

Be Prepared For Ransomware Recovery



“According to a poll by CSO, the rate and variety of cyberattacks are growing every year, and it is already the largest financial threat to most businesses. Estimates suggest that by 2021, the total cost of cyberattacks will hit \$6 trillion”

Ransomware Landscape

Cyber-attacks like Ransomware are becoming extremely popular in specific verticals like healthcare, education, and municipalities. This trend is due to several different reasons, amongst which the two important ones are:

- Lack of dedicated resources (human resources or tools) aimed at protecting against threats
- Higher ransom payout rates

If a ransom is not paid for a few days, these verticals come to a standstill, and 93% of businesses end up filing for bankruptcy(1). Even though individual victims do end up paying the ransom, the attackers may not end up decrypting the files. Ransomware attacks are becoming increasingly sophisticated and pervasive, often using multi-tiered, as-a-service deployment models targeting not just live production data but also backup servers and secondary copies. Attackers monitor for backup credentials and end up either encrypting or deleting them. As a result, many victims not only lose access to their primary data but cannot recover from their traditional backups. In most data protection environments, backup applications are vulnerable to bad actors and malicious software due to their architectural dependency on conventional servers and file systems.

A typical, layered approach to the ransomware threat looks at the problem from different angles – prevention, detection, mitigation, and recovery. Read further to learn how Clumio uniquely provides key capabilities around mitigation and recovery in response to the threat of Ransomware, which we summarize as the

Essential Pillars for the Cure:

- Air-Gapped Copy of data, independently secured using cloud-native services
- Immutable Backups stored on encrypted, highly durable object storage
- Rapid recovery enabled by cloud microservices which scale on demand, independent of customer infrastructure
- Cross restores that allow customers to recover to alternative locations, domains, or infrastructure flexibly

Clumio Essential Pillars to Cure Ransomware



The Solution

During backups, Clumio uses a secure, stateless cloud connector to directly write all backup data, encrypted in transit, to an immutable object store that resides in the Clumio service, whereby we enable:

Air-Gapped Copies

- The data, metadata, and catalog are stored in separate locations where any compromise in the customer environment does not compromise data secured in Clumio. Backup data can only be accessed through the Clumio UI or REST API calls. The requests go through multiple checkpoints to validate the origin of initiation and appropriate permissions. The customer has neither direct access nor root permissions to the backup data and catalog. There's no filesystem or storage location to mount, which could put existing data at risk in cases of user error, software bugs, or malicious intent. For additional protection, all Clumio customer accounts are secured independently by encrypting data at rest with unique rotating keys.

Immutable Backups

- Backups written to Clumio can never be overwritten. Using a secured S3 object store, Clumio leverages an append-only write structure with versioning enabled, so overwrites or updates create a new version of the object, leaving the original version intact and unharmed. New data is stored in new locations within the S3 object store that provides (11) 9s of durability.

Rapid Recovery

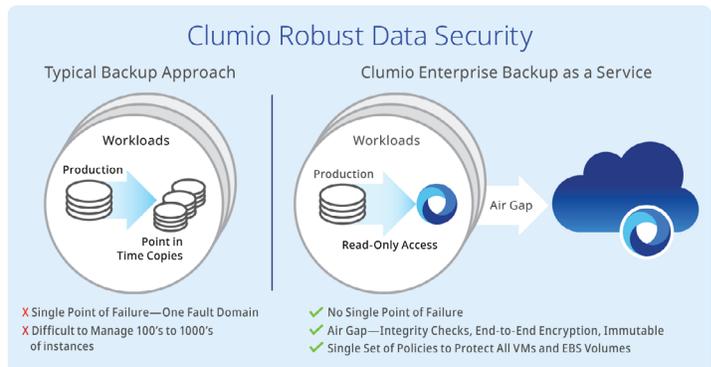
- Quickly restoring data is not dependent on having any stateful backup infrastructure deployed on the customer side. For full virtual machine restores, we can also reduce recovery time using highly parallelized restore functions and delta-based transfers of unique data only.

Cross Restore Capabilities

- All of Clumio's backup and restore services can be enabled for alternate locations, data sources and targets as part of the typical workflow, providing the utmost in fast, flexible recovery capability.

Clumio's isolation of backups in the cloud is much like sending backup tapes to a physically secure facility without the tapes, trucks, and lost data, of course.

We also add the functional equivalent of shipping a pristine backup catalog to an additional secure location, independent from backup data. Clumio provides a significant advantage over shipping tapes by enabling immediate online restore capability with layered immutability, which facilitates reliable and efficient recovery.



A Hardened Cloud Data Protection Approach

The necessity of securing backup data is more critical today than ever before. As the conversation changes from data protection to highly secure data protection, Clumio's SaaS offers many significant advantages over traditional data protection approaches. At the core of this approach, Clumio literally protects the customer data from the customer to ensure that a bad actor with assumed administrative credentials cannot harm the recorded backups in the customer's history. By building our platform using loosely coupled cloud native services with a layered security model and affinity for serverless compute, we offer scale, immutability, and flexibility beyond traditional fixed backup servers, appliances, and persistent shared storage. Clumio's approach is an intentional departure from backup platforms that were designed only with traditional data center workloads in mind, which are hindered by a scarcity of resources and inefficient scaling when responding to new demands of hybrid cloud environments. The added complexity and cost of trying to adapt these archaic approaches only increases the risk profile for organizations that need the utmost in protection for all their essential data assets, regardless of where they reside.

Clumio's mission is to provide a unified, comprehensive data protection strategy for modern SaaS applications and hybrid cloud infrastructures. Clumio dramatically changes the data protection landscape by offering a solution that offers a simple, secure, and predictable consumption model for backup, recovery & data management.