COMMVAULT

WHITEPAPER

# Secure your data, your recovery and your mission

**Data management and protection software must share your mission with proven technology, constant vigilance, updates, and guidance.**

The cyber threat landscape, including ransomware, has transitioned to a case of when not if. To ensure you can recover your data and not pay the ransom, you need to trust that your data protection vendor shares your level of vigilance. The right solution requires the best technology, the right people, and processes.

At Commvault, much like a CISO, we operate in a constant state of alertness. We are highly responsive to our customers with the products and services we deliver. Commvault has earned a strong reputation as a dedicated and trusted partner; and has many customers who will testify to our responsiveness, innovation, and rapid execution in the high-pressure, high-impact world of a ransomware attack.

Data security is a strategic goal for Commvault and is addressed through our multi-layered protection, advanced detection, and rapid recovery from security threats, including ransomware and data breaches.

Organizations require tools to constantly measure their recovery readiness state to expose and remediate problems, validate the recoverability of their data and business applications through automated testing, and continually harden their environment to improve their security and reduce their risk profile.

When thinking about threats to the backup data itself, a common approach is to create data copies with a level of isolation, such as an air gap and immutable copies. Commvault agrees with this approach and has a proven history of providing immutable protection, geographic segregation, and air gap capabilities for the on-premises and cloud storage targets we write to, with the choice of using our appliances or your storage.

Providing data security while allowing for software to be administered effectively can be a challenge for many. Commvault leads the way, securing data and providing protection for concerns such as privacy, theft, corruption, and deletion, whether by internal, external threats, either malicious or misguided.

The AAA Security Framework for Authentication, Authorization, and Accounting is a valuable way to assess any software solution and is well known within the security community. Commvault uses it to assess, improve, and showcase its capabilities and adherence to industry regulations and best practices. Adhering to the zero trust principles as outlined in NIST SP 800-207, Commvault provides customers the range of services required to segment/isolate data, establish the user identity, provide access with the least required privilege, be safe from user error, and have a full granular logging and auditing capability. These controls work via all access types, UI, Command-Line, or API.

Threats are not always externally sourced, the result of compromised credentials or deliberate acts of rogue actors. To combat internal threats, Commvault has implemented a control mechanism to ensure administrative tasks that could threaten data are approved by two or more administrators from a selected privilege group, applying the four-eyes principle to data security.

A recovery solution is only viable if it is resilient across various failure modes. One scenario may be a data recovery event to revert to the prior instances before the corruption. At the same time, another may require complete recovery of the business applications at a new location. Designing recoverability across environments and providing simplified automation to test and validate each scenario helps build the recovery readiness state. Knowing the mission-critical data and applications were already validated for recovery by an automated process completes the needed security, compliance, and comfort level.

Commvault has developed ways to supplement security software with monitoring and detection capabilities with the critical aspects of a data protection architecture delivered. Machine Learning (ML) algorithms detect anomalies in file activity, and the implementation of honeypot files provides early warning about potential ransomware attacks. These tools provide additional early warning capabilities without increasing cost or management effort.

**The chart below summarizes key concerns and how they can be addressed with Commvault.**

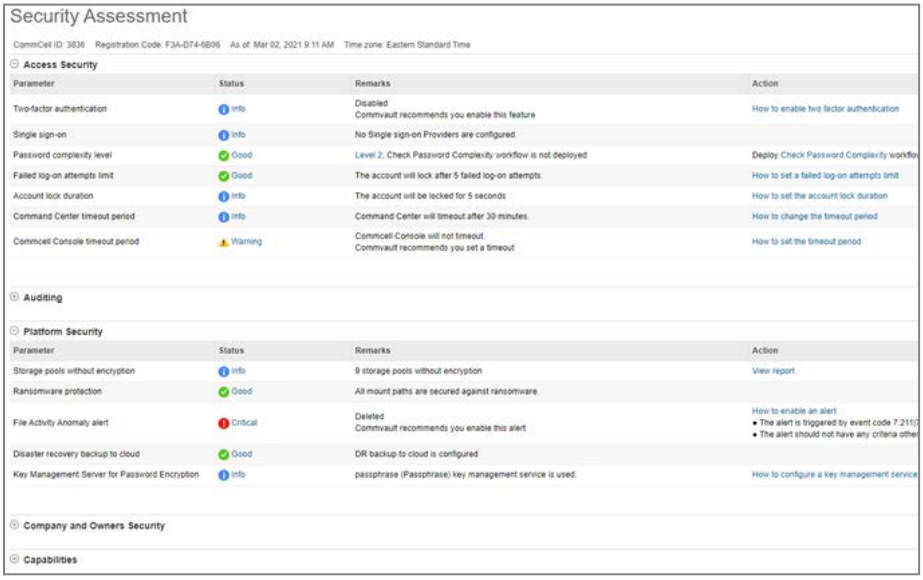
| Threat | Strategy |
|---|---|
| **Backup data volumes are targeted for destruction by ransomware** | Secure backup volumes, making them immutable to any administrator account. Modifications can only be made for verified Commvault processes. Additional security is provided by digitally signing the Commvault binaries and requiring certificate authentication between Commvault components. |
| **Threat actors target passwords, policies, and data** | Secure authentication with a choice of multi-factor controls, with granular role-based access lock-down to capabilities and systems within their scope. Data is encrypted and has external key management support. Four-eyes principle workflow protects against potentially destructive administration tasks. |
| **Rogue administrator access to backup data** | In addition to the four-eyes principle and being limited by granular role-based lock-down, every access and change will be logged, with any critical changes alerted to a system of choice. The privacy lock option protects sensitive and private data by ensuring it cannot be seen or restored by an administrator. |
| **Accidental deletion by the administrator** | All controls that keep out a threat actor and rogue administrator will also apply and remove the potential for mistakes by an administrator. |
| **Comply with security implications and regulations for log file management** | Organizations must establish policies to ensure compliance with laws and regulations they are subject to, typically preserving logs for extended periods. Log files from servers, endpoints, and network devices can be preserved independently from the regular backup retention policy. |

This discussion guide offers a collection of key security best practices employed across our global customer base. These practices have been adapted through a process of continuous improvement and innovation to provide data security and recovery readiness as data volume continually increases and the data landscape expands beyond open storage systems and into the cloud.

## Data security recommendations

Data security helps organizations protect and recover from security threats, including data breaches and ransomware, while controlling access to key data. Commvault's Intelligent Data Services includes advanced threat and anomaly detection — part of a multi-layered protection capability that helps mitigate the impact of threats to your data. Ransomware attacks are in the headlines, and with Commvault, you can mitigate the risk of ransomware occurrences and help accelerate your recovery efforts in the event of a ransomware attack.

### Security Health Assessment Dashboard




The starting point is to properly identify and assess the risks and gaps. The Security Health Assessment Dashboard is available in both Commvault Cloud Metrics Reporting and Commvault Command Center™. The Security Health Assessment Dashboard will quickly provide insights and recommendations to build an action plan. All of the recommended controls and settings can be found in this dashboard and quickly implemented using interactive actions. For more information, read Improving risk management with the Commvault Security Health Assessment Dashboard.

### Develop a plan with a multi-layer strategy

Commvault knows that it is paramount to have a multi-layer security strategy for data security and that recovery readiness is critical. Ensure your mission-critical data can withstand a targeted attack designed to destroy primary and backup copies of your data, and complexity has been removed with a recovery process that is as automated and orchestrated as possible.

Any plan you develop must work broadly and deeply enough to reach valuable data wherever it resides. Your plan should extend beyond central servers and organization-wide applications to cover laptops, files in a wide range of media formats, and function-specific applications.

### Backup target immutability

Ensuring backup copies are immutable and cannot be altered or encrypted by ransomware is critical. It must be cost-effective for all data within your environment and can be turned on for the storage of your choice; on-premises, in the cloud, or Commvault HyperScale™ solutions. It is a clear choice with greater benefit than air gap-only solutions without additional complexity and cost.

The backup store immutability feature employs proven methods to restrict write and delete operations, which prevent bad actors or malware from modifying files in the protected path. Commvault recently tested the reliability and effectiveness of this capability with the RIPlace bypass technique, which could breach several security endpoint solutions that share a similarity in the reported capability. Commvault, however, was proven to provide secure protection from the RIPlace bypass method.

With a multi-layer strategy recommendation, some customers choose to implement additional strategies for greater protection. For specific data, organizations may write once, read many (WORM) copies on-premises or in the cloud, and implement air gap isolation strategies. These are simple to implement in Commvault through policies, including network segmentation, encrypted network topologies, gateways, and firewalls. Also, it supports automation to orchestrate network and server disconnection.

### Foundational hardening

The principles of foundational hardening are essential for all software environments. The core components of the Commvault solution rely on the underlying operating system, database, application, and web server technology. Therefore all security vulnerabilities within the underlying technologies need to be closed not to become entry points for cyber threats.

- **Apply hardening recommendations** – automatic enablement of hardening recommendations based on National Institute of Standards and Technology (NIST) standards.
- **Binary signing including 3rd party** – a Commvault framework to digitally sign binaries and ensure a malicious actor has not modified them. Any 3rd party libraries are updated regularly and in response to reported vulnerabilities.
- **CIS Level 1 hardening** – Commvault software has been tested and confirmed as capable of Center for Internet Security (CIS) Level 1 hardening.

### Application hardening with authentication, authorization, and accounting

Authentication, authorization, and accounting (AAA) is a Security Framework for intelligently controlling access to computer resources, enforcing policies, and auditing usage. These combined processes are considered essential for effective network management and security. Commvault delivers a secure, robust, and complete set of features in each of these three areas.

COMMVAULT

WHITEPAPER

# AAA Security framework for controlling access

| Authentication | Authorization | Accounting |
| --- | --- | --- |
| Proving and granting access | Control what level of access is required | Tracking and auditing access and capabilities |

## Authentication

The authentication process is based on each user having a unique set of criteria for gaining access. Commvault enables multi-factor authentication (MFA) methods to make it highly unlikely that a valid user account can be impersonated.

- **Secure Lightweight Directory Access Protocol (LDAP)** – supports Activate Director and generic LDAP identity servers.
- **External identity providers** – are supported using secure protocols such as Open Authorization (OAuth) and Security Assertion Markup Language (SAML).
- **Multi-factor authentication** – with logins using authenticator application, smart cards, and hardware authentication keys.
- **Certification authentication** – for Commvault infrastructure to protect against spoofing.
- **Multitenancy** – providing administrative micro-segmentation and compartmentalization of access.
- **Privilege Access Management (PAM) with CyberArk** – centrally store, organize, secure, and manage Commvault. credentials, service account credentials, and admin login sessions without exposing passwords.

## Authorization

Following authentication, authorization must be granted to the user to allow specific tasks. Commvault provides a rich and complete set of capabilities:

- **Role-based security** – manage capabilities by assigned roles to users and groups, including support for multi-tenant environments, and limited in function and scope of servers, applications, and data sets that can be accessed and managed.
- **Dual authorization workflows** – supporting the four-eyes principle for administrative tasks such as deleting data sets, clients, restores, targets, jobs, and policies.
- **Passkey and privacy lock** – supporting the principle that administrators manage the data but should not view or restore the data they do not own. Used together, only the owner of the dataset at the individual, department, or company level can restore data with the required passkey.
- **Data encryption** – Federal Information Processing Standards (FIPS) certified encryption, 6+ ciphers including AES 256, encrypt data from the first touch and throughout the entire data management lifecycle.
- **Encryption key management** – built-in Key Management System (KMS) or use an external third party KMS including any compatible Key Management Interoperability Protocol (KMIP) system, AWS KMS, Azure Key Vault, and passphrase.
- **Network encryption** – HTTPS encapsulation, TLS 1.2, Proxy/Gateway support.
- **Third-party port mapping (TPPM)** – tunnel third-party communications through Commvault network ports, dramatically reducing implementation complexity in a secure environment.
- **WORM copy support** – WORM policies, when applied to data copies, enforce the removal and deletion rights and impose fixed data retention.
- **Cloud WORM service support** – bucket and object-level storage supported for WORM configurations.

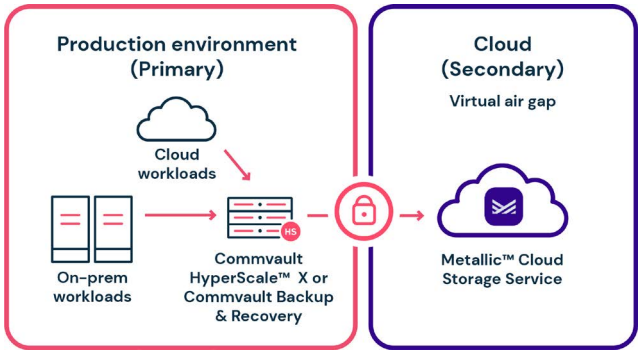
## Accounting

Accounting should focus on complete logging of user access and actions from the security aspect, ensuring observability through specific reports and alerting for certain conditions. Answering essential questions such as:

- **Who has too much access?** The volume of access via UI, Command line, and API is tracked and reported.
- **What is being done with the access?** An entire audit trail of user access and action.
- **What access can be removed?** The system will report users who have not accessed in a specific time period for possible removal.
- **What data is not encrypted?** A report confirms encryption status, which is a typical recommendation.

### Data isolation and air gap

The "Air Gap" control concept is a data protection architecture that limits exposure to an attack and allows for data restoration to a point-in-time before the attack began. Commvault can effectively address the risk of encrypted data being replicated in the data backup architecture with; immutable backup targets, periodically applying a WORM security policy to data copies, and removing deletion capability until the retention policy is met. Commvault has improved upon physical access controls available to every solution, enhanced security, simplified, and reduced cost.

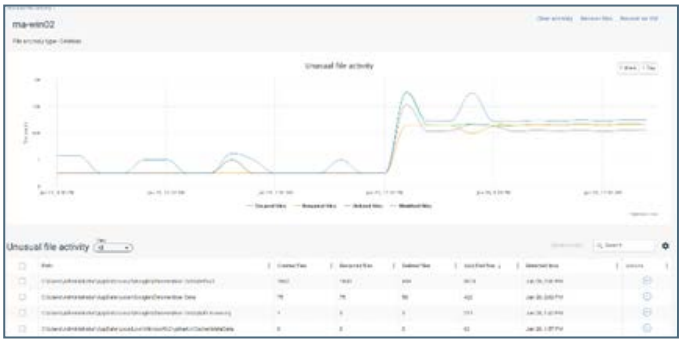



- **Air gap orchestration** – automate workflows to orchestrate network and server disconnection.
- **Network segmentation** – use Network security controls to block incoming access to secondary storage targets both logically and physically.
- **Encrypted network topologies** – use Commvault network policies to isolate communications and create encrypted tunnels outbound from the isolated storage target. Commvault gateways can control persistent connections automatically.
- **Easily adopt secure and scalable cloud storage** – Metallic™ Cloud Storage Service (MCSS) – this is the "easy button" to deliver secure air gapped cloud storage for secondary copies with predictable cost and no infrastructure required.

Greater ransomware protection with data isolation and air gap technologies. **Read >**

### Monitoring and detection

Many experts recommend having a layered anti-malware and ransomware strategy. Commvault has built these capabilities to existing security software and policies for more significant benefits without the incremental management overhead.

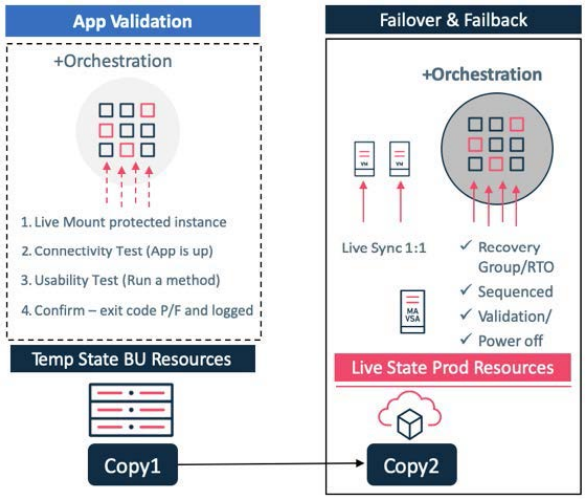


- **Monitor file system activity** – utilizes historical data and a machine-learning algorithm to detect statistically variant file system behavior.
- **Monitor honeypot files** – hidden files that are common and attractive to ransomware attacks are monitored for signature changes.
- **Security Information and Event Management (SIEM) integration** – use existing security monitoring platforms to manage and orchestrate Commvault actions and events centrally. Through Syslog, plugins, or APIs, export audit trail, events, alerts, and logs securely into your SIEM and SOAR platform for preservation and event orchestration.
- **Certificate authentication lock-down** – when certification lock-down is enabled, clients cannot be added to the data protection architecture without additional administrative steps and privileges.
- **Actionable alerting** – automatically act and alert for awareness or embed a recommended action workflow into the alert for administrator execution.

### Simplifying recovery readiness

True peace of mind comes from having a comprehensive, continuous recovery readiness plan. The last thing you want to do when contending with a high-pressure attack is to stop to figure out which data needs to be recovered in what order. Recovery readiness means that recovery stages are documented, automated, and predictable. Commvault capabilities to support recovery readiness include:

- **Highly available data protection architecture** – Commvault architecture can be protected using Live Sync replication of the database to one or more standby nodes. The database can be protected natively in any public cloud and is a free protection service offered by Commvault.
- **Recovery orchestration** – the Commvault control plane manages, operates, and maintains records for all collected data. It can be fully recovered with a single click, which can be tested ahead of time by a fully orchestrated test failover to provide a validated restore without disrupting production.
- **Data integrity validation** – Commvault provides multiple methods of data integrity validation. Data signatures are used to confirm the integrity of any data transferred, received, and written to storage media. In addition, automated tasks for regularly validating the data on storage are provided.




- **Application recoverability validation** – a fully orchestrated application recovery validation task can provide access directly to the data protection copy from the backup infrastructure, start the application, connect and run a test method to validate both the data and application recoverability.
- **Easily identify data to recover** – data can be searched across any time period, and options applied include show/hide deleted items, latest, specific point-in-time, and time range. These options provide a simple way to select the right data to recover.

### Industry certifications

The following certifications of compliance are held (or pending where indicated) with the Commvault data protection solution:

- **Common Criteria Certification** – Pending
- **FedRAMP** – Federal Risk and Authorization Management Program (FedRAMP) "High Ready" status for Metallic Backup as-a-Service (BaaS) portfolio and Metallic Cloud Storage Service (MCSS)
- **FIPS 140-2 Certified** – Cryptographic Module Validation Program
- **NIST 800-53 CP9 Compliant** – NIST Special Publication 800-53 (Rev. 4) CP-9
- **NIST 800-53 CP10 Compliant** – NIST Special Publication 800-53 (Rev. 4) CP-10
- **STIG (Security Technical Implementation Guide)** – Certification for Commvault HyperScale™ Storage Pool
  - STIG Certification – Scan Results at https://documentation.commvault.com
- **VPAT 2.0 – WCAG and 508 Compliant** – VPAT 2.0 Statement

The risks and rewards of defending against a ransomware attack are significant to your organization and career. Done poorly, it results in lost data, revenue, and credibility. Done correctly, it can lead to operations being successfully restored quickly and greater recognition for a job well done. The choice is yours; the choice is simple, be recovery ready!

Learn more about using data protection as your defense against ransomware. Visit **commvault.com/ransomware >**