

Ransomware Protection for a Safe Digital Transformation Journey

Digitally transforming your company is what brings new business to your front door. It allows you to take advantage of new technologies, better serve your customers, innovate, and gain a financial advantage. The digital transformation journey starts as workloads evolve to keep up with the changing market demands and business needs of your IT organization. But it can present risks to your organization:

- Data scattered across multiple platforms leading to data sprawl
- Complexity from managing multiple generations of data
- Vulnerability to ransomware and other cyberattacks

Plan to succeed

“Of businesses who pay the ransom and regain access to their data, forty–six percent found their data to be at least partially corrupted and unrecoverable.”¹

Ransomware used to be viewed as something that could happen. Unfortunately, today the reality is it will occur. Therefore, minimizing the impact of a ransomware attack must be a high priority when undergoing digital transformation.

Consider this all-too-familiar scenario: your organization’s data suddenly becomes encrypted and your files are erased or blocked until a ransom is paid. Even by paying the ransom, which is not recommended, there is no guarantee that you will recover all your data. Should you regain access to your data, it could take months to completely restore it without the right disaster recovery solution.

Fortunately, there’s plenty you can do to avoid this untenable situation. For starters, choose a data protection and management solution that offers advanced ransomware protection – one that can help you do these three things:

- 1 Reduce your available attack surface to decrease the risks of cyberthreats.
- 2 Detect unusual behavior before a threat impacts your IT environment.
- 3 Quickly recover data in the event of an attack to resume business operations.

Comprehensive data protection and management

Mitigating ransomware–related risks requires a comprehensive data management solution that provides wide–ranging data insights, broad workload coverage, and security capabilities. Having your data protected at this level and available during your digital transformation is critical for avoiding data loss, especially when your data is being migrated between on–prem and multiple cloud environments. To bring about a successful digital transformation, you must know at all times what data you have, its impact on business operations, where it is stored, and that it’s secure.

¹ Group, Global CTI. “The True Cost of a Ransomware Attack” 2022

Commvault Complete™ Data Protection combines support for the industry’s broadest workload coverage with resilient ransomware protection. It helps you move your evolving data across every type of infrastructure with confidence, knowing it is protected, secure, and recoverable from a ransomware attack. This ensures data availability and business continuity across your on-prem and cloud environments – all made possible by using a single, extensible platform that conforms to your digital transformation strategy.

Testing your ransomware protection? Let us do the heavy lifting.

Commvault® Professional Services provides the resources and expertise needed to harden your Commvault solution against ransomware attacks, review the state of your environment over time, and help you return to normal business operations should an attack occur. Through our Commvault Ransomware Protection Services, you choose the service level that best aligns with your business requirements. Service offerings include:

- **Ransomware Protection Design and Plan** 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.
- **Ransomware Protection Review** validates your recovery solution and helps verify the implementation of previous recommendations and that no adverse changes have occurred.
- **Ransomware Response** provides immediate access to a dedicated response team in the event of an attack to help you identify the problems and initiate the process of quickly restoring normal operations.

Move the right data and reduce your attack surface

Accelerate migrations and reduce your ransomware attack surface with Commvault® File Storage Optimization. Commvault provides insights into your unstructured file data, allowing you to easily identify and exclude redundant, obsolete, and trivial (ROT) data before migrations – shrinking your attack surface, accelerating migrations, and ensuring that you only move the right data.

Gain peace of mind with air gapping

Commvault helps you easily safeguard your data from outside threats such as ransomware by implementing air gapping. Use Commvault’s fully integrated, secure, and scalable cloud storage solution Metallic® Recovery Reserve™ to create a virtual air-gapped, immutable copy of your data – ensuring your business-critical data is always safe from ransomware attacks.

Take the next step. Learn more.

Don’t let a ransomware attack bring your digital transformation initiatives to a screeching halt. Commvault offers proven solutions to protect your critical business data and ensure business continuity – regardless of workload type or location. Get the power of Commvault on-prem data protection AND the convenience of our Metallic SaaS solutions – all through one simple, unified data management platform.

How prepared is your organization for a ransomware attack? Get the answer by taking our [free risk assessment >](#)