Lab Insight Report

Validation of Cohesity FortKnox

Cloud-Based Data Vaulting for Ransomware Resiliency

By Krista Macomber, Senior Analyst

and Randy Kerns, Senior Strategist

February 2023

Evaluator Group

Enabling you to make the best technology decisions

Introduction

The practice of air gapping – that is, storing tertiary backup copies in a storage environment that is isolated from the production and primary backup environments – has long been implemented by IT Operations as a best practice within their backup and broader data protection strategies. These isolated backup environments have become even more necessary with the rise of ransomware attacks, and attacks from malicious insiders such as rogue administrators. In the event that a malicious actor accesses the production or primary backup environment, they cannot access the air gapped copies. As a result, the air-gapped storage provides a clean copy of data that can be recovered from.

As more customers look to implement air-gapped storage for a larger component of their data environments, and as they look for easier accessibility and faster time-to-recovery, customers are looking beyond the tape storage solutions that traditionally have served as the air-gapped storage repository. Many have begun implementing cloud-based "data vaults." In fact, Evaluator Group's recent **Trends in Enterprise Data Protection** study showed that approximately one in five enterprises are using the public cloud as an isolated/air-gapped storage repository.

Background for Cohesity Data Vaulting

Cohesity FortKnox is a software-as-a-service (SaaS) offering for data vaulting. Like **DataProtect**, Cohesity's flagship backup and recovery offering, FortKnox is delivered as a data service supported on Cohesity Data Cloud, its data protection and security platform.

In 2021, Evaluator Group monitored detailed demonstrations performed by Cohesity, to verify DataProtect's effectiveness when it comes to ransomware protection and recovery. The version of Cohesity's software tested was 6.5.1c. The full results of this test are included in the paper, ***Validation of Cohesity Accelerated Recovery from Ransomware***. Drawing on this knowledgebase and the correlations and integrations with DataProtect, Evaluator Group has conducted a subsequent evaluation focused on FortKnox and the ability to vault data, specifically.

In response to this growing customer requirement, a number of data protection vendors have introduced cloud-based data vaulting solutions. However, these solutions are not all created equal and should be evaluated for access and security controls, as well as cost-efficiency and performance.

Validation of Cohesity FortKnox

FortKnox Overview

Today, customers require a self-managed instance of Cohesity DataProtect running Cohesity software release version 6.8 or later, for the primary backup copy to be vaulted into FortKnox. In the evaluation, Cohesity demonstrated to Evaluator Group how an administrator created and assigned backup policies in DataProtect, that facilitate the automatic creation of the copies that are vaulted to FortKnox.

Validation of Cohesity FortKnox

FortKnox sends a replica of the backup data to an AWS-hosted storage target that has physical separation, as well as network and operational isolation, from both the production and backup environments. Cohesity leverages cryptographic protocol TLS 1.2 for secure communications over the network. All data transmitted between the backup environment and cloud vault is encrypted with AES-256 cipher. Administrators set and control the vaulting window, and they can enable or disable vaults as needed, but cannot delete the vault. FortKnox supports vaulting of **a variety of data sources** including VMs, databases, files, and objects.

Data could be vaulted to multiple targets, including vaults in different regions if desired. It is also worth noting that, as an additional measure for security and isolation, the customer does not need to use their own AWS login, thereby isolating the vault from their own AWS instance.

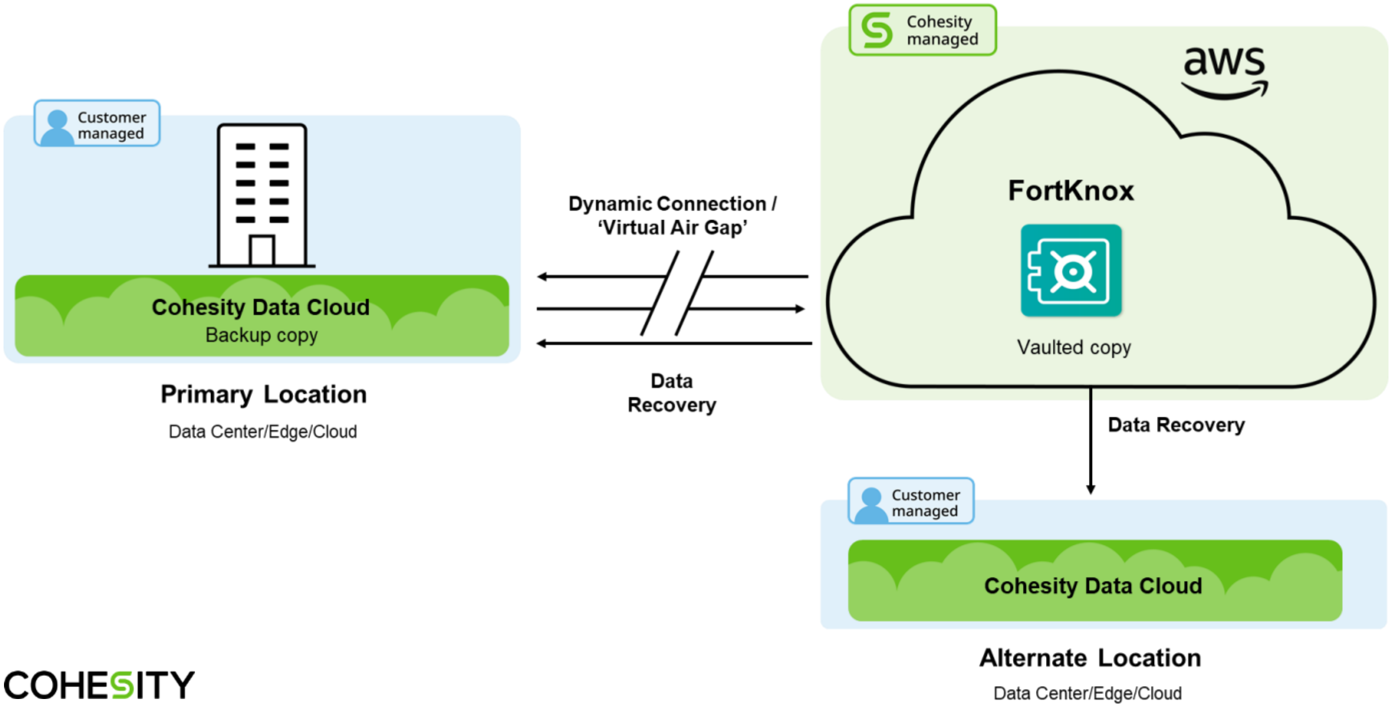

Figure 1: Cohesity FortKnox Architecture

Customers have two options for the back-end AWS storage target:

- The first option, Cohesity FortKnox Warm Storage Tier, leverages Amazon Simple Storage Service Standard Infrequent Access (S3-IA). This option uses instantaneous data access to start recovery immediately upon customer initiation, and it carries a minimum data retention period of 30 days.

- The second option, Cohesity FortKnox Cold Storage Tier, leverages Amazon S3 Glacier Flexible Recovery (FR). It is a lower-cost option, but recovery begins four hours after customer initiation due to the data hydration that is required to access data from the cold tier. It carries a minimum data retention of 90 days.

Supporting more than one tier provides customers with the ability to make tradeoffs between cost, recovery times, and retention periods, as appropriate. With both options, customers benefit from the same enhanced data security features of FortKnox, including virtual air gapping, immutability, role-based access control (RBAC), quorum, multi-factor authentication (MFA) and a Cohesity key management system (KMS), that are discussed further in this document.

Management and Recovery Options

As observed by Evaluator Group, the dedicated FortKnox user interface provides visibility into the status of protection jobs, and storage resource consumption over time. It also allows administrators to identify the objects they wish to recover, using a global search functionality that supports wildcards. Once the desired object is selected, administrators can then identify and select their desired recovery point – including from which cluster the object is recovered from. Cohesity Helios, the SaaS-based control plane that is common to all Cohesity services, uses machine learning to identify a clean copy of data for recovery. Data can be recovered to the original location or to an alternate one, including public or private cloud. For instance, the existing virtual machine (VM) can be overwritten, or it

Summary of Validated Capabilities

- Ability to oversee designation for vaulting via DataProtect policies.
- Ability to control vaulting target and vaulting window via FortKnox UI.
- Ability to control recovery operations via FortKnox UI. This includes determining what is recovered, and where it is recovered to.
- Visibility into protection jobs and storage resource consumption via FortKnox dashboard.
- Utilization of Helios to identify clean data copies for recovery
- Cohesity Instant Mass Restore and granular recovery capabilities
- Immutability through AWS Object Lock
- End-to-end encryption
- Creation of Quorum Groups and designation of admin responsibilities, and the approval process by the second admin. This includes validating that an admin cannot be the secondary approver on their own request.
- Audit logging and review as well as alerting via the FortKnox dashboard.
- Data cataloging and global search.
- Identification of anomalous behavior and the last backup prior to the behavior.
- Scanning snapshots of VMs against known vulnerabilities.

can be retained for forensics purposes. FortKnox Warm Tier also supports granular recovery of specific files and folders without having to recover whole objects. These capabilities allow for faster recovery times, and they enable customers to recover to a location that they know is clean.

Data vaulted to Cohesity FortKnox can be recovered to the original on-premises Cohesity cluster or, if the original cluster is not available, customers can deploy a new cluster for recovery. Customers have two options – Cohesity Instant Mass Restore (IMR), and copy-based recovery.

- The IMR option makes recovered VMs available for use as soon as data is pulled down from the vault to the self-managed Cohesity DataProtect backup cluster. In this instance, VMs are powered on in the customer's primary environment using a temporary data store from the Cohesity platform, a live storage vMotion is conducted in the background to the primary storage, and ultimately the temporary data store is cleaned up and removed. Note that the IMR option is available only for VM workloads.
    - In its evaluation of DataProtect, Evaluator Group observed Cohesity provide access to cloned copies of the VMs and power on 100 VMs in less than three minutes with locked down networking after restoring from the vault to the customer managed cluster. This allows for a mass number of VMs to be inspected before being restored back into the production environment, and it can reduce business downtime resulting from a cyber-attack.
- In copy recovery, the recovered VMs are available for use after the data pulled down from the vault gets moved from the Cohesity cluster to the customer's primary environment.

Secure Data Transfer and Network Segmentation

Data is encrypted (specific details included in the Encryption and Immutability section of this report) and directly transmitted from the customer cluster to the AWS S3 infrastructure hosting the vault. The data transfer happens over HTTPS which is a stateless protocol, and the connection is severed after each call to AWS S3. The vaulting window is static, and customers have the flexibility to configure the vaulting window per their business needs.

FortKnox leverages AWS PrivateLink capabilities to provide private connectivity between virtual private clouds (VPCs), AWS services, and on-premises networks, without exposing network traffic to the public internet. Using AWS PrivateLink, the on-premises Cohesity software can communicate privately with Amazon S3 for storing and retrieving backup data. Cohesity assigns each FortKnox customer their own dedicated Amazon S3 bucket, and it employs network segmentation to isolate access to data and applications to specific private and public subnets, security groups, and network access control lists.

> ***"With limited staff being a top issue facing IT operations teams, SaaS-delivered solutions like FortKnox allow data vaulting practices to be implemented without the hassle of managing infrastructure and key security features such as access control. The most significant value-adds of FortKnox specifically include the ability to choose between two back-end storage targets, the option for both granular and mass recoveries, and Cohesity's Quorum two-person concurrence and full data cataloging and search capabilities."***
>
> **-Krista Macomber,**
> **Senior Analyst, Evaluator Group**

Access Control and Quorum

As another method of protection against rogue internal administrators, and to separate access from other Cohesity clusters, Cohesity manages access control including mandatory MFA, granular RBAC, and short-term token-based authentication. There is no option in the Cohesity management interface or in Cohesity's APIs for a customer or hacker to delete a vault, and no Cohesity employee is allowed to delete licensed customer vaults for any reason. Access to the FortKnox vault on Cohesity's side is restricted to two senior individuals— the Senior Director and Senior Manager of Cloud Operations— who both require Okta validation to perform any actions on the vault. In the event that a customer cancels their FortKnox subscription, Cohesity handles the deletion of the FortKnox target (with the customer having the option to pull their data off first).

For additional security, FortKnox includes a "Quorum" feature that makes it necessary for at least two authorized administrators at the customer end to approve changes to, or to recover data from, the vault (also known as the four eyes principle). During demonstrations, Evaluator Group observed that, using RBAC, administrators are assigned the rights/privileges of what they can approve or deny, and "quorum groups" are created. For example, specific quorum groups of two or more admins may be set up for specific clusters. This process is controlled by the "super-admin" function, with the approval of a second administrator. The "super-admin" is a Cohesity construct that is responsible for assigning each user their role and managing the unique permissions that are associated with each role, across Cohesity DataProtect clusters and other data services including FortKnox. This role was evaluated in detail in **Evaluator Group's lab validation of DataProtect**. In essence, the Quorum capability is an evolution of the two-person concurrence that is required for executing critical operations in FortKnox, that is also detailed in Evaluator Group's DataProtect Lab Validation.

As demonstrated to Evaluator Group, once a quorum group has been created, each member of the applicable group receives a notification to review the action that has been done. Members can add comments with their approval or denial, for communication. Requests can be automatically approved or denied after a certain number of hours or days; changes to these rules must be approved by at least one other member of the quorum group. All requests and attempts are logged and reviewable via the FortKnox dashboard.

Encryption and Immutability

All customer data sent to the vault is encrypted while in transit and, using the AWS Key Management System (KMS), at rest. Customers can bring their own encryption key, or they can have their encryption key managed as-a-service by Cohesity. The latter helps to protect against rogue administrators internal to the customer's organization.

Cohesity automatically applies DataLock, its Write Once Read Many (WORM) capability that is based on the AWS Object Lock feature, to the replicas vaulted to FortKnox, in order to make them immutable (for an in-depth analysis of Cohesity's capabilities for immutability, please refer to **Evaluator Group's lab validation of DataProtect**). There are two forms of AWS Object Lock – Compliance Mode, which does not allow for any administrator tampering, and Governance Mode, which allows administrators to adjust retention holds. The Governance Mode lock is applied to FortKnox data because Compliance Mode would not allow Cohesity to adjust the retention period if it is accidentally set to be too long, or if the client terminates their service before the end of the retention hold. Because of this, it is possible that FortKnox (or any other solution using the Governance Mode AWS Object Lock) will not meet requirements for customers that must meet regulations such as SEC 17a-4.

Analytics and Machine Learning

Through the FortKnox user interface, administrators can access Cohesity DataProtect's analytics, machine learning and data cataloging capabilities to uncover anomalous/suspicious activity that could indicate a cyberattack, and to identify which systems and data stores have been impacted by a cyberattack. For example, these capabilities allow administrators to identify a clean copy of data for recovery by monitoring data change rates indicating suspicious behavior. This can help customers to mitigate the impact and spread of an attack, to accelerate recovery, and to prioritize what to respond to and what to recover first. For forensics purposes, administrators can dig into specific snapshots. FortKnox also includes audit logging and full inventory reporting, with the ability to both export and schedule reports. Additionally, audit logging information from FortKnox can be integrated into security operations tools like Splunk SIEM to support analytics on the broader IT environment.

A customer concern with ransomware analytics tools is becoming inundated with alerts on "false positives" – incidents that Cohesity reports as anomalous, that are not in fact malicious activity. In order to mitigate false positives, Cohesity built a feedback mechanism into its ransomware anomaly detection engine. Once an anomaly has been identified and reported on the anomaly dashboard, admins choose to recover the object, or they can choose to ignore the anomaly, indicating a false positive alert. This feedback is used as input for the anomaly detection engine, which then uses artificial intelligence to ensure that such alerts are not triggered for 30 days. Additionally, ransomware anomaly information from the platform can be integrated into security operations tools like Cisco SecureX, Cortex XSOAR which can greatly accelerate threat detection and response and decrease an organization's risk exposure.

Operational Simplicity

In being cloud-delivered, FortKnox allows for agile and streamlined consumption of data vault infrastructure services. Customers can bypass the hassle of self-managed data vaults, which burden in-house IT teams that are already stretched thin. It also helps to shift from large CapEx to more transactional OpEx purchasing. Cohesity includes egress fees and the price of the underlying cloud storage infrastructure in its licensing, which increases the solution's predictability in terms of cost.

Summary

In today's tide of malicious internal and external attacks, including ransomware, customers are faced with the burden of needing to isolate or vault a growing amount of data. They are also pressured to mitigate business downtime, in the event that they are hit with an attack and need to recover from vaulted data. To address these needs, many customers are looking to public cloud storage to obtain an isolated data vault, without the cost and complexity associated with maintaining and upgrading tape storage infrastructure, and potentially to accelerate recovery times.

While a "do-it-yourself" approach is possible when it comes to setting up and managing a cloud-based data vault, this approach lacks the added security capabilities necessary within today's threat landscape. Cohesity FortKnox offers customers an "as-a-service" solution to data vaulting that includes by default security features such as immutability, isolation, encryption, access control, tamper resistance, and more, while enabling a path to faster deployment and implementation as well as simplified management. Offloading these tasks to Cohesity through the FortKnox service can save customers money from an operational expense perspective, as well as valuable IT staff time, which is at a premium. Customers can also save on cloud storage and data egress fees, which can quickly become very expensive, because they are included alongside compression and deduplication as a part of the FortKnox subscription. The ability to choose between two back-end storage targets provides customers flexibility to balance their budget with recovery time and retention requirements. For example, choosing the "warm" storage tier can speed up recovery times especially compared to on-premises tape. Cohesity's Instant Mass Recovery capability can furthermore accelerate recovery times following a cyber-attack. Cohesity brings data cataloging, search and analytics capabilities to the table that support granular recoveries (for the Warm Storage Tier option) and ransomware forensics. Meanwhile, FortKnox brings a host of security capabilities to the table, including a Quorum capability for two-person concurrence, that help to protect the data in the vault.

About Evaluator Group

Evaluator Group LLC, an Information management and data storage analyst firm, has been covering systems for over 20 years. Executives and IT Managers rely upon us to help make informed decisions to architect and purchase systems supporting their data management objectives. We surpass the current technology landscape by defining requirements and providing an in-depth knowledge of the products as well as the intricacies that dictate long-term successful strategies.