ActualTech Media

CLUMIO

Recovering from Ransomware Attacks

Dan Sullivan

IN THIS PAPER

Ransomware attacks are growing more prevalent, driven in part by the availability of ransomware software on the dark web and the promise of quick and easy money. Attackers analyze network infrastructure to learn about backup procedures and where those backups are kept, so traditional backups are not sufficient to address the risk of ransomware.

Air-gapped backups—backups stored outside the infrastructure or security sphere of the enterprise in a separate service with immutable, highly durable storage—keep data out of the reach of bad actors and ensure your ability to quickly recover or redeploy when a proper response plan is in place. This brief discusses why it's a logical choice.

> Just as a good driver still wears a seat belt, an organization needs to be prepared for a successful ransomware attack.

Highlights include:

- Top attack vectors
- Why you should separate your backups
- Reasons it makes sense to use a secure backup service
- Why rapid recovery is critical to have

Anyone with an Internet connection knows that ransomware attacks are growing ever more prevalent each and every day. The ransomware attack on the Colonial Pipeline in May 2021 demonstrated how far-reaching such a strike can be: 5,500 miles of pipeline carrying 45% of U.S. east coast fuel was shut down for four days before operations could be completely restored.

Darkside ransomware used in the Colonial Pipeline attack is an example of *crypto ransomware*, which encrypts files and data. *Locker ransomware*, the other form of ransomware, prevents users from accessing an infected device, but doesn't actually alter or encrypt the data. This means a storage device could be moved from a compromised machine to a safe system to retrieve the data. Not surprisingly, locker ransomware isn't as effective in securing payments from victims and most attacks today employ crypto ransomware.

Common security practices aren't sufficient to defend your organization against ransomware attacks and as organizations expedite their movement to the cloud, the need to ensure data is protected is paramount. Just as a good driver still wears a seat belt, an organization needs to be prepared for a successful ransomware attack. Likewise, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) recommends that organizations have the right data protection or backup strategy to defend and recover against a successful ransomware attack.

> Snapshots are essentially backups that are typically stored within your infrastructure or security sphere. This makes them vulnerable, as both your source and backup data can be compromised in an attack. A better approach is to separate your backups from your source data.

Snapshots Are Not Enough

In the public cloud most enterprises confuse snapshots, providing operational recovery, as backups that will protect your data from ransomware. Unfortunately, this couldn't be further from the truth. Snapshots work well for operational recovery, but fall significantly short when it comes to ransomware protection. Others try to leverage traditional backups, not optimized for the cloud, which drags the complexity of on-premises into the cloud and has the perpetual threat ransomware poses of modifying the backups making them useless.

> Native snapshot-based data protection in the cloud is not an air-gap solution, since snapshots are created in the same account as the primary data.

Snapshots are essentially backups that are typically stored within your infrastructure or security sphere. This makes them vulnerable, as both your source and backup data can be compromised in an attack. A better approach is to separate your backups from your source data.

Not All Backups Are Created Equal

What's needed to safeguard this important data is an "air-gap backup," in which backups are stored in a separate service or vault outside the reach of hackers (see **Figure 1**). While it might initially seem that the public cloud provides secure backups, there are some key gaps when it comes to protecting against ransomware. For example, when you use AWS backup to protect your AWS data, the snapshots created are all stored in the same account as the primary data. This is not an air-gap solution. These backups can also be modified or deleted that makes it easy for an attack to play out. Additionally, there will be high storage and egress costs for copying data from one account to another account (or cloud) to separate the primary data from its backup.

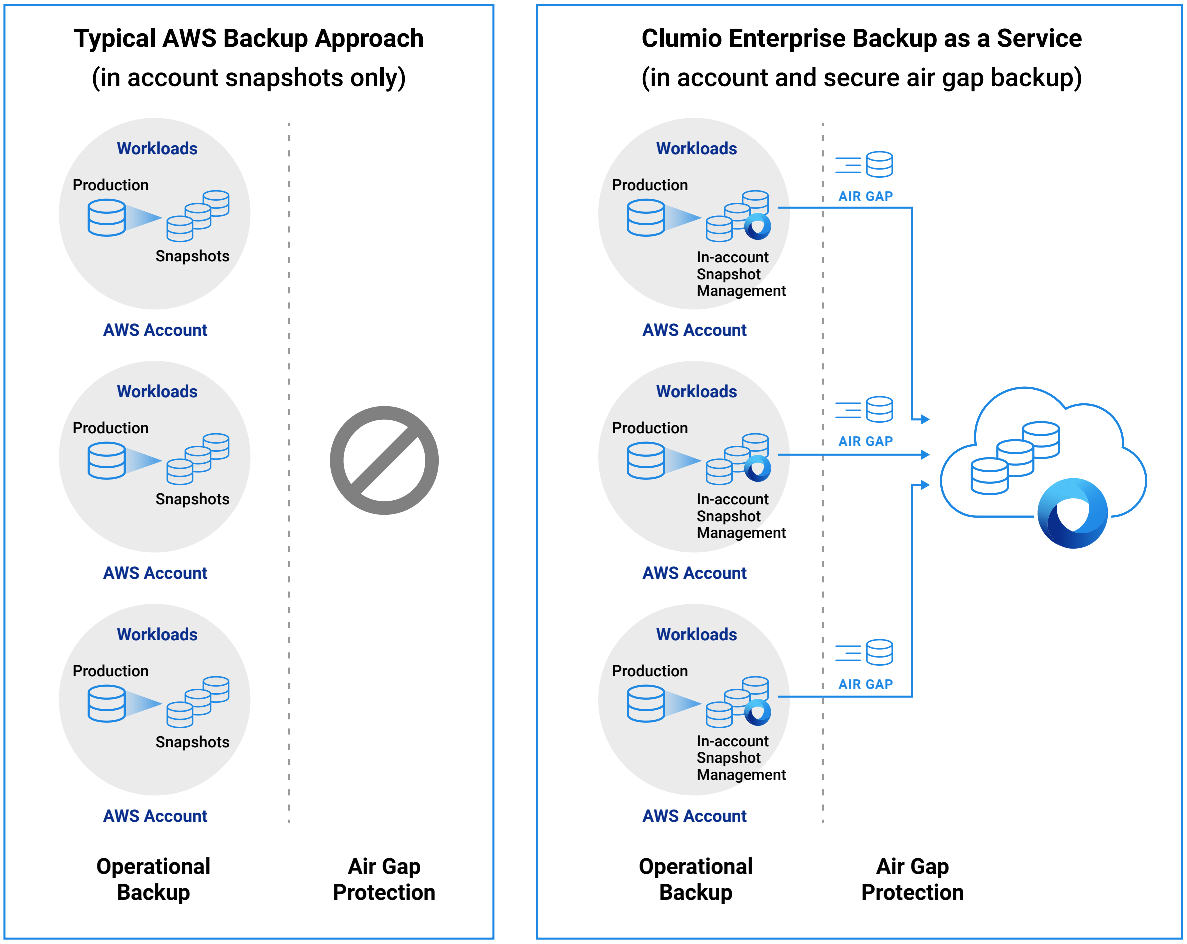

Figure 1: Clumio's solution to backup and restore is less prone to failure, and more secure, in addition to being a SaaS offering, freeing up your IT staff

In computer networking, an "air gap" is a security practice that separates networks so traffic can't flow between them. An air gap can be physical, such as two local area networks that have no connection, or it can mean isolating access to a part of a larger network, such as when cloud customers create virtual private clouds. In the first case, traffic can't get through because there are no physical links between the networks. In the second scenario, traffic is blocked by firewalls, access control rules, and other measures that prevent traffic from flowing into restricted parts of the network.

Consequently, it can become quite expensive and complex to back up data to a different cloud or a different region within a cloud. The bottom line is that native snapshot-based data protection in the cloud is not an air-gap solution, since snapshots are created in the same account as the primary data. Thus, much like traditional backups, native snapshot solutions don't provide sufficient protection for ransomware attacks.

Air-gap isolation alone is not even enough to protect your organization from ransomware attacks. It's important to have a security-first mindset that includes immutable backups to prevent internal bad actors or operational mistakes from destroying your backups. Administering backups should also be protected by multifactor authentication. Of course, backups should be encrypted and you should have the option to use your own keys as needed.

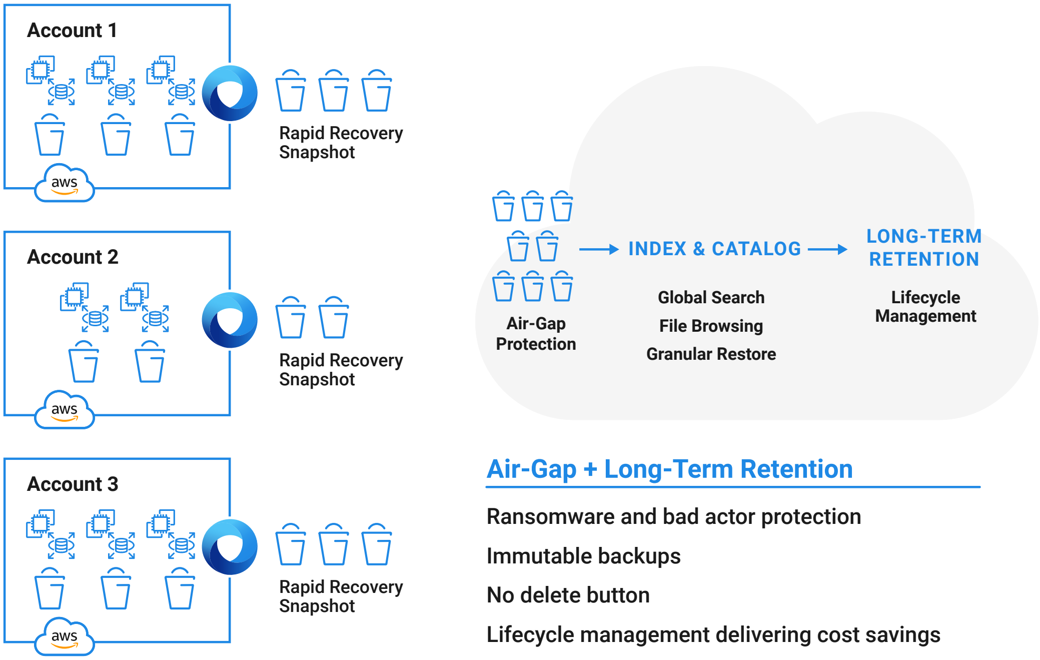

Figure 2: Clumio Protect provides true air-gap defense, in addition to other security features to protect against ransomware attacks

It's important to understand the difference between RTOs and RPOs. RTOs specify the time from the loss of a service to the time the service has been restored. Business requirements will dictate appropriate RTOs. For example, a health insurance company may have short RTOs for systems used by doctors, pharmacies, and other health care professionals to query information about insurance coverage. That same company may have a significantly longer RTO for the batch reporting systems used by the human resources department.

RPOs specify what state systems should be in when recovery is complete. This includes having applications available, as well as having data up-to-date. Like RTOs, RPOs are driven by business requirements. A data warehouse, for example, may have an RPO of restoring data from 24 hours before the failure because the more recent data can be recreated by rerunning daily data load procedures. However, a transaction processing system, such as a sales and order management system, would need to be restored to nearly the time of the system failure.

Ransomware Recovery with Clumio

Another key element in mitigating the impact of ransomware attacks is the ability to rapidly recover data that has been encrypted or otherwise compromised. We typically describe recovery plans in terms of recovery time objectives (RTOs) and recovery point objectives (RPOs).

One solution to the drawbacks commonly found in backup services is Clumio Protect, a secure backup as a service that provides turnkey air-gap plus immutable backups and fast, cost-efficient recovery protection (see **Figure 2**). Clumio Protect eliminates new hardware investments, the need for additional in-account cloud resources (for example, Amazon EC2 instances or Amazon EBS storage), infrastructure maintenance, support or maintenance fees, and egress charges on restores.

It not only provides air-gap backups of your data but provides rapid and granular recovery from an attack—customers can recover individual files, records, or specific entries from a database table instead of recovering an entire instance or snapshot. This reduces attack recovery times from hours or days to just a few minutes and enables business continuity.

To learn more about how Clumio can help secure your organization's data from ransomware, visit https://saas.clumio.com/ransomware.