Commvault®

WHITE PAPER

# Mastering Cyber Resilience: Fortifying Your Commvault® Data Protection Infrastructure

Commvault

# Table of Contents

## INTRODUCTION

In today's increasingly hostile cyber threat landscape, cyber resilience requires more than just reliable data backup; it demands a hardened, secure infrastructure that helps meet compliance requirements. As ransomware and data-wiping attacks grow in complexity, organizations leveraging Commvault must implement a defense-in-depth strategy that spans physical, OS, and application layers, including secure configuration of the Commvault platform itself. Many leading industry reports reinforce the need for layered security architectures to support rapid, scalable recovery.

This guide outlines architectural, operational, and procedural controls to fortify Commvault environments with emphasis on cyber recovery readiness, policy-driven governance, and alignment with regulatory frameworks such as NIST CSF, ISO/IEC 27001, HIPAA, GDPR, and CMMC. These controls support technical resilience, auditability, data privacy, and compliance with growing industry and government mandates.

This guide targets IT, data protection, and resiliency administrators who manage Commvault Cloud environments. It presents best practices for protecting your Commvault environment and your data from cyber threats, ransomware, and malicious attacks. This covers both high-level concepts and practical, built-in features like multi-factor authentication (MFA), multi-person authorization (MPA), and ransomware protection. These functions are ready for immediate activation to strengthen your defenses.

## 1. INFRASTRUCTURE AND SECURITY FOUNDATIONS

Cyber resilience begins with a strong foundation. This section details how to build a hardened infrastructure for your Commvault environment. Beyond the physical and operating system layers, the software running on that infrastructure, including Commvault itself, must also be rigorously secured and configured for defense.

### 1.1 Physical Server Deployment

**Recommendation:**

STRATEGIC INFRASTRUCTURE HARDENING IS YOUR FIRST LINE OF DEFENSE AGAINST EVOLVING CYBER THREATS.

- Deploy your Commvault infrastructure, including the central control plane, data plane, and storage on dedicated physical infrastructure within your on-premises data centers for the utmost resilience.
- Isolate and continuously monitor management interfaces such as Integrated Lights-Out and Dell Remote Access Controller, as these often-overlooked components can present significant attack vectors if not properly secured. Configure MFA to further improve the security posture.
- Prevent the risk of simultaneous compromise by using unique credentials and isolated networks for production environments, disaster recovery (DR) sites, and cyber recovery (CR) sites.
- Establish a geographically separate DR site with dedicated physical infrastructure to host a standby control plane, maintained through Commvault's Live Sync replication.
- Encrypt Commvault's control plane databases with SQL TDE and configure strong authentication for additional security (e.g., SQL Server, PostgreSQL).

**Rationale:**

- Minimized Attack Surface: Physical infrastructures inherently reduce the attack surface compared to virtualized environments, which can be susceptible to hypervisor compromise and lateral movement from a compromised production virtual environment.
  - Significantly higher number of IT environment compromises today are because of VM escape attacks by malicious actors where they break away from the confines of the VM to gain unauthorized access to the host system or other VMs on the same hardware. With the entire VM landscape destroyed, data protection landscape if hosted on virtual instances can also be affected and rendered inaccessible. By deploying data protection control and data planes on physical infrastructure, much of impact from this method of attack can be mitigated.
- Consistent Performance: Dedicated physical resources deliver predictable and consistent performance. This is crucial for high-demand recovery operations.

**Benefits:**

- Maintains data protection infrastructure isolation and operational status even if the virtualized production environment is compromised.
- Reduces dependencies on potentially compromised hypervisors.

Pro Tip: Validate the robustness of your architecture and the operational readiness of your DR procedures with conducting quarterly failover tests between primary and DR Commvault sites by leveraging both physical server environments. The same approach holds true for CR recovery tests as well.

Note: DR failover testing and CR testing need to be treated independently as the expected outcomes and deliverables from each are different.

## 1.2 Hardened Operating Systems

**Recommendation:**

MINIMIZE YOUR ATTACK SURFACE BY ADOPTING HARDENED OPERATING SYSTEMS.

- Leverage CIS-hardened L1 operating system images such as Commvault VaultOSTM operating system for Commvault managed instances or other OS images from cloud hyperscaler marketplaces for all Commvault data protection infrastructure deployments.
- Perform regular vulnerability scanning on both the operating system and the Commvault application in environments in collaboration with IT and Security teams. Use configuration management tools to enforce hardening measures at scale.
- Monitor and log OS-level events, and forward logs to a SIEM for centralized analysis and alerting.
- Avoid generic or unhardened public cloud images.
  - Configure security for Commvault's control plane and data plane.
  - Limit network port exposure: Restrict Commvault services to only essential ports, using internal firewalls or Commvault's network topology settings.
  - Disable unnecessary features/roles: Review and disable any Commvault features or roles not actively used in your environment. Audit access of all systems including Commvault environment frequently.
  - Implement strict service account permissions: Run Commvault services with the minimum necessary permissions.
    - Follow our updates and deploy promptly.
    - Disable Windows Administrator ability to create shares on the data plane.
    - Local user accounts should remain independent and must not be integrated with Active Directory.
    - Enable ransomware protection on all data plane mount paths. This secures the mount path to protected data and internal databases of the data plane components of Commvault from access by external non-Commvault processes.

**Rationale:**

- Minimized Attack Surface: Purpose-built or hardened OS images provide a reduced attack surface by disabling unnecessary services, closing open ports, and implementing secure configurations by default. This foundational OS hardening creates a secure base for all deployed applications, including Commvault.
- Protection of OS: Given the increased targeting of Linux environments by cyberattacks, a rigorously hardened OS is critical for defending against evolving threats and hosting secure data protection software.
- Unified Defense Layer: The Commvault application is the core of your data protection and must also be configured to resist attacks and operate in a highly secure posture. This complements the underlying hardened OS, creating a unified defense layer.

**Benefits:**

- VaultOS operating system for Commvault managed instance deployments offers CIS Level 1 hardening, SELinux restricted process access, controlled auto-patching, read-only partitions, and built-in deletion protections, directly contributing to a secure-by-design posture. Certification for CIS Level 2 hardening is in progress.
- Use Linux across the control plane and data plane for a consistent and inherently hardened environment.
- Implement these hardened OS recommendations with secure Commvault software configurations to create a robust, multi-layered defense.
- Existing Windows control plane deployments can be migrated to Linux images as part of hardware refresh, accelerating hardening efforts.

Architect's Note: Hardware Refresh cycles create an opportunity to shift Commvault control plane from Windows to Linux.

## 1.3 Commvault HyperScale Appliances (X, Flex, Edge)

**Recommendation:**

STREAMLINE DEPLOYMENT WITH PURPOSE-BUILT APPLIANCES TO BOOST SECURITY FROM DAY ONE.

- Leverage Commvault's HyperScale appliances for a streamlined, integrated, and hardened approach to securing data protection infrastructure.
- Change default credentials on all appliances immediately upon deployment, and do not expose management interfaces to public networks.
- Do not integrate local Commvault user accounts with Active Directory.
- Disable root logins to enhance security. Manage break-glass local user accounts through Privileged Access Management (PAM) or Privileged Identity Management (PIM) solutions.

**Rationale:**

- Reduced Vulnerability Exposure: These appliances incorporate hardened VaultOS images, minimizing the infrastructure's exposure to known vulnerabilities.
- Automated Management: Automated patching and management processes offload the operational burden of manually maintaining system updates.

**Benefits:**

- Minimize the risk associated with unpatched systems.
- Simplify overall data protection infrastructure management to free up valuable IT resources and reduce operational complexity.
- HyperScale X: Recommended for hyperconverged architectures where storage and compute are integrated, providing a scale-out approach to data protection.
- HyperScale Flex: Designed for high-performance scenarios, integrating with high-performance external storage solutions like Pure Storage All-Flash or VAST Data.
- HyperScale Edge: A single-node architecture suitable for dispersed or remote locations such as retail stores, branch offices, and remote manufacturing sites.

## 2. ENCRYPTION & KEY MANAGEMENT

### 2.1 External Key Vault Integration

**Recommendation:**

DECOUPLE CRITICAL SECRETS TO ELEVATE YOUR SECURITY POSTURE.

- Commvault's built-in key management server (KMS) provides the first layer of security through encryption of data at rest and in flight. Integrate with an external KMS or key vault solutions (e.g., Azure Key Vault, AWS Key Management Service) to manage the lifecycle of encryption keys, and PAMs (e.g., CyberArk Beyond Trust) for storing passwords, encryption keys, and other critical credentials used by the Commvault control plane.
- Lock key vaults and monitor them for suspicious activity. Rotate the storage of encryption keys regularly and maintain a documented key rotation policy.

**Rationale:**

- Decoupling Secrets: Enforce the security of your primary identity management system by storing encryption keys remotely, separate from the Commvault control plane and potentially from your main Active Directory. This can reduce the likelihood of having your primary identity system and your encryption keys being simultaneously compromised.
- Enhanced Security Posture: This adheres to industry best security practices by externalizing critical encryption keys management.

**Benefits:**

- Create an isolated tenancy for the key vault that is independent of the Active Directory. This enhances security of your critical encryption keys against exposure to potential Active Directory breaches.

Pro Tip: Schedule periodic tests on external key vault connectivity and access to validate key availability for data protection and recovery operations.

### 2.2 Key Management Best Practices

**Recommendation:**

PROACTIVE KEY MANAGEMENT PRACTICES FORTIFY DATA AGAINST CURRENT AND FUTURE THREATS.

- Separate public and private keys.
- Document key recovery procedures and test them regularly. Encrypt and securely store data protection repositories, ideally in a separate location.
- Avoid direct authentication access to key vaults via Active Directory.
- Control access to key vaults via just-in-time (JIT) access mechanisms.
- Your organization should plan for crypto-agility and prepare for post-quantum cryptography (PQC). Commvault supports Key Encapsulation Mechanism (KEM) using PQC by leveraging NIST-approved algorithms like CRYSTALS-Kyber and hybrid quantum-classical (HQC) to support future-proof data protection efforts.
- Implement encryption for storage pools. This secures data stored at rest within these pools, over and above the data encryption provided by Commvault's built-in KMS.
- Encrypt passwords for Commvault application user accounts using the built-in key management service or a third-party key management server.

**Rationale:**

- Key Security: These measures provide additional layers of security against unauthorized access or manipulation of encryption keys.
- Crypto-agility: Early planning for crypto-agility is critical. This requires thorough inventory creation and management of IT assets and applications that can benefit from crypto agility. Learn how Commvault helps protect data from post-quantum security threats.

**Benefits:**

- Commvault's built-in encryption algorithms encrypt data in transit and at rest. Data encryption at rest should utilize AES-256. We recommend using Commvault encryption in addition to encryption at the storage layer. This provides additional data protection for on-prem and cloud workloads.
- Encryption keys for data protection are stored in the control plane and protected by the external key vault mechanism. The external component is a crucial security control. Further, evaluating your environment for crypto agility contributes to your organization's compatibility with PQC requirements for safe and secure data transmission.

## 3. IDENTITY AND ACCESS CONTROL

### 3.1 Isolated Data Protection Infrastructure Domains

**Recommendation:**

CREATE A CRITICAL SECURITY BOUNDARY BY SEGMENTING IDENTITY SERVICES.

- Deploy the Commvault infrastructure within a dedicated Active Directory domain that has no trust relationships with your production Active Directory. Alternatively, use local user credentials that are independently managed by a Privileged Access Management (PAM) solution.
- Regularly review and audit privileged account usage to detect and prevent unauthorized activities. Consider implementing Privileged Access Workstations (PAWs) to provide a secure environment for administrative access.

- Implement stringent access control measures within this isolated domain.
  - Change default SQL and Commvault administrator account names with strong, unique values.
  - Enforce minimal default privileges for all accounts.
    - Do not allow persistent administrative privileges on data plane or the control plane.
    - Utilize JIT administrative elevation with automated revocation for all privileged access requests.

**Rationale:**

- Prevention of Lateral Movement: Isolating the data protection domain prevents attackers from moving laterally across a compromised production domain into the critical Commvault environment.
- Mitigation of Insider Threats: These address scenarios involving rogue administrators attempting to delete or corrupt protected data.

**Benefits:**

- Limit the impact of a compromised production Active Directory.
- Commvault provides workflows to counter the use of compromised Active Directory credentials for data-destructive Commvault API operations for additional security against data aging, dropping libraries, or data deletion.

## 3.2 Restrict Access and Enable Multi-Person Authorization (MPA)

**Recommendation:**

ROBUST ACCESS CONTROLS AND MPA BLOCK INSIDER THREATS AND COMPROMISED CREDENTIALS.

- Restrict Commvault's Command Center and API command line access to corporate-authorized devices. Prohibit personal device access to Commvault infrastructure. This helps reduce the surface areas of attack.
- Log all privileged actions and review them regularly to identify potential security issues. Consider integrating with a SIEM to enable real-time alerting on privileged operations.
- Service providers can whitelist tenant IP addresses to restrict access to the Command Center and APIs. This helps prevent abuse and malicious activity if credentials are compromised.
- Require MPA for destructive actions such as deletion of jobs, plans, libraries.
- Require MPA for restore operations.
- Enforce Level 3 password complexity for local accounts. This requires a minimum of twelve characters with at least two uppercase letters, two lowercase letters, two numbers, and two special characters.
- Implement a 90-day password rotation policy for all system accounts used by the data protection tool.
- Mandate MFA for every login to Commvault administrative interfaces. Commvault provides support for CAC, FIDO2 and Yubikey.
- Implement an account lockout policy. For example, user accounts will lock after 3 failed log-on attempts for a duration of 5 minutes. You can customize these settings to meet your needs.
- Configure Command Center to time out after 15 minutes of inactivity. You can customize this setting to meet your needs.
- Require user authentication for agent installation. This prevents unauthorized agents from connecting to the data protection environment.
- The restrictions can also be extended to API users to limit access to consoles.
- Implement continuous monitoring and set alerts to report multiple failed login attempts.

**Rationale:**

- Secure Against Unauthorized Users: These measures collectively prevent unauthorized access and malicious actions, especially in cases of compromised credentials or insider threats.
- Layer Protection with MPA: MPA is increasingly critical as sophisticated attackers often target APIs for data-destructive operations.
- Early Detection: Timely detection of failed logins can signal brute-force or credential stuffing attacks.

**Benefits:**

- MPA requires consensus for destructive operations, providing a critical layer of defense.
- Mandatory password rotation reduces the risk of long-term compromise.
- Multi-factor authentication (MFA) adds a crucial layer of authentication security, making unauthorized access more difficult.

## 4. DATA PROTECTION & COMPLIANCE

### 4.1 Compliance Lock

**Recommendation:**

APPLY DATA FOR STRONGER DEFENSE AGAINST MALICIOUS DELETION.

- Enable Compliance Lock across all critical Commvault environments to prevent the reduction of retention periods or the deletion of libraries.
- Document the process for requesting and approving changes to retention policies and require MPA for modifications.

**Rationale:**

- Data Integrity and Forensics: This feature preserves crucial evidence for post-incident investigations and supports regulatory compliance by preventing data from being deleted before its required retention period.
- Protection Against Malicious Deletion: It acts as a safeguard against malicious or accidental shortening of data retention periods, which could lead to the loss of critical recovery points.

**Benefits:**

- Compliance Lock prevents alteration of retention periods for cloud copies so that retention periods cannot be shortened and libraries cannot be deleted.

### 4.2 Multiple Data Protection Copies

**Recommendation:**

TRADITIONALLY THE PHILOSOPHY HAS BEEN TO ADOPT 3-2-1-1-0 RULE FOR ROBUST DATA PROTECTION BASED ON ASSET CRITICALITY.

- 3 copies of your data
- 2 different storage media
- 1 copy stored offsite
- 1 copy is immutable/air-gapped
- 0 errors (via verification)

Pro Tip: In most cases, especially cloud deployments where cloud networking costs such as inter-regional and cross-cloud egress charge may apply, it may be prudent to make the necessary adaptations so that at least 2 copies are maintained with immutability and indelibility.

- By Asset Criticality:
  - Production Systems: Maintain at least two copies of this data in two distinct locations.
  - Critical Systems (Tier 0/1): For the most critical applications requiring recovery within the first hour of an attack, maintain a minimum of three copies in three distinct locations (production site, DR site, cloud, or an isolated immutable site).
  - Dev/Test Environments: Protect at a lower frequency or retain for a shorter retention period based on their business impact.
  - Endpoints/Desktops/Laptops: Store these data copies in the lowest-tier storage appropriate for endpoint recovery needs.
  - Excluded Assets: Utilize Commvault's automatic client groups to classify and tag assets that do not require protection for cost or compliance considerations.
- By Storage Target and Recovery Objective:
  - Production Data: Use scale-out storage solutions like Commvault HyperScale X or a variety of supported storage arrays for primary data copies, depending on the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) SLAs of the data when catering to operational recovery or disaster recovery scenarios. For cyber recovery scenarios, a reliable and fast underlying infrastructure helps restore data rapidly to an IRE for data validation purposes.
  - Critical Data (Tier 0/1): Utilize all-flash storage arrays (e.g., Pure Storage, VAST Data) with Write Once, Read Many (WORM) capabilities at the storage tier level.
  - WORM Locking: Commvault strongly advises enabling WORM locking on all critical storage repositories where Commvault data is placed to prevent accidental or malicious deletion.
  - Cloud Storage: Use public cloud storage that is in a different tenant or cloud platform from your own cloud platform or tenant. This allows air gap and immutability abstracting of administrator access to the storage container when it is on a completely different tenant. Commvault's Air Gap Protect is available to customers using Azure, AWS and OCI cloud platforms.
  - Tape: Use tape for ultra-critical, irreplaceable data such as source code and financial records.

Architect's Note: Tape is not recommended for data that demands frequent, high volume rapid restores. Hence, understanding the restore profile of data from protected copies is critical. Answering questions such as how often data is recovered, how much data is recovered and how rapidly the data is required to be restored each time, are key to architecting for the achieving right business outcomes.

- Maintain auxiliary copies across diverse locations.
  - Use a dedicated disaster recovery site.
  - Leverage cloud environments with Active Directory separation.
  - Create at least one copy that is immutable and physically or logically air gapped.
- For the most critical assets, maintain at least four copies: two in production, one in an offsite location, and one in the cloud, and/or on tape.
- Regularly test restores from each storage type to verify recoverability.
- Ensure that air-gapped copies remain truly offline and are not accessible through any network connection.

**Rationale:**

- Multi-Pronged Approach: This multi-pronged strategy provides high availability and superior resilience against various failure types and sophisticated cyberattacks.
- Reduce Risks for Active Directory: An Active Directory compromise could potentially lead to the deletion of data protection repository in cloud/hyperscalers.

**Benefits:**

- All-flash storage provides super-fast, multi-stream restores.
- Cloud storage provides off-site logically separated repositories, especially if the copies of data reside on a different cloud tenant further bolstered with object-level locking mechanisms.

### 4.3 Retention Rules

**Recommendation:**

STRATEGIC RETENTION POLICIES ARE VITAL FOR COVERING BREACH DETECTION WINDOWS AND FORENSIC NEEDS.

- Retain all production data protection for a minimum of 30 days.
- Review retention policies at least bi-annually for alignment with business needs and regulatory requirements.
- Retain cloud copies and Active Directory data for a minimum of 90 days.

**Rationale:**

- Breach Detection Window: The average breach detection window can exceed 23 days. Therefore, retention periods shorter than 30 days are insufficient for adequate protection.

**Benefits:**

- Longer retention periods provide a broader window for comprehensive recovery and forensic analysis, which is crucial in today's threat landscape.

## 5. RECOVERY PREPAREDNESS

### 5.1 Regular Failover Testing for the Control Plane

**Recommendation:**

**Proactive failover testing converts recovery plans into proven capabilities.**

- Conduct quarterly failover testing between primary and DR control plane sites.
- Document findings from each test and update procedures to continuously improve processes and resilience. This involves full validation of failover procedures and confirming that all dependencies (DNS, certificates, network connectivity) are functional and correctly configured.

**Rationale:**

- Operational Readiness: Regular testing confirms your ability to quickly shift operations to a DR site if a primary site is hit with an outage or compromise.

**Benefits:**

- The alternate site is consistently ready. The failover process is smooth and well-understood by the team. This minimizes potential downtime during a real incident.

## 5.2 Cleanroom™ Recovery Tests

**Recommendation:**

CLEANROOM RECOVERY TESTING PROVIDES A PRISTINE PATH TO BUSINESS CONTINUITY.

- Simulate full-stack recovery in isolated cleanroom environments. These environments should include:
  - An isolated Active Directory (or a replica)
  - An external Key Management System (KMS)
  - Critical Tier 0/1 applications
  - Scanning, monitoring and forensics tools
  - Relevant SIEM/SOAR tools
- Regularly update cleanroom environments to reflect changes in production systems. Consider involving third-party incident response teams in at least one annual test to enhance preparedness and gain external perspective.
- Safeguard the latest verified OS and application binaries by maintaining them in isolated offline storage such an Azure file share accessed by a physical USB key not connected to the corporate Active Directory, or a secure, air-gapped vault.
- Maintain a sandbox environment for creating and validating the latest golden images of your operating systems, complete with updated patches and necessary software. This supports high-velocity validation of hardened instances for recovery.

**Rationale:**

- Reinfection Prevention: Practice and refine the recovery process for critical systems in an environment completely isolated from the production network, preventing re-infection from persistent threats.
- Access to Binaries: In a ransomware scenario, a complete loss of production access necessitates readily available and clean binaries for environment reinstallation.

**Benefits:**

- Quarterly cleanroom recovery of critical assets rotating between cloud, tape, and DR copies supports versatility and proven capability in recovery options.
- Cleanroom testing needs to be isolated from your production environment.
- Utilize pre-defined break-glass accounts managed by a Property Management System (PMS) and a third-party KMS within the cleanroom.
- Mandatory malware scanning of data within the cleanroom supports clean recovery and can prevent the reintroduction of malware.

## 5.3 Leverage "Commvault Validate Restore"

**Recommendation:**

AUTOMATED VALIDATION TRANSFORMS PROTECTED DATA STORED IN REPOSITORIES INTO VERIFIABLE, RECOVERABLE ASSETS.

- Utilize the Commvault Validate Restore feature for scheduled mock restores to test recovery times and confirm data readability without overwriting live environments.
- Automate the reporting of test results to relevant stakeholders.

**Rationale:**

- Confidence in Recoverability: Provides confidence in the recoverability of critical data and enables accurate estimation of recovery speed in DR and CR scenarios.
- Comprehensive Testing: This feature offers comprehensive testing of storage, data restore performance, and network speeds to validate that data is restorable.

**Benefits:**

- This powerful tool allows data protection administrators to conduct recovery testing independently of application teams, exercising the storage, reading data, and transferring it across the network.
- It provides daily reports on success and failure, supporting continuous readiness and early detection of any data integrity issues.

## 6. COMMUNICATION AND COORDINATION

### 6.1 Plan for Communication Failures

**Recommendation:**

RESILIENT COMMUNICATION CHANNELS ARE VITAL WHEN PRIMARY SYSTEMS FAIL.

- Corporate communication platforms (e.g., Microsoft Teams, Slack) can be unreliable, unstable, and possibly compromised during an incident.
- Test out-of-band communication channels at least quarterly and train all key personnel to access and use these channels responsibly.
- Establish and regularly test out-of-band, secure applications (e.g., Signal, WhatsApp, Everbridge) for coordination among key personnel.
- As part of your incident response plan, include a RACI matrix with non-corporate contact information covering all areas of your cyber recovery team. Identify multiple tiers of team members in the event the primary team member is unreachable.
- Maintain all cyber recovery collateral such as plans, passwords, binaries, and golden images in an air-gapped location.

**Rationale:**

- Corporate communication mechanisms may be compromised or unavailable during a widespread cyber incident.
- Dedicated crisis communication channels provide a resilient method for CXOs and key stakeholders to coordinate and deliver broadcast messages.

**Benefits:**

- Manage communication and authentication between security operations teams, IT operations teams, and crisis management independently of the production environment so that when faced with compromise, efficient incident response and recovery is supported.

Pro Tip: Maintain physical, printed copies of the incident response plan, the cyber recovery plan, critical contacts, and communication instructions in a secure off-site location. Many 3rd party incident response teams offer cyber resiliency plan custodial services for safe keeping of plan documentation.

## 6.2 Document Dependencies and Workflows

**Recommendation:**

COMPREHENSIVE DOCUMENTATION GUIDES STRUCTURED RECOVERY AMIDST CHAOS.

- Maintain current application categorization and a robust business impact analysis.
- Store documentation in both digital and physical formats. Apply access controls to all digital copies.
- Document critical interdependencies between applications and detailed restoration workflows for each tier.
- Update documentation quarterly to account for evolving environments, new applications, and changing business needs.

**Rationale:**

- Recovery and Rebuild Sequencing: In the event of a total compromise, you need to rebuild and restore with precision. This starts with your infrastructure dependencies and carries through data requirements which dictate the sequence in which the applications need to be rebuilt.
- System Communication: Re-establishing inter-system communication is often the most challenging set of operations.
- Plan Documentation: Proactive documentation promotes success.

**Benefits:**

- Categorizing applications by criticality enables prioritized recovery, with AD typically assigned a 0–1-hour priority.
- Clear documentation can prevent recovery from being a chaotic event by supporting a structured, executable process.

## 6.3 Maintain Business Impact Analysis (BIA)

**Recommendation:**

ALIGN RECOVERY WITH A BIA TO DRIVE EFFECTIVE INCIDENT RESPONSE.

- Recovery plans must continually align with current business criticality and expectations for application recovery.

**Rationale:**

- Prioritized Recovery Efforts: A current BIA prioritizes recovery efforts in alignment with business impact, bringing the most critical applications back online first.
- Critical Capabilities: A BIA helps identify the minimum viable capabilities required to bring your organization back after a disaster or cyber event. Learn how Commvault helps organizations achieve minimum viability.

**Benefits:**

- A clear and up-to-date BIA supports efficient recovery efforts aligned precisely with organizational needs, particularly for complex and interconnected workflows.
- BIA to identify minimum viability helps rationalize and justify the appropriate security investments for your cyber resilience strategy.

## 7. MONITORING, REPORTING, AND ALERTS

### 7.1 Set Up Comprehensive Monitoring with Reports and Alerts

**Recommendation:**

VIGILANT MONITORING ENHANCES BASIC DATA PROTECTION SYSTEMS WITH EARLY WARNING SENSORS.

- Monitor your Commvault environment so that you can identify threats and issues before they escalate, such as NDR/EDR/XDRs and deception technology tools and sensors.
- Test alerting mechanisms regularly, such as by simulating a ransomware event and confirming that appropriate alerts are triggered. Integrate Commvault logs with your organization's central SIEM to enable holistic monitoring and faster incident response.
- Review the Security IQ Dashboard regularly to look for weaknesses and unusual activity.
- Audit Trails: Enable and monitor audit logs for Commvault operations. Information about audited operations is saved in the control plane for one year.
- Commvault monitors for unusual file activity patterns that could indicate ransomware. The system tracks significant changes in file modifications, creations, or deletions compared to historical baselines. Anomalies can include large numbers of files being created, deleted, modified, or renamed, or changes in file type/extension.
- Utilize Commvault's Threat Scan feature with embedded antivirus to scan protected data from file systems and virtual machines for malware signatures, encryption, and corruption.
- Set up alerts for critical events. Leverage the email notification feature or use a SIEM connector to send alerts to a third-party application, such as a syslog server or a webhook.

**Rationale:**

- Rate of Recovery: Early detection of malware or abnormal behavior can reduce recovery time during a ransomware incident. Commvault's integration with both SIEM/SOAR improves detection, response and mitigation efficiencies by providing additional context to Commvault's own alerts and gives 360-degree visibility to SecOps.
- Vigilant Monitoring: Regular review of security dashboards helps identify gaps and track user behavior. Timely alerts support immediate response against potential security incidents.

**Benefits:**

- Boost your Commvault environment with early-warning sensors for cyber threats.
- Identify security gaps and track of user activities.

## FINAL THOUGHTS

Cyber incidents are rampant. It is not a question of "if" you will be impacted. The more relevant question is "when" this your organization will face an attack. Successful cyber resilience is built from meticulous preparation, comprehensive documentation, and rigorous testing.

Cyber resilience is a team sport and requires continuous executive level reviews, bolstered by building the muscle memory within teams by performing periodic tabletop exercises to test ongoing effectiveness and alignment with organizational objectives.

Commvault provides a robust foundation for data protection and recovery. By hardening your environment, isolating your data protection infrastructure, and continuously validating your recovery plans, your organization can plan for a structured and executable cyber recovery. Stay prepared. Stay secure. **Commvault is your line of truth to clean and confident recovery.**

## APPENDIX

### Checklist: Commvault Security Best Practices Implementation

- ☑ **Data Protection Copies (3-2-1-1-0 Rule):** Maintain at least three copies of data on two different media, with one offsite/offline, one immutable/air-gapped, and zero errors via verification. For example:
  - Primary local copy of data to disk
  - Secondary copy to cloud with WORM lock
  - Tertiary copy to an archive tier on same hyperscaler or a different one
- ☑ **Strong Passwords:** Enforce Level 3 password complexity for local accounts with at least:
  - 12 characters
  - 2 uppercase letters
  - 2 lowercase letters
  - 2 numbers
  - 2 special characters
- ☑ **Least Privilege Access:** Utilize Commvault RBAC to grant users only the minimum permissions they need to perform their tasks. Create distinct roles for data protection and resiliency operators versus administrators. Prohibit the use of master administrator accounts for routine daily tasks.
- ☑ **Just-in-Time Administrator Access:** Implement JIT privilege elevation mechanisms so that high-privilege accounts are active only for the duration necessary. Integrate with enterprise PAM solutions where available.
- ☑ **Multi-Factor Authentication:** Mandate MFA for every login to Commvault administrative interfaces. Leverage strong authentication methods like authenticator apps or FIDO2-compliant hardware tokens.
- ☑ **Multi-Person Authorization:** Require dual approval for critical, destructive operations and restore operations in Commvault.
- ☑ **Security IQ Dashboard:** Regularly review the Commvault Security IQ Dashboard for your environment. Monitor the security posture score, investigate operational anomalies, and review threat indicators. Act promptly to address weaknesses and suspicious activities.
- ☑ **Threat Scan:** Enable Commvault Threat Scan to scan protected data for malware signatures. Confirm signature definitions are kept up to date. This is crucial for identifying and isolating compromised data before restoration.
- ☑ **Anomaly Detection Alerts:** Activate Commvault Anomaly Detection for unusual file activity and configure immediate alerts. This includes monitoring honeypot files, file anomalies, file encryption activities, and file type anomalies in data protection jobs. Alerts can be sent via email or integrated with SIEM systems.
- ☑ **Immutability (WORM/Compliance Lock):** Enable Commvault Compliance Lock on all critical copies to prevent alteration or premature deletion of data via the Commvault interface. For an even stronger defense, enable WORM storage lock on supported targets (disk or cloud object storage) for hardware-level immutability.
- ☑ **Encryption:** Enable native Commvault encryption for data at rest and in transit within storage policies. Software encryption should utilize AES-256. Securely manage and back up your encryption keys or integrate with an external Key Management Server (KMS).
- ☑ **Control Plane DR Protection:** Schedule daily protection of the control plane using the disaster recovery plan. Store copies separately from the control plane itself. Leverage the Commvault Cloud upload feature or an offline, air-gapped repository to secure the control plane database metadata offsite.

- ☑ **Isolated Data Protection Environment:** Segment the network where your control plane and data plane reside (e.g., dedicated VLANs). Implement strict firewall rules to limit inbound access to the control plane. Consider deploying the Commvault infrastructure in a separate AD forest or as standalone servers to limit exposure from production AD compromises.
- ☑ **Administrative Access Hygiene:** Prohibit direct RDP/SSH access to control plane and data plane from general production hosts. Utilize a secure jump server for any required direct administrative access. Restrict internet access from the control plane and data plane to minimize external attack vectors.
- ☑ **Password and Account Security:** Change default SQL and Commvault administrator account names to strong, unique, and randomized values. Implement an account lockout policy, such as locking the accounts after 3 failed log-on attempts for a duration of 5 minutes.
- ☑ **Patching Cadence:** Maintain a consistent schedule for applying Commvault software updates (service packs, hotfixes) and underlying OS security patches on control plane, data plane, and protected clients. Subscribe to Commvault security advisories for critical vulnerability notifications.
- ☑ **Data Verification of Protected Data:** Enable routine data verification jobs within Commvault to validate data integrity using checksums. Perform regular sample restore tests (daily or weekly) by restoring files or spinning up virtual machines to confirm data usability.
- ☑ **Test with Cleanroom Recovery:** Regularly practice restoring critical systems into an isolated "cleanroom" environment (cloud-based or off-network). Verify that data can be restored cleanly and that the process for recovering core services is well-understood and executable.
- ☑ **Tiered Recovery Plan:** Develop and document a tiered recovery plan for applications based on their criticality (e.g., Tier 0/1 for immediate recovery). Confirm Commvault storage policies and recovery configurations align with these tiers. Prepare comprehensive runbooks or automated workflows for prioritized recovery.
- ☑ **Minimum Viability Mapping:** Clearly identify the absolute minimum set of systems and data required for the business to achieve minimum viable operations after a major cyber incident. These crown jewel assets should be protected with the highest priority and their recovery procedures routinely tested.
- ☑ **Network Time Protocol (NTP) Poisoning Protection:** Implement measures to protect your NTP infrastructure against poisoning or manipulation, as accurate time synchronization is critical for logs, security events, and cryptographic functions. Similarly, any time-shifts noticed in the data plane access nodes' system clock forces the service to be brought down automatically.
- ☑ **Timeout Periods:** Configure the Command Center to time out after 30 minutes of inactivity.
- ☑ **Agent Installation Authentication:** Require user authentication for agent installation. This prevents unauthorized agents from connecting to the Commvault environment.

**GRC Guidance:**

- ☑ A**lign with regulatory requirements such as GDPR, HIPAA, and PCI DSS**, as organizations must demonstrate compliance for legal and operational integrity.
- ☑ **Regularly review this checklist to learn about new Commvault features that enhance your recovery when faced with a cyber incident.** Assign clear ownership for each checklist item and assign accountability for effective implementation.