

Commvault Ransomware Protection and Response Services

Offering overview

By 2025, ransomware attacks are predicted to cost businesses an estimated \$10.5T annually in lost revenue, brand impact, and missed opportunities.¹ In a 2021 Proofpoint survey, 65% of CISOs feel at risk of suffering a cyberattack.²

Minimizing such attacks' impact requires a comprehensive readiness plan to prepare for and respond to potential outages.³

Being Recovery Ready means you have the confidence and ability to quickly address ransomware issues across your environment, across physical servers, virtual machines, and various cloud platforms. You support multiple data-recovery tiers – extending into applications, endpoints, and more – to meet your workload Service Level Agreements (SLAs). From prevention to disaster recovery, you want your data protected and available when needed, and you want the freedom to choose the infrastructure types that best fit your needs and budget.

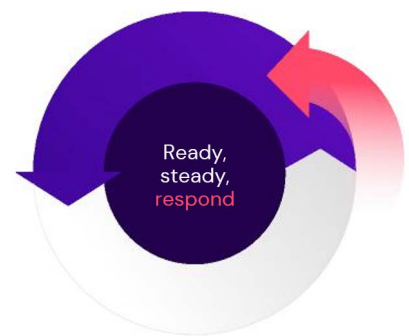
Key benefits of the Commvault Ransomware Protection and Response Services

Your Commvault data protection and management solution plays a critical role in your multi-layered security and recovery plan but recovering from an attack requires more than great technology.

Commvault Ransomware Protection and Response Services provide the resources and expertise needed to harden your Commvault solution from an attack, review the state of your environment over time, and help you return to normal business operations when an attack does occur.

As part of the Commvault Readiness Solutions, these services are designed to provide the service level that best aligns with your business requirements. If you are interested in securing your data protection solution ahead of a potential attack, the Commvault Ransomware Protection and Response Services will help you determine your organization's state of "Readiness" and provide a roadmap to help you better protect your data and provide higher levels of recoverability if an attack does occur.

If you are more concerned about ensuring you have access to the data recovery experts when an attack occurs, the Commvault Ransomware Response Service is a just-in-time offering that will help you return to normal business operations as quickly as possible.



¹ 2019 Official Annual Cybercrime Report, sponsored by Herjavec Group, Steve Morgan, Editor-in-Chief.

² Proofpoint, Voice of the CISO 2021 Report, May 12, 2021

³ While every effort is made to detect and protect against ransomware while enabling full recoverability, these services cannot guarantee absolute protection or recoverability

Commvault Ransomware Protection

Commvault Ransomware Protection and Response Services are designed to provide the service level that best aligns with your business requirements. The three components of this offering provide the resources and expertise needed to harden your Commvault solution from an attack, review the state of your environment over time, and help you return to normal business operations when an attack does occur. The Services are comprised of:

- Ransomware Protection Design and Plan
- Ransomware Protection Review
- Ransomware Response

1. Ransomware Protection Design and Plan

Your data must be available for your organization to be successful. When it is unavailable, or worse encrypted by ransomware, brings business processes to a halt. You must maintain data access with a strategic recovery solution to protect your organization's reputation, provide enhanced customer experience, and help provide business continuity. Ultimately, it all boils down to can you recover confidently?

Commvault empowers you to recover intelligently through holistic risk-mitigation and prevention strategies to assist you to become more than ready for any eventuality. The result is you can quickly recover from events — like ransomware — or anything else that could threaten your operations, systems, users, or customers.

Commvault's Ransomware Design and Plan offering will help you understand potential threats and risks impacting your ability to "Be Ready." By understanding the current state of your recovery solution, Commvault will help identify gaps in your solution and propose a path forward so that you are ready in the event of a ransomware attack or other disaster.

This offering examines and reviews the recovery capabilities of your solution relative to your business requirements and helps align Commvault's technical capabilities with your recovery objectives.

Commvault Ransomware Design and Plan will deliver:

- Readiness scorecard
- Key findings
- Prioritized action plan
- Readiness architectural design and roadmap recommendations

2. Ransomware Protection Review

External threats are continually evolving. Protecting against them requires diligence and constant attention to detail.

Commvault's Ransomware Review offering validates your recovery solution and can verify previous recommendations have been implemented and that no adverse changes have occurred. This review process includes an objective scoring of your Readiness so that you can quantify your risk exposure and take corrective action as needed.

In the review phase, Commvault will conduct a Ransomware Protection workshop and review the environment, comparing it against the initial scorecard and plan. The output will be:

- Updated Readiness scorecard
- Key findings
- Prioritized recommendations

3. Ransomware Response

Commvault understands that a ransomware attack or other disaster means all eyes will be focused on the IT organization — the ability to resume normal business operations as quickly as possible is a defining moment for most leaders. When you experience an event that impacts your organization's ability to operate normally, you need immediate assistance.

As a customer of Commvault's Ransomware Protection and Response Services, you will have immediate access to a knowledgeable and experienced Response team to help you identify the problems and initiate the process of restoring normal operations.

Commvault Ransomware Response Service is included as part of the Ransomware Protection and Response Services. It is an on-demand service that provides operational expertise and resources necessary to help you recover critical data following a ransomware attack.

Key program activities and benefits

Activity	Description	Benefit
Ransomware Protection Design and Plan	Identify the gaps and risks limiting your ability to "Be Ready." Develop a roadmap and plan to address those risks.	<ul style="list-style-type: none"> Validates the Commvault solution is ready to sustain both ongoing protection and recovery activities Identifies features to maximize application security Identifies tools and processes to expedite recovery Identifies solution ability to support RTO/RPO of critical systems and applications
Ransomware Protection Review	Validate that Commvault solution continues to meet your business requirements despite an evolving threat landscape.	<ul style="list-style-type: none"> Assure key stakeholders that Commvault Solution remains operationally ready to support recovery activities if/when needed
Ransomware Response	Ransomware Response team guides, supports, and manages the recovery of critical systems.	<ul style="list-style-type: none"> Experienced Commvault resources to help navigate the recovery process Real-world recovery experiences and Commvault best practices accelerates recovery process Additional resources are available for operations, allowing customers to focus on critical business functions

Applicable terms and conditions will be created for each customer. While every effort is made to protect against ransomware attacks and enable recoverability, these services cannot guarantee protection or recoverability.

To learn more about Commvault Readiness Solutions, please visit commvault.com/readiness-solutions >