Crack the Code on Cloud Data Protection Costs

CLUMIO

You moved to the cloud for savings, not to scratch your head wondering about high cloud bills. Good news, it's avoidable—read on.

Let's Get Cracking with Some Important Questions:
When it comes to your cloud storage costs and data protection, here's what you need to consider:

- Are you, or will you be paying for more operational recovery capacity than you need?
- It's time to re-evaluate your data protection strategy:
  - Can you safely recover from a ransomware attack and still meet or exceed your RTOs?
  - Are you able to meet compliance mandates?
- How can you get more value from your data protection strategy, and pay less for it?

> "Clumio seamlessly handles operational recovery while significantly reducing our snapshot costs. We now have line of sight to significantly reduce our TCO for long-term data retention"
>
> **Brian Cahill**
> Director, Technology, & Dev Ops Frogslayer

Don't Assume Your Data is Protected

Many enterprises assume AWS has their data protected. But if you look at the AWS shared responsibility model, that's not their job—that's yours. AWS offers snapshots for some level of data protection, but you don't have to learn the hard way that snapshots are neither cost-effective nor adequate for data protection.

Let's face it, traditional, on-premise methods are costly and complex for the cloud, for example:

- Snapshots replicated to a storage array
- Snapshots backed up to a secondary site
- Backing data to an offsite data center

Data continues to grow exponentially and compliance requirements are not going away. Enterprises require the same level of resiliency, recoverability, and retention in the cloud.

Crack the Code on Cloud Data Protection Costs

Snapshots Were Built for Storage Systems

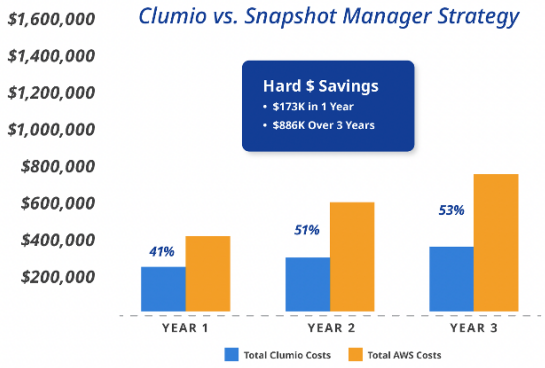
Snapshots were built for enterprise storage systems, not the cloud. While they offer some operational recovery, they fail to deliver full data protection and are inefficient for long-term data retention.

Snapshots are point-in-time data copies that offer quick operational recoveries from accidental deletions or data corruption. But in the case of more catastrophic threats, like a ransomware attack—snapshots will leave you exposed. With the cloud, IT teams must oversee and manage snapshots to ensure data consistency and integrity to meet RTOs.

Unfortunately, snapshots are not as simple when it comes to the cloud—often requiring scripting and other workarounds. With AWS, IT must tediously manage, tag, and catalog snapshots to ensure data consistency for a quick recovery.

Snapshots are 2-5x More Expensive

Snapshots are not true backups, but cumulative, real-time copies of a data set, generated at multiple points in time. Every time a block or file is changed, a new snapshot is generated—quickly multiplying snapshots, costs, and storage requirements. Creating and retaining snapshots for long periods can significantly increase your overall bill.



Do you want to get to the bottom of your cloud spend? We can help you crack the code on your bill and show you ways to save between 30-50% on your data retention costs—and be compliant. If you haven't transitioned yet, we can help you cost-effectively transition to the cloud.

Let's talk.

CLUMIO