

# Mapping HKMA STDB Characteristics to Cohesity

How Cohesity addresses all 9 Secure Tertiary Data Backup (STDB) characteristics defined by the Hong Kong Monetary Authority (HKMA)



## TABLE OF CONTENTS

|                                                 |   |                      |    |
|-------------------------------------------------|---|----------------------|----|
| Executive summary                               | 3 | 04: Secure           | 7  |
| Cohesity Platform security overview             | 4 | 05: Control          | 7  |
| HKMA STDB 9 characteristics – Cohesity coverage | 5 | 06: Verifiable       | 8  |
| Detailed mapping                                | 6 | 07: Assurance        | 8  |
| 01: Immutable                                   | 6 | 08: Heterogeneous    | 8  |
| 02: Survivable                                  | 6 | 09: High Performance | 8  |
| 03: Air-Gapped                                  | 6 | Compliance summary   | 9  |
|                                                 |   | Conclusion           | 10 |

# Executive summary

The Hong Kong Monetary Authority (HKMA) requires all regulated financial institutions to maintain a Secure Tertiary Data Backup (STDB)—an independent, cyber-resilient data vault that remains recoverable even when primary and secondary systems are destroyed. This is a compliance mandate with nine defined characteristics that institutions must demonstrably satisfy.

Cohesity meets this mandate through a zero-trust data platform built to survive the attacks that defeat

conventional backup infrastructure. Immutability, air-gapping, end-to-end encryption, least-privilege access, and dual-authorization controls are architectural principles baked into every deployment.

The result is a single, auditable platform that satisfies all nine HKMA Data Vault Characteristics, delivers documented RTO/RPO evidence for board and regulatory review, and turns a compliance requirement into genuine operational resilience.

# Cohesity Platform security overview

Cohesity’s Threat Defense Architecture places Data Resiliency at the core - encryption, immutability, and fault tolerance—surrounded by Zero Trust controls (MFA, RBAC, Quorum, Auditing), Detection and Analytics (near real-time anomaly detection with AI/ML, data classification,

adaptive behavioral analytics), and deep integrations with leading Security platforms (SIEM/SOAR, identity management, key management, and vulnerability management).

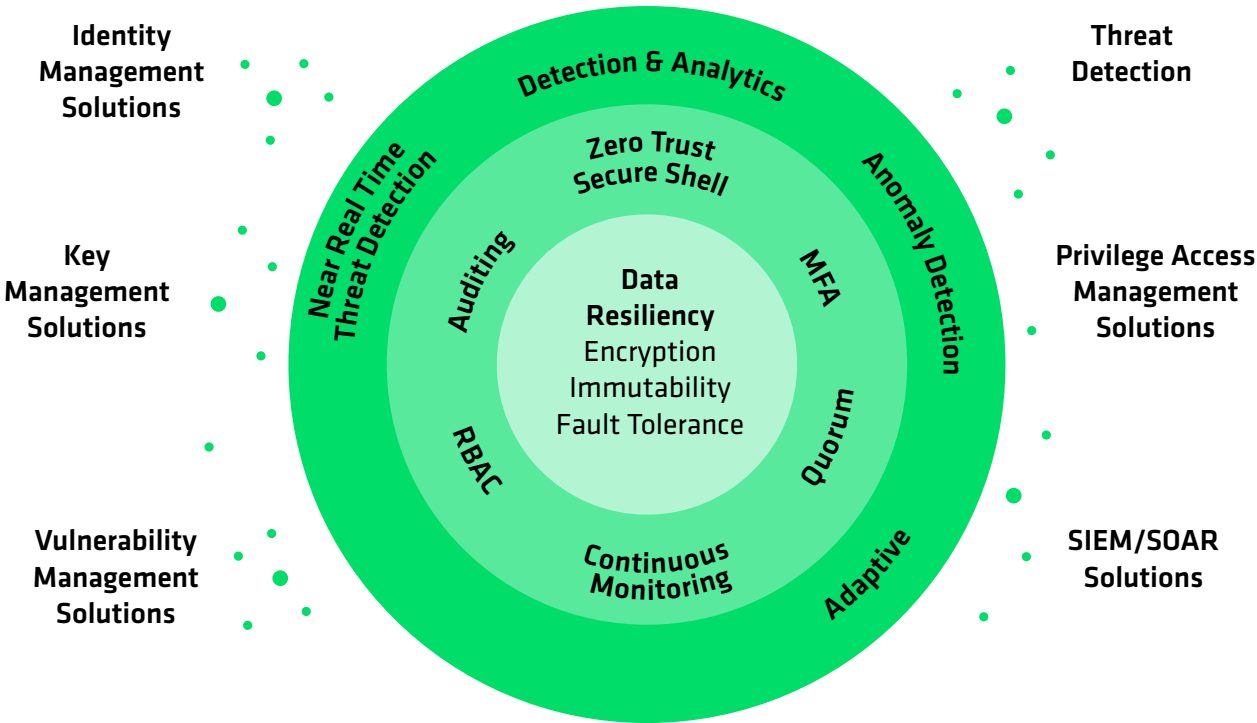
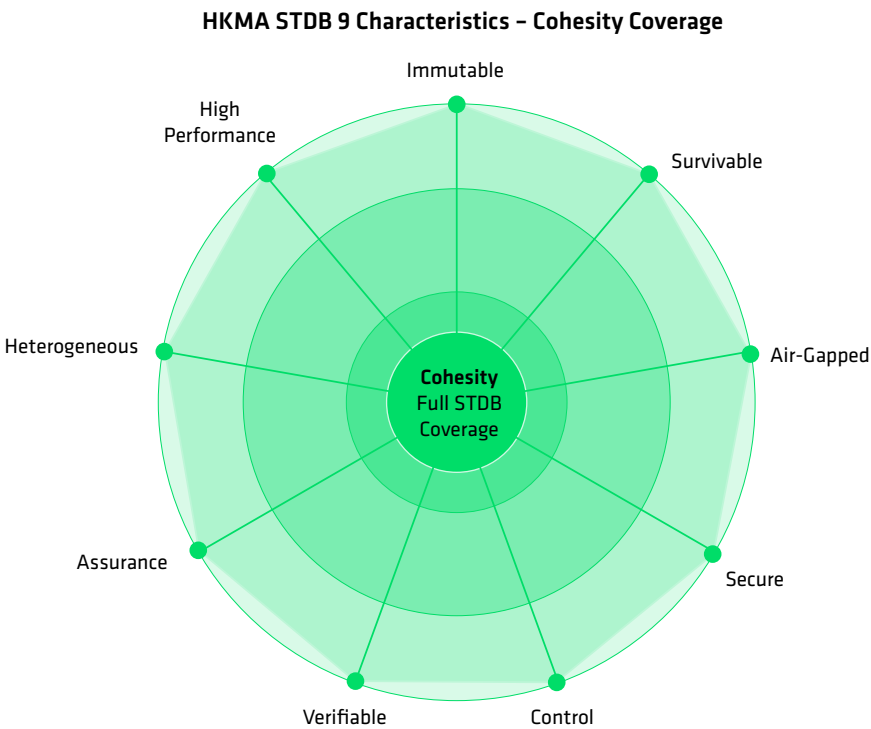


Figure 1: Cohesity Threat Defense Architecture - Data Resiliency at core, Zero Trust ring, Detection and Analytics outer ring, and Security Integration ecosystem (2024-2025)

# HKMA STDB 9 characteristics – Cohesity coverage

Financial institutions must demonstrate compliance across all nine STDB pillars. The diagram below shows how Cohesity satisfies every characteristic—all 9 spokes are shown in the wheel on the left with Cohesity capability cards on the right.



All 9 HKMA STDB data vault characteristics satisfied – Cohesity Zero Trust Platform • [cohesity.com](https://cohesity.com)

Figure 2: HKMA STDB Data Vault - All 9 Characteristics fully covered by Cohesity Zero Trust Platform (wheel left, capability cards right)

| #  | Characteristic   | Core Requirement                                                                                          |
|----|------------------|-----------------------------------------------------------------------------------------------------------|
| 01 | Immutable        | Data cannot be altered or deleted during the defined retention period                                     |
| 02 | Survivable       | Backup survives destructive cyber-attacks and disasters                                                   |
| 03 | Air-Gapped       | Isolated from primary and secondary environments with no persistent network connectivity                  |
| 04 | Secure           | Strong access controls, identity management, and encryption must protect all STDB data                    |
| 05 | Control          | Centralized, auditable governance and change management must span all STDB environments                   |
| 06 | Verifiable       | Data integrity must be continuously verifiable throughout the full retention chain                        |
| 07 | Assurance        | STDB must enforce dual-authorization controls and deliver board-level RTO/RPO evidence                    |
| 08 | Heterogeneous    | STDB must present a fundamentally different technology stack and attack surface from production           |
| 09 | High Performance | STDB must deliver high-throughput ingestion and rapid large-scale recovery within defined RTO/RPO windows |

# Detailed mapping

The following sections address each of the nine HKMA STDB characteristics in detail, describing the specific requirement, its compliance significance, and how Cohesity directly satisfies it.

## 01: Immutable

**Requirement:** *Data cannot be changed or erased during the defined retention period.*

**Why It Matters:** Ransomware and insider threats can destroy or encrypt backups, rendering recovery impossible.

### How Cohesity Addresses This

Cohesity DataLock enforces WORM retention at both the cluster and policy level. Retention periods are cryptographically enforced—no admin override, no API bypass possible.

|                            |                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DataLock (WORM)</b>     | Policy-driven Write-Once-Read-Many with Compliance and Enterprise modes. Once set, retention locks cannot be shortened—even by administrators. |
| <b>Immutable Snapshots</b> | Every backup snapshot is immutable by default. Snapshots are point-in-time, append-only, and cannot be modified in-place.                      |
| <b>SpanFS File System</b>  | Purpose-built distributed file system enforces immutability at the storage layer, independent of the management plane.                         |

## 02: Survivable

**Requirement:** *STDB must maintain a long clean backup history that survives destructive attacks on primary and secondary systems.*

**Why It Matters:** If ransomware destroys all backup copies, recovery is impossible—only a surviving tertiary copy guarantees continuity.

### How Cohesity Addresses This

Cohesity DataProtect maintains granular historical snapshots with policy-driven retention. FortKnox provides an immutable, air-gapped cloud vault that remains intact even if all on-premises infrastructure is compromised.

|                        |                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>DataProtect</b>     | Granular, policy-driven snapshot retention (hourly to yearly) across on-premises and cloud—always a clean copy available. |
| <b>FortKnox Vault</b>  | Immutable, air-gapped cloud vault (AWS / Azure) ensures at least one copy survives even total on-premises compromise.     |
| <b>Security Centre</b> | ML-driven anomaly detection identifies earliest clean restore point—guaranteeing a survivable copy from before infection. |

## 03: Air-Gapped

**Requirement:** *STDB must be logically or physically isolated from all other environments with no persistent network connectivity.*

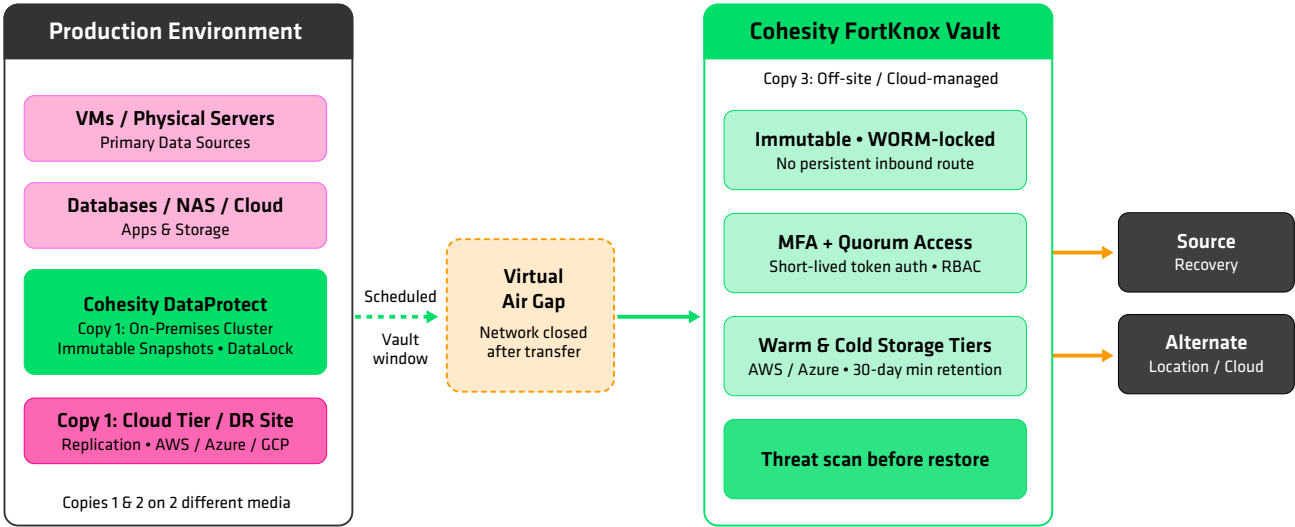
**Why It Matters:** Backups reachable from production can be encrypted by ransomware—a true airgap removes this attack vector entirely.

### How Cohesity Addresses This

FortKnox operates as a fully air-gapped vault—data is ingested on a configurable schedule, and the network path closes after transfer, leaving no persistent inbound route to the vault.

|                              |                                                                                                                                     |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>FortKnox Cyber Vault</b>  | Fully air-gapped SaaS vault on AWS/Azure. Network closes after scheduled vault window - zero persistent inbound route.              |
| <b>CloudArchive</b>          | Policy-driven archival to cloud object storage with configurable connectivity windows - logical air-gap with auditable access logs. |
| <b>Isolated Recovery Env</b> | Network-isolated sandbox to validate backups without re-exposing data to production networks.                                       |

Cohesity FortKnow – Modern Cyber Vault Architecture (3-2-1 Strategy)



3-2-1 Rule: 3 copies of data | 2 different media | 1 off-site in FortKnox vault (virtual air-gap, immutable, isolated)

Figure 3: Cohesity FortKnox - Modern Cyber Vault Architecture implementing the 3-2-1 strategy with virtual air-gap and threat scanning (2024-2025)

04: Secure

**Requirement:** Strong access controls, identity management, and encryption must protect all STDB data from unauthorized access.

**Why It Matters:** A single compromised admin credential can silently delete or encrypt all backups, voiding years of data protection.

How Cohesity Addresses This

All data is encrypted at rest (AES-256) and in transit (TLS 1.3). Granular RBAC with AD/LDAP/SSO and mandatory MFA protect the management plane. Quorum Authorization requires multi-person approval for all sensitive operations.

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Encryption AES-256/TLS | Data encrypted at rest (AES-256-CBC) and in transit (TLS 1.3). Keys via built-in KMS or external KMIP-compliant KMS.     |
| RBAC and MFA           | Granular Role-Based Access Control with AD/LDAP/SSO. MFA enforced for all management plane access. No service backdoors. |
| Quorum Authorization   | Sensitive operations require approval from a configurable quorum—prevents single-credential compromise.                  |
| Audit Logs and SIEM    | Immutable audit trails with real-time anomaly alerts and SIEM integration (Cisco XDR, CrowdStrike, MS Sentinel).         |

05: Control

**Requirement:** Centralized, auditable governance and change management must span all STDB environments and operations.

**Why It Matters:** Distributed silos create blind spots; centralized control enables rapid, consistent policy enforcement across all vaults.

How Cohesity Addresses This

Helios provides a single management plane with full visibility across all clusters and vaults. The Policy Engine automates RPO, retention, encryption, and replication targets.

|                           |                                                                                                                           |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Helios Central Management | Unified policy-based management plane across all clusters and cloud vaults. Full SLA visibility and compliance reporting. |
| Policy Engine             | Automated backup policies enforce RPO, retention, encryption, and replication targets. Compliance is built-in.            |
| Threat Scanning           | Deep scanning of backup contents before restoring—detects malware and ransomware signatures before production promotion.  |

# 06: Verifiable

**Requirement:** Data integrity must be continuously verifiable throughout the full retention chain, from ingestion through restoration.

**Why It Matters:** Corrupted backups discovered only at recovery time make restoration impossible when it matters most.

## How Cohesity Addresses This

Threat Intelligence Anomaly Detection continuously analyses backup metadata and data entropy using ML models. Cryptographic checksums stored at ingest detect bitrot or tampering.

|                                |                                                                                                                          |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Anomaly Detection</b>       | ML models flag unexpected entropy changes (ransomware signatures) or deletion anomalies near real-time.                  |
| <b>Cryptographic Checksums</b> | Checksums stored for every object at ingest. Any bitrot or tampering detected automatically across full retention chain. |
| <b>Backup Validation</b>       | Automated recovery verification mounts backup in isolated environment and runs configurable health checks.               |

# 07: Assurance

**Requirement:** STDB must enforce dual-authorisation controls and deliver board-level RTO/RPO evidence to satisfy regulators.

**Why It Matters:** Regulators require documented proof of recoverability; untested or unaudited backups fail to satisfy this obligation.

## How Cohesity Addresses This

Quorum Authorization directly implements the two-man rule. Recovery Agent delivers automated runbook-driven DR with documented RTO/RPO execution logs.

|                             |                                                                                                                                  |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Quorum Authorization</b> | Multi-person approval workflow for all restore invocations, policy modifications, and vault access—implements STDB two-man rule. |
| <b>Recovery Agent</b>       | Automated runbook-driven DR with defined RTO/RPO. One-click failover with auditable execution logs.                              |
| <b>Helios SLA Reporting</b> | Real-time dashboards confirming backup success rates, RPO adherence, and recovery readiness for regulators.                      |

# 08: Heterogeneous

**Requirement:** STDB must present a fundamentally different technology stack and attack surface from production environments.

**Why It Matters:** Identical platforms share exploitable vulnerabilities—a heterogeneous stack eliminates common ransomware attack paths.

## How Cohesity Addresses This

Cohesity runs SpanFS—a purpose-built distributed file system—presenting a fundamentally different attack surface from typical Linux/Windows-based production environments.

|                              |                                                                                                                           |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>SpanFS Purpose-Built</b>  | Cohesity runs its own distributed file system—different attack surface from Linux/Windows-based production systems.       |
| <b>Hardened SpanOS</b>       | Immutable OS image with STIG controls, FIPS cryptography, default firewall, and no SSH shell access by default.           |
| <b>50+ Workload Coverage</b> | VMware, Hyper-V, AWS, Azure, Oracle, SQL Server, SAP HANA, Kubernetes, M365 - heterogeneous across all production stacks. |

# 09: High Performance

**Requirement:** STDB must deliver high-throughput ingestion and rapid large-scale recovery within defined RTO/RPO windows.

**Why It Matters:** Slow restores extend outages and risk breaching regulatory recovery time commitments during a live incident.

## How Cohesity Addresses This

SpanFS's scale-out architecture supports massively parallel ingest and restore. Instant Mass Restore enables recovery of thousands of VMs simultaneously via direct NFS/SMB mount from backup snapshots.

|                             |                                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>SpanFS Scale-Out</b>     | Linearly scalable distributed file system. Adding nodes increases capacity and performance simultaneously—no bottlenecks.  |
| <b>Instant Mass Restore</b> | Restore 1000s of VMs simultaneously—near-zero RTO via instant NFS/SMB mount directly from backup snapshots.                |
| <b>Global Deduplication</b> | High data reduction ratios reduce storage footprint and network bandwidth, accelerating backup windows and restore speeds. |

# Compliance summary

The mandate raises the bar for data resilience across Hong Kong’s financial sector. Cohesity’s zero trust platform delivers certified compliance today, with the

operational resilience to protect your institution against tomorrow’s threats.

| Characteristic   | HKMA Requirement                     | Cohesity Solution                       | Key Capability                        |
|------------------|--------------------------------------|-----------------------------------------|---------------------------------------|
| Immutable        | Cannot be altered during retention   | DataLock / Immutable Snapshots          | WORM - no admin override              |
| Survivable       | Survives destructive cyber-attacks   | DataProtect / FortKnox / Security Ctr   | Deep retention + clean restore point  |
| Air-Gapped       | Isolated, no persistent connectivity | FortKnox / CloudArchive                 | Virtual airgap; scheduled ingest only |
| Secure           | Access control, identity, encryption | Encryption / RBAC / Quorum / MFA        | Multi-layer zero-trust access control |
| Control          | Centralized auditable governance     | Helios / Policy Engine / Threat Scan    | Central governance + pre-restore scan |
| Verifiable       | Integrity validated throughout chain | Threat Intelligence / Checksums         | ML anomaly detection + crypto verify  |
| Assurance        | Dual-auth + board-level RTO/RPO      | Quorum / Recovery Agent / Helios SLA    | Two-man rule + automated DR runbooks  |
| Heterogeneous    | Different stack from production      | SpanFS / SpanOS / DataProtect           | Purpose-built OS + FS                 |
| High Performance | MPP + fast recovery at scale         | SpanFS Scale-Out / Instant Mass Restore | Near-zero RTO for 1000s of VMs        |

# Conclusion

The HKMA STDB mandate requires a platform built from the ground up around the assumption of breach. Cohesity satisfies every dimension - from immutable, air-gapped storage and AI-powered threat intelligence, to granular RBAC with quorum-enforced dual authorization and massively parallel recovery at petabyte scale.

By consolidating compliance across all nine characteristics into a single, auditable platform, Cohesity helps financial institutions not only meet the HKMA requirement, but demonstrate it—to regulators, boards, and auditors - with documented RTO/RPO evidence and continuous operational assurance.

Learn more at [Cohesity.com](https://cohesity.com)

© 2026 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

## COHESITY

[cohesity.com](https://cohesity.com)

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

2000087-001-EN 5-2026