapTree® technology stores each backup as a fully hydrated snap, supporting instant large-scale restoration to any point in time.

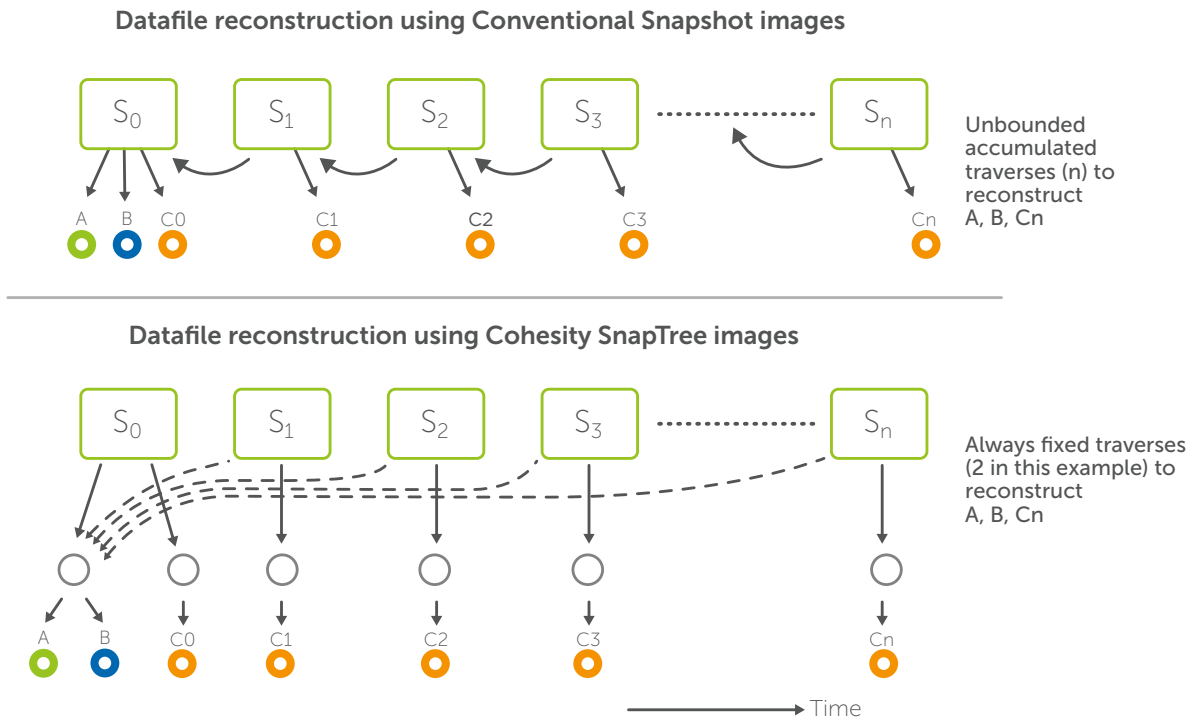

Figure 3: *Cohesity patented SnapTree technology delivers unlimited snaps with no overhead, supporting instant recovery at scale*

Counter Ransomware Attacks with Cohesity

Cohesity's comprehensive approach—to prevent, detect, and respond—to ransomware attacks results in zero data loss and the confidence to refuse to have to make a ransomware payment. Should a breach, disaster, or ransomware attack occur, Cohesity is the only solution to support the instant recovery of hundreds of VMs to bring your business back online. Always-protected backups are available—on-premises or in the cloud—so your enterprise can return to business faster.

Prevent, detect, and respond to ransomware with Cohesity.

Learn more at www.cohesity.com/solution/security-and-compliance/ransomware