

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.

Overview

The cyberthreat landscape, including ransomware, has evolved to the point where it's not a matter of if a security event will compromise your data, it's a matter of *when*. To ensure you can efficiently protect your data and, if necessary, recover it without paying a ransom, you need confidence that your data protection vendor offers a proven solution to empower your people and processes with the best technology.

Commvault addresses data security through multilayered protection, advanced detection, and rapid recovery from security threats, including ransomware and data breaches. With Commvault Complete™ Data Protection, you can create a multi-tiered replication strategy that accommodates your restoration priorities for various data types and workloads.

Organizations require tools to constantly measure and evaluate their recovery readiness state and they need a plan such as a Zero Loss Strategy to reduce the impact of ransomware.

Air gapping immutable copies is an effective strategy for isolating backup data. Commvault has a proven history of providing immutable protection, geographic segregation, and air-gap capabilities for on-premises and cloud storage targets, with the choice of using our appliances or your storage. Commvault also leads the way in securing data and providing protection for concerns such as privacy, theft, corruption, and deletion, whether by internal or external threats – either malicious or misguided.

The AAA Security Framework defines access control best practices as having stringent authentication, authorization, and accounting processes. Commvault adds value in each of these areas while also adhering to zero trust principles outlined in NIST SP 800-207. Commvault continues to harden credentials and key management systems with multi-factor authentication methodologies with support for YubiKey and Common Access Card (CAC).

Since threats don't always come from an external source, Commvault addresses internal threats using a control mechanism that requires two or more administrators from a selected privilege group to approve administrative tasks that could threaten data.

A recovery solution is only viable if it is resilient across various failure modes. The Commvault platform automates the testing and validation of recovery scenarios for mission-critical applications and data to boost security, compliance, and stakeholder confidence.

Commvault also supplements security software with monitoring and detection capabilities. Machine Learning (ML) algorithms detect anomalies in file activity, and honeypot files provide early warning about potential ransomware attacks – without increasing cost or management effort. Commvault even offers greater insights into suspicious activity, including file-type changes that indicate if data is impacted by unauthorized changes from ransomware, helping to ensure fast and accurate threat detection.

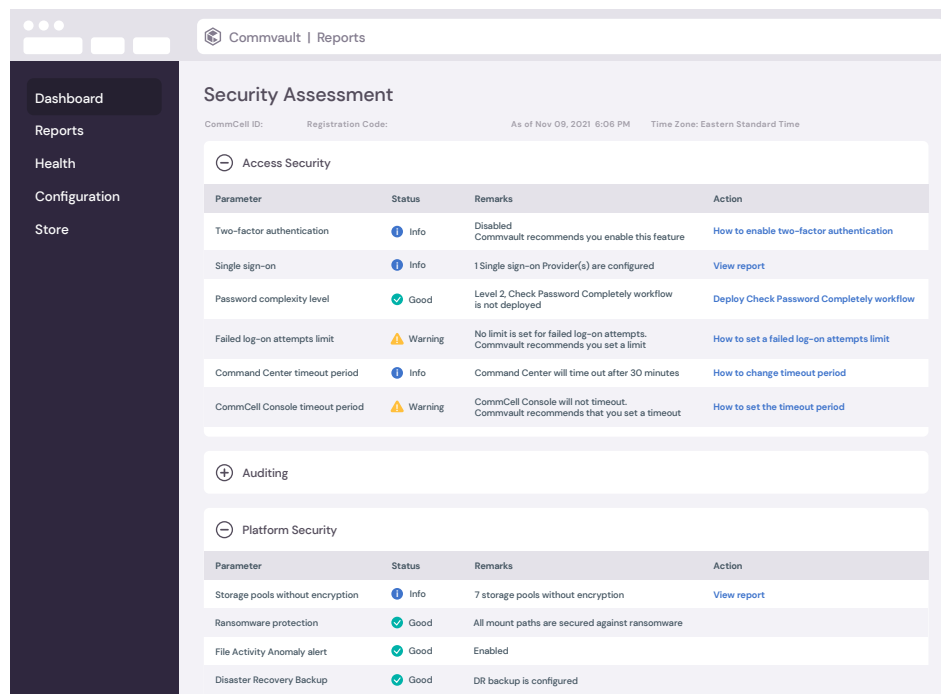
The chart below summarizes key concerns and how Commvault addresses them.

Threat	Strategy
Ransomware targets backup data volumes for destruction	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 lockdown to capabilities and systems within their scope. Data is encrypted and has external key management support. The four-eyes principle workflow protects against potentially destructive administration tasks.
Rogue administrator gain access to backup data	In addition to the four-eyes principle and being limited by granular role-based lock-down, all access and changes are logged, with automated alerts of critical changes sent to your system of choice. The privacy lock option protects sensitive and private data by ensuring it cannot be seen or restored by an administrator.
Administrator accidental deletes data	All controls that keep out a threat actor or rogue administrator will also apply and remove the potential for mistakes by an administrator.
Teams fail to comply with policies and regulations for log file management	Organizations must establish policies to ensure compliance with applicable laws and regulations – typically requiring log retention for extended periods. Log files from servers, endpoints, and network devices can be preserved independently from the regular backup retention policy.

Data security recommendations

Data security measures help organizations protect and recover from security threats, including data breaches and ransomware, while controlling access to key data. The Commvault Security Health Assessment Dashboard includes advanced threat and anomaly detection — part of a multilayered protection capability that helps mitigate the impact of threats to your data.

Security Health Assessment Dashboard



Commvault | Reports

Security Assessment

CommCell ID: Registration Code: As of Nov 09, 2021 6:06 PM Time Zone: Eastern Standard Time

Access Security

Parameter	Status	Remarks	Action
Two-factor authentication	Info	Disabled Commvault recommends you enable this feature	How to enable two-factor authentication
Single sign-on	Info	1 Single sign-on Provider(s) are configured	View report
Password complexity level	Good	Level 2, Check Password Completely workflow is not deployed	Deploy Check Password Completely workflow
Failed log-on attempts limit	Warning	No limit is set for failed log-on attempts. Commvault recommends you set a limit	How to set a failed log-on attempts limit
Command Center timeout period	Info	Command Center will time out after 30 minutes	How to change timeout period
CommCell Console timeout period	Warning	CommCell Console will not timeout. Commvault recommends that you set a timeout	How to set the timeout period

Auditing

Platform Security

Parameter	Status	Remarks	Action
Storage pools without encryption	Info	7 storage pools without encryption	View report
Ransomware protection	Good	All mount paths are secured against ransomware	
File Activity Anomaly alert	Good	Enabled	
Disaster Recovery Backup	Good	DR backup is configured	

The best way to start bolstering data security is to properly identify and assess your organization's risks and gaps. The Security Health Assessment Dashboard is available in both Commvault Cloud Metrics Reporting and Commvault Command Center™. The dashboard quickly provides insights and recommendations for building an action plan. Recommended controls and settings in this dashboard can be quickly implemented using interactive actions. For more information, read [Improving risk management with the Commvault Security Health Assessment Dashboard](#).

Zero Loss Strategy

Reducing the risk of ransomware is challenging, but incorporating a strategy that provides visibility across your data and the ability to recover quickly is essential to resume normal business operations. Adhering to zero trust principles and a multilayered security framework is a good start. However, you need a strategy to help plan, manage, and reduce the impact of ransomware and have the ability to recover quickly in the event of an attack. Use a centralized management platform to reduce complexities and protect what matters most through a [Zero Loss Strategy](#).

Backup target immutability

Ensuring backup copies are immutable and cannot be altered or encrypted by ransomware is critical. Immutability must be cost-effective for all data within your environment, with the ability to enable it for the storage of your choice: on-premises, in the cloud, or across Commvault HyperScale™ solutions. Immutability offers greater protection 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 tested the reliability and effectiveness of this capability with the RIPlace bypass technique, which has been shown to breach several security endpoint solutions with a similar capability. Commvault, however, was proven to provide secure protection from the RIPlace bypass method.

With a multilayer 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 deploy air-gap isolation solutions. These are simple to implement in Commvault through policies, including network segmentation, file type anomaly detection, encrypted network topologies, gateways, and firewalls. Also, they support 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 underlying technologies must be remediated to close entry points for cyberthreats. This can be accomplished by:

- **Applying hardening recommendations** – automatic enablement of hardening recommendations based on National Institute of Standards and Technology (NIST) standards.
- **Binary signing including third parties** – a Commvault framework to digitally sign binaries and ensure a malicious actor has not modified them. Third-party libraries are updated regularly 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.

AAA security framework for controlling access

Authentication	Authorization	Accounting
Proving identity and granting access	Controlling 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 generic LDAP identity servers as well as Active Directory.
- **External identity provider support** – 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 set of capabilities:

- **Role-based security** – manage capabilities by assigned roles to users and groups, including support for multi-tenant environments, and limit the 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 data but should not view or restore 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** – choose the built-in Key Management System (KMS) or use an external third-party KMS, including 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 removal and deletion rights, and impose fixed data retention.
- **Cloud WORM service support** – bucket and object-level storage supported for WORM configurations.

Accounting

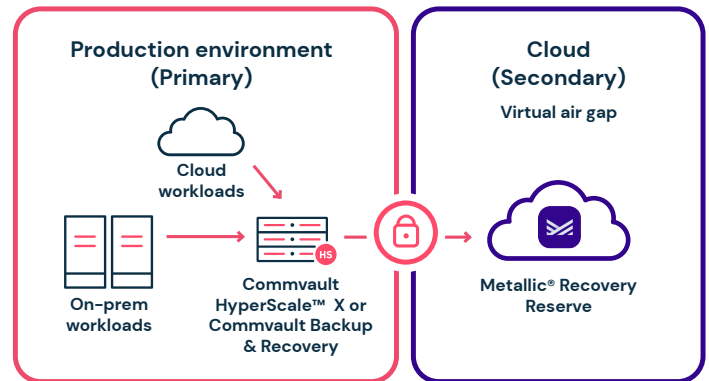
Accounting should focus on complete logging of user access and actions from the security aspect, ensuring observability through specific reports and alerting for certain conditions. Answering essential questions such as:

- **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 actions.
- **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 gapping

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: 1) immutable backup targets, 2) periodically applying a WORM security policy to data copies, and 3) removing deletion capability until the retention policy is met. Commvault improves upon physical access controls available to every solution, enhances data security, simplifies administration, and reduces costs.

- **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® Recovery Reserve is the “easy button” to deliver secure air-gapped cloud storage for secondary copies with predictable cost and no infrastructure required.

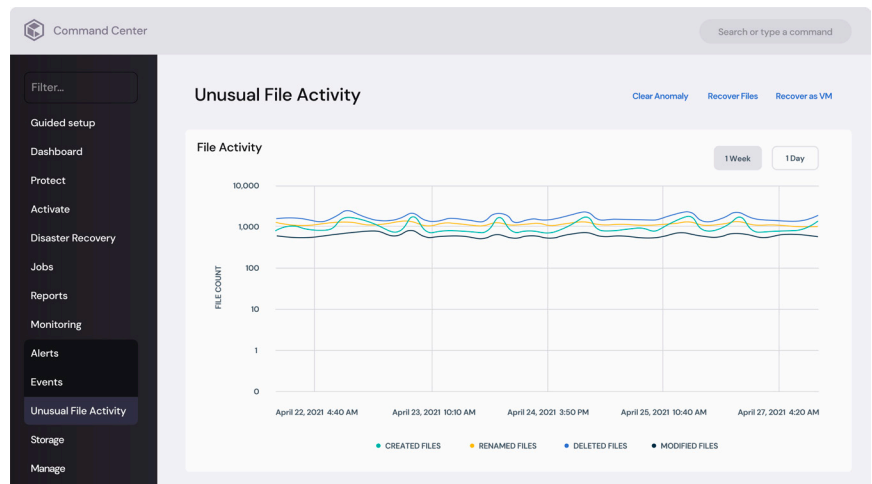


Greater Ransomware Protection with Data Isolation and Air-Gap Technologies. [Read >](#)

Monitoring and detection

Leading experts recommend having a layered antimalware and ransomware strategy. Commvault has built these capabilities into existing security software and policies for significant benefits without the incremental management overhead of point solutions.

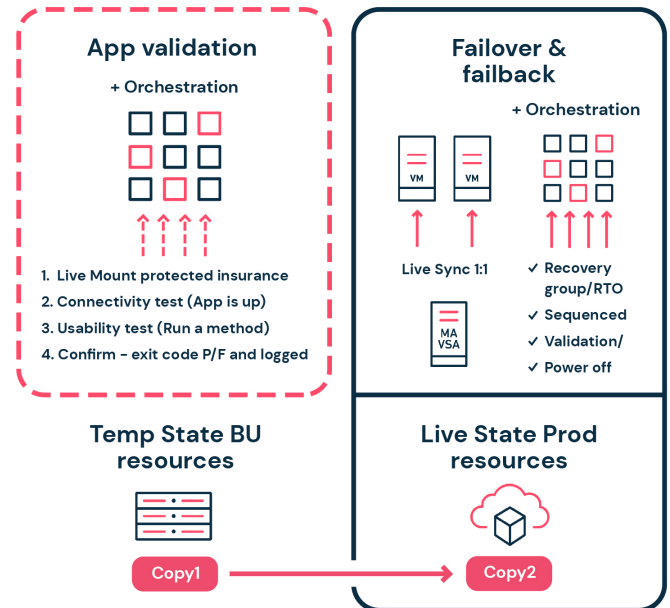
- **Monitor file system activity** – use historical data and a machine-learning algorithm to detect statistically variant file system behavior.
- **Monitor honeypot files** – hidden files that are common and attractive to ransomware attacks are monitored for signature changes.
- **Anomaly detection** – gain insights into suspicious activity and changes at the file level that indicate if data is impacted by ransomware.
- **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 in place. 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 and 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’s 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 and 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 that can be 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 compliance certifications 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 Recovery Reserve
- **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

How well your team defends against a ransomware attack can dramatically affect your organization and career. Done poorly, it results in lost data, revenue, and credibility. Done well, it can lead to operations being protected, and when necessary, successfully restored quickly, with accolades all around. Commvault Complete Data Protection can help you do it well.

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