



COMMVault  BUYER'S GUIDE

ALIGNING RANSOMWARE PROTECTION AND RECOVERY PLANS WITH **CRITICAL** **CAPABILITIES**

 SOLUTIONS

THE EVOLVING ENTERPRISE AND THE RANSOMWARE THREAT

Organizations face an increasingly turbulent data environment, with damage from cybercrime predicted to hit \$10.5 trillion annually by 2025.¹ The trend of hybrid and remote employment, coupled with accelerating data sprawl and the rise of advanced cyberthreats makes protecting data and ensuring service continuity an even more daunting challenge. Companies need a cutting-edge data protection solution that goes beyond traditional backup and recovery to protect against tomorrow's evolving threats to secure, defend, and recover your data – helping to reduce your risk and control costs.



\$10.5
TRILLION
annually by 2025.¹

Organizations are adopting multilayered security frameworks to deal with these vulnerabilities and need a next-generation data protection platform with active defense and automation. This approach offers the best blueprint for protecting against and recovering from ransomware attacks.

THE PURPOSE OF THIS GUIDE

Use this guide to map your current ransomware protection and recovery capabilities and determine how best to optimize your readiness plan across hybrid, cloud, or SaaS workload environments.

¹ Cybersecurity Ventures, Steven C. Morgan, Cybercrime to Cost The World 8 Trillion Annually In 2023, October 2022

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBERSECURITY FRAMEWORK

To help strengthen the resilience of your data infrastructure, the [NIST Cybersecurity Framework](#) focuses on five primary pillars for a successful and holistic cybersecurity program. Attention to these pillars can aid your organization in developing a comprehensive risk management strategy.

In each section of this guide, we cover why each security layer is essential and review key capabilities to incorporate into your ransomware protection and recovery solution.



01 IDENTIFY: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.



02 PROTECT: Develop and implement appropriate safeguards to ensure the delivery of critical services.



03 MONITOR: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.



04 RESPOND: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.



05 RECOVER: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.



01 IDENTIFY

Do you know how and where your critical data is used? Effective data security tools can identify where there is risk and provide visibility across your entire data environment. Identify risks and protect and backup data with zero-trust architecture that includes built-in security protocols to secure data, prevent unwanted access, and drive compliance in the face of evolving cyberthreats. In the event of a successful attack, end-to-end observability helps organizations make better data decisions, anticipate risks, and eliminate blind spots before, during, and after a cyberattack.

IDENTIFY KEY COMPONENTS	RANSOMWARE REQUIREMENTS	COMMVault CAPABILITIES
Automated Security Assessment	Easy, interactive toolsets for quickly assessing security posture and applying recommendations to improve security.	Take proactive action before attacks can damage or spread with comprehensive dashboards that provide deep insight into all aspects of data security.
Automated Backup Health Assessment	Verify that backups are healthy.	Cloud and on-prem metrics provide regular health reports.
Data Management Reports and Dashboards	Ability to quickly view the status of backup and recovery readiness. Customized reports and dashboards for specific items of interest.	Unified dashboards & extensible reporting provide recovery readiness with detailed KPIs.
Auditing	Keep track of data changes, including who accessed it and when it was changed.	Audit logins tied to specific users & IP addresses. Monitor all configuration changes and backup & restore events in detailed audit trails.
Threat Deception	Intercept attacks before they reach their targets.	Metallic® ThreatWise™ provides differentiated tools to detect zero-day and unknown threats in production environments, helping customers spot advanced cyberthreats before data compromise.
Risk Analysis	Identify and investigate sensitive and at-risk data to minimize data exposure and exfiltration.	Identify, categorize, and classify sensitive information, such as personal and financial data, to prioritize security measures and reduce data exfiltration in the event of a breach. Take proactive measures to ensure compliance with regulations and save storage costs by archiving outdated (ROT) data.
Threat Scan	Identify and investigate file anomalies to ensure you recover good data and avoid malware reinfection.	Identify malware threats to avoid reinfection during recovery. Threat Scan analyzes backup data to find encrypted or corrupted files, ensuring users recover trusted versions of their data quickly.



Reduce your attack surface by limiting and containing potential threats and preventing a systemic spread. Protect against changes from inside and outside your backup solution with zero trust architecture, helping to prevent unwanted access. Isolate and segment networks, adopt air-gapping to isolate and secure backup copies, and incorporate cyber deception technology to intercept threats before data leakage, encryption, and exfiltration. Ransomware attacks can occur when credentials are compromised or a user's credentials allow privileged access to systems they shouldn't have had in the first place. Ensure industry-standard security protocols are in place to encrypt and secure data to reduce the impact of a ransomware attack.

PROTECT KEY COMPONENTS	RANSOMWARE REQUIREMENTS	COMMVault CAPABILITIES
Immutability	Keep backup data safe from unauthorized changes.	<ul style="list-style-type: none"> • Anti-ransomware protection for Windows and Linux-based systems. • Apply storage locks for on-prem and cloud — customize to meet business needs. • Enable WORM (Write Once, Read Many) to prevent unauthorized changes and cloud air-gapping technology to further protect from ransomware threats.
Infrastructure Hardening	Reduce exposure to threats on backup infrastructure.	<p>Commvault® software has been tested and confirmed as capable of Center for Internet Security (CIS) Level 1 hardening.</p> <p>Compliance with CIS Level 1 security controls is available as a pre-hardened CIS VM (deployed via OVA) or as a hardware appliance delivered as Commvault® HyperScale X™. All sub-components, including CommServe, media agents, and access nodes can also be hardened to CIS Level 1.</p>
Authentication and Authorization	Control who has access and what level of access they have while adding multiple layers of authorization to ensure extra security.	<ul style="list-style-type: none"> • Role-based access controls limit unauthorized usage along with SAML (Security Assertion Markup Language) and OATH IdPs to provide an extra layer of security. • Integration with Active Directory and LDAP. • Multi-Factor Authentication (MFA) and Multi-Person Authentication (MPA) controls for retention locks and command authorization to protect data from accidents and prevent destructive actions. • Integration with privileged access management (PAM) and enhanced identity and access management (IAM) tools such as CyberArk, Yubikey, and biometrics for added user authentication and assurance (AAL3). • Just-in-Time (JIT) integration with CyberArk to minimize the risk of stored credentials. • End-to-end data encryption while allowing external key management platforms to manage and control keys, and certificate authentication – protecting against malicious data access. • Software WORM (retention lock). • Multitenancy.



PROTECT KEY COMPONENTS	RANSOMWARE REQUIREMENTS	COMMVAULT CAPABILITIES
Encryption	Implement encryption standards that meet industry guidelines.	Standards and tools to effectively manage encryption keys for backup and restore in Commvault: <ul style="list-style-type: none"> • FIPS (Federal Information Processing Standards) encryption module. • Built-in key management. • Integration with third-party key management. • Passphrase KMS (Key Management System).
Backup Catalog Protection	Protect data in multiple areas, whether on-prem local copies or in the cloud.	<ul style="list-style-type: none"> • Strong ransomware protection for local copies. • Backup to Metallic® Recovery Reserve™ or to third-party cloud.
Isolation/ Air-gapping	Segment and isolate data away from external networks and ensure quick recovery in the event of an attack.	<ul style="list-style-type: none"> • Metallic® Recovery Reserve™ uses air-gapping to isolate and protect sensitive data. • Commvault® HyperScale X™ appliances feature integrated air-gap controls. • Network topologies: Use one-way or proxy topology.
Active Directory Protection	Create the ability to protect and restore Active Directory, back up object attributes, and perform full, differential, incremental, and synthetic backups.	The Commvault platform and Metallic solutions offer air-gapped on-prem and cloud-based Active Directory protection.
3-2-1 Backup Strategy	Create an effective backup strategy that ensures data is always available. Have at least three copies of data, two of which are local but at different locations, and one copy off-site.	<ul style="list-style-type: none"> • Configure unlimited copies of data on-prem or in multiple cloud endpoints. • Metallic® Recovery Reserve™ provides the ability to enable air-gapped cloud storage.
Threat Deception	Spot ransomware attacks early - before data leakage, encryption, exfiltration, or damage.	<ul style="list-style-type: none"> • Cover your surface area by deploying threat sensors (fake decoys) in bulk. • Mimic critical assets with preconfigured sensors. • Emulate highly specialized assets unique to your environment.
On-Demand Security Controls	Be compliant and in control with password rotation policies that do not impact backup protection.	Improve security posture with zero trust control and eliminate compromised credentials. CyberArk integration allows just-in-time credential retrieval, including secure credential storage and management within CyberArk.



Organizations impacted by a security threat may not even be aware they have been attacked until it is too late and the breach spreads beyond their control. Ensuring appropriate tools are in place to quickly gain insight into a cybersecurity event is imperative to help contain a ransomware attack before it affects broader infrastructure. Incorporate next-generation early warning and in-depth monitoring to surface and neutralize zero-day and insider threats to defend your data. Detect, divert, and flag malicious activity sooner to reduce recovery efforts.

MONITOR KEY COMPONENTS	RANSOMWARE REQUIREMENTS	COMMVault CAPABILITIES
Backup Anomaly Detection	Establish what types of anomalies can occur.	<ul style="list-style-type: none"> Analyze events and behavior as well as backup runtime. Monitor whether backups are successful, pending, or failed. Predict future SLA compliance with trend analysis of backups.
File Anomaly Detection	Obtain granular visibility of unusual file activity by using an audit trail to determine where potential security events occur.	<ul style="list-style-type: none"> Obtain file activity changes from ransomware encryption and backup activity changes. Identify anomalies with file characteristics changes due to corruption, encryption, or malicious files on live and backup data. Monitor root size changes and suspicious IOCs (extensions).
System Monitoring	Monitoring critical workloads and infrastructure.	<ul style="list-style-type: none"> Gather information on key resources such as CPU, memory, disks, networks, streams, and read/writes. Obtain details on logins, logouts, and file activity and send them to SIEM/SOAR systems for visibility and remediation.
Log Monitoring	Search for specific log events to monitor log activity in your environment. Search for a particular event across all log events indexed on the dashboard. Search log events associated with a particular client, log file, template, or monitoring policy.	The Commvault platform lets you monitor log file conditions and Syslog and Windows events in granular detail.



MONITOR KEY COMPONENTS	RANSOMWARE REQUIREMENTS	COMMVault CAPABILITIES
Threat Awareness	Proactively gain immediate insight into active and latent threats.	<ul style="list-style-type: none">• Expose sensors to bad actors only; invisible to legitimate users and systems.• Gain critical intelligence into activities and tactics.• Eliminate false positives and alert fatigue.• Lure bad actors into engaging fake resources.
Security Monitoring with AI	Use artificial intelligence to monitor for anomaly frameworks that support VM backups and other workloads, such as SaaS apps.	<ul style="list-style-type: none">• Gain insights into when backups are abnormally changing to drive clean, fast secure recovery.• Find clean versions of data to drive clean, fast secure recovery.• Reduce false positives with AI/ML.
Honeytrap and Live File Activity	Monitor assets at risk of ransomware and identify clean recovery points.	Monitor live suspicious files to detect threats and protect backups to ensure clean file recovery and avoid file reinfection.





Once ransomware is detected, your response must be immediate. Gaining insight through security tools and proactive alerts allows your organization to defend your data. Documented policies and an incident response plan help determine what comes next. There must be both a technical and a business response, and every stakeholder in each of their respective areas must understand their role and the action to take. Coordination and communication between various teams are essential. The key is for security teams to do as much as possible to contain and stop the spread while putting the proper tools in place to avoid any potential reinfection.

RESPOND KEY COMPONENTS	RANSOMWARE REQUIREMENTS	COMMVAULT CAPABILITIES
SIEM (Security Information and Event Management) and SOAR (Security Orchestration Automation and Response) Integration	Integrate seamlessly with your existing SIEM and SOAR platforms to monitor, manage, and orchestrate actions and events from a central location. Export audit trails and events and securely log them into your SIEM and SOAR platforms for preservation and event orchestration. With real-time monitoring, you can quickly respond to any detected threats and protect your backup assets with the appropriate action.	Commvault's Integrations enable interoperability with various orchestration platforms such as Microsoft Sentinel, Palo Alto Networks XSOAR, Splunk, and ServiceNow. Our integrations provide: <ul style="list-style-type: none"> • Real-time visibility into security events and incidents. • Enhanced automation and orchestration capabilities. • Reduced incident response times and manual intervention. • Improved internal collaboration and overall security posture.
Alerts	Provide automatic notification about operations, such as failed jobs. Alerts are displayed on the Triggered Alerts page and defined users receive an email notification.	Get actionable alerts in various forms: Email, SCOM (Systems Center Operations Manager), SNMP (Simple Network Management Protocol), webhooks, etc.
Dashboards	Display a preview of the most critical information gathered from all the CommServe computers in your organization, such as SLA percentage, capacity usage, and backup strikes.	Cloud Command provides a single unified view of data protection for on-premises & SaaS. It provides security, capacity, and usage dashboards globally. The Commvault Security Health Assessment, Commvault Command Center, and Unusual File Activity dashboards provide additional insights.
Orchestration Tools	Create orchestrated workflows to respond quickly to ransomware events. Even integrate with third-party vendors.	<ul style="list-style-type: none"> • Easily create workflows for pre-/post- backup commands. • Workflows through command-line interface, REST APIs, PowerShell Modules, and Python SDK. • Integrate with Splunk, ServiceNow, Ansible, or Terraform.
Proactive Threat Response	Actively defend data recoverability by alerting security the moment the attacker begins.	Threat sensors are deployed around valuable assets (such as file servers, databases, VMs, etc.) to create decoys within your environments. Get highly accurate alerts the moment an attack begins.



05 RECOVER 1 – 2

A recovery process begins once threats are identified and a proper incident response isolates and removes the malware. It is crucial to ensure that all impacted data is restored to normal operating conditions from the point in time before the cybersecurity incident occurred. Proactive and reliable recovery tools and options across the broadest workload coverage are proven to reduce downtime, thwart data loss, and accelerate response times for unrivaled business continuity. The recovery plan begins after the root cause is identified and files are restored with the intention that proper security tools will mitigate any future potential impacts. During the recovery phases, it is essential to only recover clean files from all affected technologies.

RECOVER KEY COMPONENTS	RANSOMWARE REQUIREMENTS	COMMVAULT CAPABILITIES
Hybrid Multi-Cloud Recovery	Recover data quickly from anywhere, whether on-prem or in the cloud.	Automate and recover to different hypervisors, hyperscalers, or other platforms.
High Availability	With the CommServe LiveSync feature, keep the CommServe server ready for disaster recovery and provide the ability to quickly failover to a designated standby host in the event of a disaster.	The Commvault LiveSync feature enables the backup of catalogs and other critical workloads.
Incident Response Recovery	Allow incident response teams to securely recover data for data forensics.	<ul style="list-style-type: none"> Orchestrate out-of-place recoveries to an isolated clean room environment. Run pre-/post-scripts and workflows to validate and scan key data.
Malware Scanning	Validate backup data is recoverable and that there are no threats within the content.	<ul style="list-style-type: none"> Live mount VMs using application validation to securely run scripts and scan VMs for malware. Scan for threats before they spread with AI/ML, anomaly detection, and malware signature scanning.
Curated Recovery and Sanitization	Reduce data loss through a consistent, sanitized recovery by removing suspicious files and knowing the exact point in time from which to bring about healthy file recovery.	Remove, isolate, and quarantine suspected files through anomaly detection, and sanitize backup content by browsing and removing threats.
Proactive Recovery	Surface and remediate threats before they reach their target.	With Metallic® ThreatWise™ deceive bad actors, divert their attacks toward fake assets, get immediate visibility into attacks, and remediate threats early – before they reach your data.



RECOVER KEY COMPONENTS	RANSOMWARE REQUIREMENTS	COMMVault CAPABILITIES
Recovery Validation	Plan, implement, validate, and show demonstratable evidence of recovery readiness.	<ul style="list-style-type: none">• Validate backups continuously or periodically to detect corrupted backups early in the cycle.• Prove and demonstrate recovery readiness without disrupting operations.• Reduce recovery testing complexities by eliminating manual steps.
Recovery Forensics	Perform forensics securely in isolated networks without causing further infections.	<ul style="list-style-type: none">• Use File Data Analysis to detect files that may be encrypted or corrupted by malware to ensure you are not backing up infected files.• Incorporate threat analysis to detect malicious content in the backed-up data at the time of restore to ensure you are not risking reinfection of production systems while restoring from the last good point-in-time on backups.
Recovery Orchestration	Disaster and cyber recovery orchestration with automated compliance reporting.	<ul style="list-style-type: none">• One-click recover clean copies across workloads to production after validating and sanitizing recovery points.



COMMVAULT IS DATA, PROTECTED.



Commvault multilayered security consists of feature sets, guidelines, and best practices to manage cybersecurity risk and ensure readily available data. For information on Commvault's core platform, check out [Commvault Complete™ Data Protection](#) and [Metallic® SaaS Backup](#). Our multilayered security approach is enhanced through integration with:

[METALLIC® RECOVERY RESERVE™ >](#)

[COMMVAULT® HYPERSCALE X™ >](#)

[COMMVAULT® THREAT SCAN >](#)

Be proactive and strengthen your security posture against ransomware attacks by adding

[METALLIC® THREATWISE™ >](#)

[COMMVAULT® RISK ANALYSIS >](#)

[COMMVAULT® AUTO RECOVERY >](#)

And last but far from least, assess your level of protection against ransomware attacks by taking the free

[COMMVAULT® RISK ASSESSMENT >](#)

Learn More About Cyber Security

COMMVAULT.COM/RANSOMWARE >

commvault.com | 888.746.3849 | get-info@commvault.com

z7solutions.com | 407-605-5845 | office@z7solutions.com

