COHESITY

Cohesity FortKnox

Cyber Vaulting and Recovery as a Service

Data powering business operations is more valuable than ever. It is also more vulnerable than ever to cybersecurity threats, power outages and natural disasters. This reality has forced organizations to rethink their approaches to the 3-2-1 strategy of backing up data—three copies of data, on two different media, with one of them in an off-site environment. Although a traditional air gap model where data is stored on magnetic tapes and moved off-site for data isolation ensures data security in the face of increasing ransomware attacks, it impedes rapid recovery which prevents teams from achieving stringent service-level agreements (SLAs). To stay competitive while protecting data, enterprises are embracing a modern 3-2-1 strategy that includes a virtual air gap with physical separation and network isolation and provides both secure and highly available data.

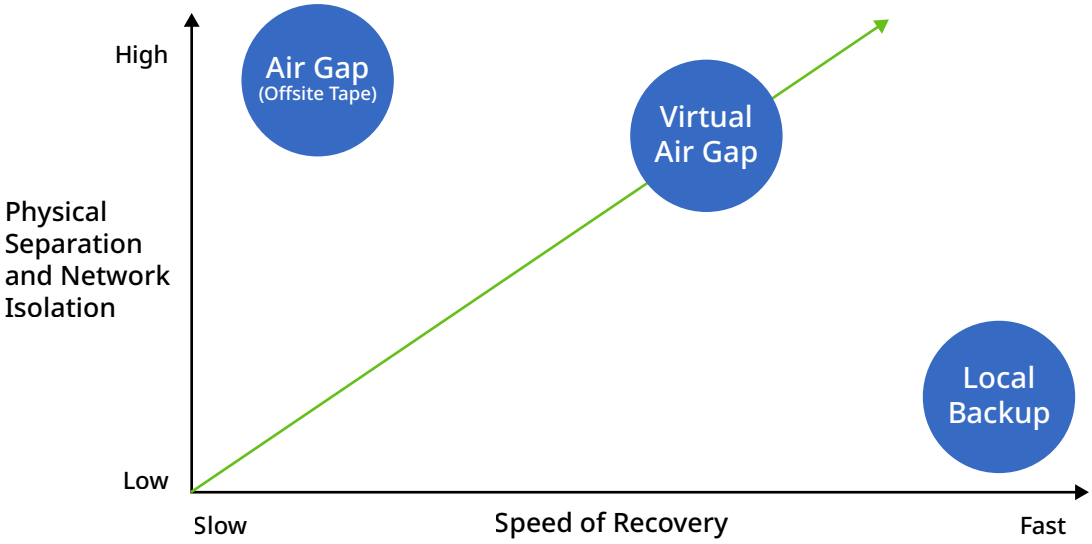

Figure 1: Modern data isolation via virtual air gap balances security and agility

Modern Air Gap for the Cloud Era

Cohesity FortKnox powers a modern 3-2-1 strategy for the cloud era that effectively balances organizations' security and agility priorities. A SaaS cyber vaulting and recovery solution, FortKnox improves cyber resiliency with an immutable copy of data in a Cohesity-managed cloud vault via a virtual air gap. Organizations relying on FortKnox gain an additional layer of security against ransomware and other cybersecurity threats through physical separation, and network and operational isolation. FortKnox dramatically simplifies operations and lowers costs, eliminating the complexity and resource requirements of internally managed isolation solutions. FortKnox is a cloud service empowering organizations to prepare for and recover quickly and confidently from attacks with granular recovery back to the source or an alternate location, including the public cloud. Currently, FortKnox supports data vaulting on AWS and Microsoft Azure.

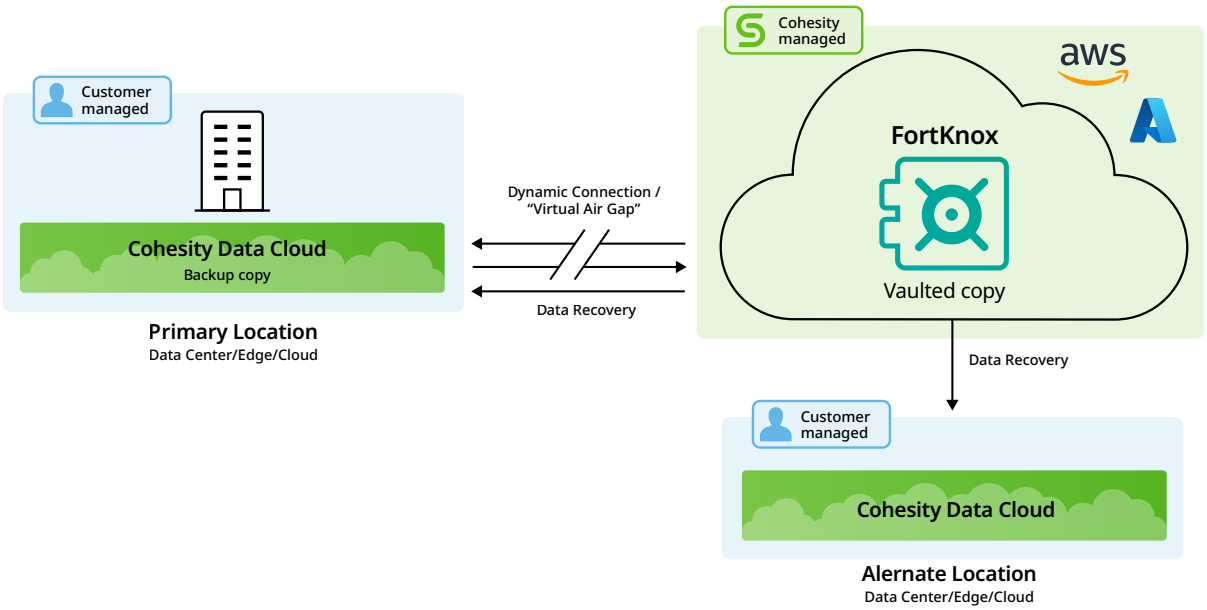

Figure 2: Cohesity FortKnox boosts cyber resilience with data recovery back to the source or to an alternate location

Key Benefits

Managing data vaults on-premises or in the cloud can be complicated and costly for internal teams, particularly as they encounter skills gaps and ever-more destructive ransomware that deletes backups and steals data. FortKnox overcomes these obstacles with a new data isolation technique that improves data resiliency amid rising ransomware attacks.

Additional Protection Layer Safeguards Data and Reputations

FortKnox is an integral part of the multilayered Cohesity Threat Defense architecture built on the notion of least privilege and segregation of duties with granular Zero Trust security principles. It keeps bad actors at bay with advanced access controls and early threat detection capabilities. FortKnox stores an immutable copy of data in a Cohesity-managed cloud vault via a configurable transfer window or virtual air gap and that copy of data is further protected with safeguards. These include role-based access (RBAC), encryption, multi-factor authentication (MFA), a WORM lock policy and a quorum rule that requires at least two employees to approve any critical actions, protecting data from unauthorized access or tampering. FortKnox allows for the management of global data vaults through a single UI and also automatically scans for cybercrimes by monitoring anomalous snapshots.

As-a-Service Consumption Dramatically Simplifies Operations and Lowers Costs

In a pay-as-you-grow service that keeps costs down, FortKnox empowers organizations to simply connect, vault, and recover data. No need to worry about deploying and maintaining "DIY" data vaults or the associated cloud storage or egress costs, as they are covered in the FortKnox subscription. When teams need to safely deposit data to the cloud vault or recover it quickly, Cohesity establishes a temporary and highly secure network connection that limits access to the isolated data by cybercriminals and unauthorized insiders while supporting business SLAs. Teams can leverage FortKnox data vaulting and recovery with customizable protection policies. Not only does FortKnox minimize enterprise attack surfaces, it also reduces the likelihood of a data breach.

Cohesity also provides customers greater flexibility to address varied RTO and budget requirements by providing a choice of FortKnox storage tier options—a warm storage tier for immediate data recoveries, suitable for ransomware protection use cases, as well as a more cost-effective cold storage tier with RTOs of up to 12 hours, suitable for compliance use cases.

Rapid Recovery Saves Time and Improves Business Continuity

FortKnox delivers fast, granular recovery of data back to the source or an alternate location, enabling enterprises to be more agile. Preferred recovery sites may be onsite, a public cloud (e.g., Amazon Web Services, Microsoft Azure, Google Cloud Platform), or an edge location. Since FortKnox prevents vaulted data from being modified, organizations with compromised or lost production data can be confident knowing that they can easily identify and recover an untainted copy of data. In contrast to legacy backup and air gap solutions, FortKnox simplifies the recovery of specific files and objects quickly—without having to restore whole data volumes.

Specifications	
Virtual Air Gap	• Configurable transfer window, outside of which vault is locked from writing into/read access • Vaulted data copy isolated from customer environment with physical separation, and network and management isolation, aka virtual air gap • Isolation from customer's own cloud instance
Immutability	• Irrevocable DataLock (WORM) using AWS S3 Object Lock/Immutable storage for Azure Blob • Read-only snapshots prevents intentional or unintentional modifications or deletions of vault data
Data Security	• Data-at-rest and data-In-flight Encryption • Flexible Cohesity or customer-managed KMS • Quorum controlled recoveries to minimize data exfiltration vectors
Access Control	• Multi-factor authentication • Granular role-based access control • Quorum for critical actions including recoveries • Short-lived token based authentication to access vault • Authenticated API call-based access over HTTPS • Access limited to authorized Cohesity clusters only
Ransomware Detection	• Machine learning-based anomaly detection and reporting
Rapid Recovery	• Machine driven recommendation of clean snapshot for faster incident response • Quick, granular recovery back to source or alternate location to meet stringent SLAs
As a Service Consumption	• SaaS solution that's as simple as connect, vault and recover • Data vaulting and recovery with customizable protection policies • Pay as you go consumption model based on back-end TB (BETB) usage • No additional cloud storage or egress costs
Public Cloud Availability	• Supports data vaulting to AWS and Microsoft Azure (*Warm Vault only; Cold Vault coming soon*)
Flexible Storage Classes	• Warm Storage Tier for recovery that starts immediately upon customer initiation, and a minimum 30-day retention period. • Cold Storage Tier for recovery that starts 4 hours after customer initiation, and a minimum retention period of 90 days or longer.
Single Pane of Management	• View and manage global data vaults with centralized dashboard • Simplified administration with SLA-based policies

COHESITY

sales@netxinc.com 866-638-9462
www.netxinc.com/cohesity 609-298-9118