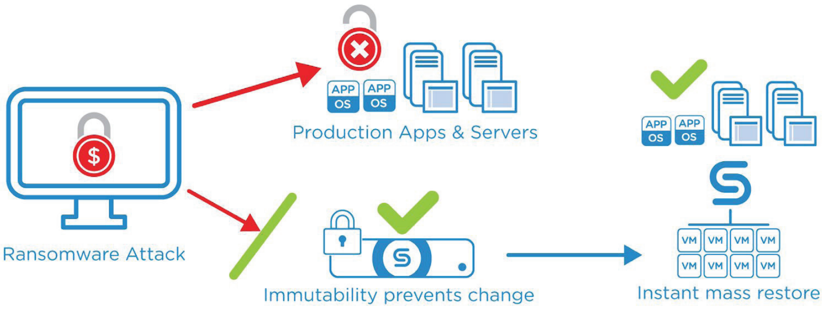
COHESITY

Detect and Protect Against Ransomware

Digital extortion is expected to cost global businesses more than $11 billion by 2019. Analysts predict ransomware will attack a business every 14 seconds by the same year.[1] Although no organization is immune from cybercriminals' attempts to take control of its data, enterprises can do more to mitigate the ransomware threat.

The Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) recommends the following as a best practice when dealing with ransomware: Perform frequent backups of system and important files and verify those backups regularly. If ransomware affects your system, you can restore your system to its previous state with any files unaffected by ransomware.[2]

Cohesity does just that, continuously backing up and verifying the protection of secondary data and applications to ensure organizations can perform a mass restore instantly when a breach happens. Cohesity's simple, fast, and clean approach to ransomware recovery results in zero data loss and the confidence to refuse to have to make a ransomware payment. The unified, web-scale secondary data solution makes always protected backups available—on-premises or in the cloud—so enterprises can instantly go back to any point in time with sub-five second recovery times. Enterprises protected by Cohesity get back to business faster.



Thwart an Attack and Recover Quickly

The Cohesity hyperconverged platform delivers the highest level of protection against ransomware in two significant ways. First, Cohesity writes time-based snapshots into internal views that are never exposed, making them inaccessible to processes and software. During data restoration, Cohesity never exposes internal views, but rather clones the snapshots and only mounts the clones. Should cyber criminals attack the Cohesity platform directly, the ransomware can, at best, change data in a clone or delete files in the user-created view. The malware can never reach the internal view nor touch a true copy of the snapshots. The Cohesity solution to ransomware recovery is as simple as requesting Cohesity to do a rapid restore of the latest healthy snapshot.

Second, Cohesity View is automatically scheduled to take a snapshot after each backup—an operation that takes only milliseconds to complete. In the unlikely event ransomware burrows into the backup repository, Cohesity's patented technology, which includes capabilities leading to extremely high space efficiency, provides an additional layer of protection in the form of Redirect-on-Write. This unique prevention approach stops ransomware should it begin to encrypt and write data back on Cohesity in an attempt to lock it. Cohesity, in response, directs the new write to a new location without modifying the last immutable backup.

Key Benefits

- Thwart ransomware and lose zero data
- After an attack, get back to business fast with instant mass restore that recovers and powers on hundreds of servers in minutes
- Simply and rapidly roll back to any point in time to discover when the malicious code appeared
- Globally search and find the infection across data center systems for fast, targeted cleansing
- Restore systems to previous states with files unaffected by ransomware
- Continuously backup and verify the protection of all secondary data and applications

Instant Mass Restore Gives You the Confidence to Refuse to Make Payments

Attacks happen fast. Recovery must, too. Cohesity speeds the process of getting back ransomed enterprise data and applications—at scale. Cohesity instant mass restore uniquely enables hundreds of servers to be recovered and powered on within minutes because patented Cohesity SnapTree® technology stores each backup as a fully hydrated snap, supporting instant large-scale application restoration to any point in time. Fast, parallel data ingest together with Cohesity zero-cost snapshots and clones ensure RPOs in minutes.

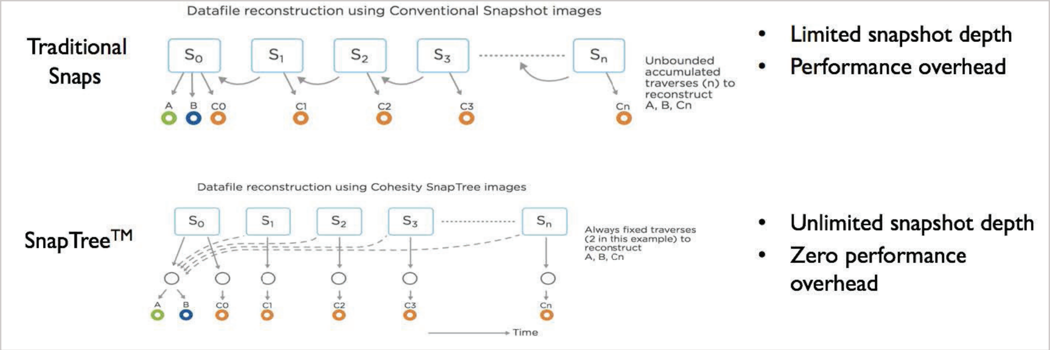

Datafile reconstruction using Conventional Snapshot images
Traditional Snaps
S_0
S_1
S_2
S_3
S_n
A
B
C0
C1
C2
C3
Cn
Unbounded accumulated traverses (n) to reconstruct A, B, Cn
• Limited snapshot depth
• Performance overhead
Datafile reconstruction using Cohesity SnapTree images
SnapTreeTM
S_0
S_1
S_2
S_3
S_n
Always fixed traverses (2 in this example) to reconstruct A, B, Cn
A
B
C0
C1
C2
C3
Cn
Time
• Unlimited snapshot depth
• Zero performance overhead

Fig1. Cohesity patented SnapTree TM technology delivers unlimited snaps with no overhead, allowing for instant recovery at scale.

Another benefit of Cohesity's differentiated ability to enable instant mass restore from any point in time is that rolling back to previous points in time makes it possible for an enterprise to simply and quickly identify when the attack actually took place. Moreover, Cohesity instant global search ensures enterprises can easily hunt down the malicious code rapidly across the entire data center—just one search is needed for quick targeted cleansing. For example, Cohesity Google-like, wild-card search helps instantly locate VMs and files. Cohesity can recover individual VMs, restore files to source VMs, and recover individual application objects. With Cohesity, all data at rest and in transit is encrypted.

Malware Meets Its Match in Cohesity

Ransomware threats fail every time because the true copy of data is still available in Cohesity, ensuring an administrator can easily restore the latest healthy snapshot and obtain forensic evidence of the cybercrime. Cohesity enables an administrator, at no cost, to quickly capture a snapshot of the encrypted Cohesity View. That proof that a crime occurred can then be sent directly to authorities for further examination.

Enterprises rely on Cohesity for both protection and detection of ransomware attacks. Cohesity indexes all backups allowing enterprises deploying Cohesity to effectively preempt ransomware demands by using indexing to verify validity of new backups. Cohesity enables enterprises to detect huge, unexpected changes in incoming data should ransomware be deployed to change underlying data in files rather than changing file names.

Cohesity Defense-In-Depth Security Protections

A single Cohesity platform eliminates the system silos and fragmentation that hackers routinely exploit. Advanced Cohesity capabilities streamline operations while safeguarding secondary data processing and management from backup and recovery to discovery and analytics through policy-driven automation and API integration. Cohesity prevents data loss while ensuring continuity of operations.

Cohesity best practices security standards offer additional enterprise-grade, industry-standard, and government-certified protections:

FIPS 140-2 validated. Always-On Encryption available. TAA compliant. Authorization to Operate (ATO) on DoD networks. WORM Compliant - SEC 17a-4f certification. Common Criteria: EAL 2+ (in process). Secure government cloud integrations (AWS GovCloud, Azure Government Cloud; C2S is ongoing).

Data segmentation, data-at-rest, and data-in-flight protections. Cohesity connects to and provides REST APIs for public clouds including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, as well as any private cloud compatible with S3. Also, data-in-cloud security, independent of data-at-rest encryption. Although Cloud encryption is recommended for public cloud targets, it can be turned off.

Internal Key Management Service (KMS) support, as well as integration with external KMS for encryption key management.

Authentication and authorization, including strong Active Directory integration, multi-factor authentication (MFA), access control lists, mixed-mode role-based access control (RBAC), and comprehensive system and product-level auditing.

Prevent, defend against, and quickly recover from malware intrusions with Cohesity. Learn more at https://www.cohesity.com/security-and-compliance.

[1] Cybersecurity Ventures. https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion

[2] US-Cert. https://www.us-cert.gov/security-publications/Ransomware