COHESITY

SOLUTION BRIEF

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.

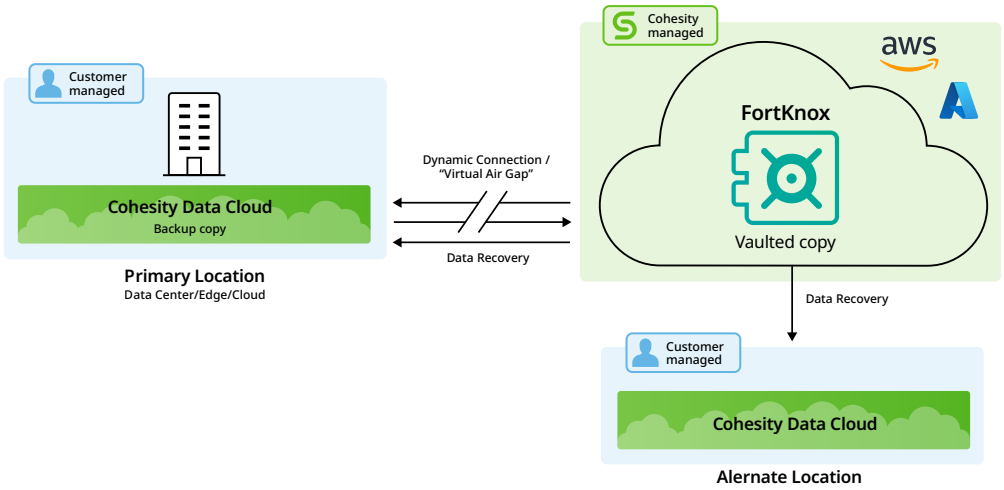

Figure 1: Cohesity FortKnox boosts cyber resilience with data recovery back to the source or to an alternate location.

Learn more at www.cohesity.com

COHESITY