More info: www.agya.cloud

Cloud Continuity
Ransomware Recovery

// Solution Overview

Description

The effects of ransomware on the business landscape include data loss, regulatory fines and reputation damage—to name a few. When such an attack happens, victims have one of two choices:

1) pay the ransom and hope the cybercriminal unlocks your data or

2) replace the infected data with clean copies.

The problem with option 1 is that it encourages the criminal enterprise to persist [1], and it is not guaranteed that your data will be restored. During the encryption process, hackers can accidentally corrupt large chunks of data, making it irrecoverable. And even intentionally, leaving behind dormant malware for future attacks.

The increase in cyber breaches year over year has for good reason made any company leadership uneasy. Companies are recognizing the similarities between cybersecurity incident response and IT disaster recovery preparedness: both emphasize fast response to return operations, attention to data preservation, etc. For this reason, these two professional groups (cybersecurity and disaster discovery) are being asked to collaborate more and more to achieve comprehensive business continuity.

Market competitiveness depends upon digital accessibility, so shutting IT systems off from the exterior world isn't an option. But what can organizations be doing to protect their critical assets against threats of ransomware attacks? Here is a solution using AGYA Disaster Recovery as a Service (AGYA DRaaS).

[1] "Why DRaaS is a Must-Have Offering for Solving Ransomware Incidents," Jeff Ton, SVP InterVision

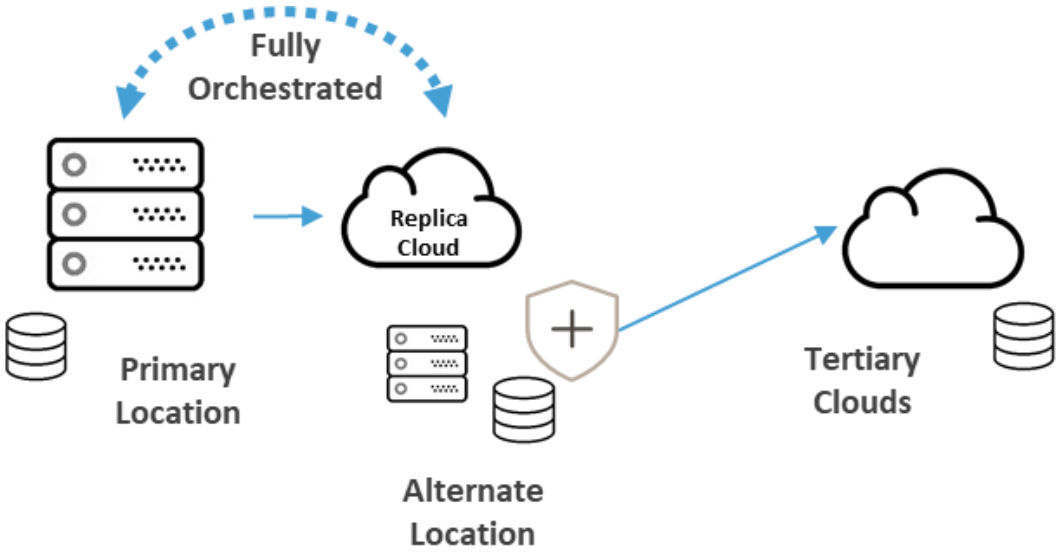
// PRE ATTACK

1 - Create a DR environment…

…and replicate data to the secondary site (alternate location) in real time to ensure data is protected from hardware failures, power/network outages, data corruption, etc..

2 - Scan DR data

In the secondary environment (alternate location), scan for malware as frequently as you wish with no impact on the production servers' performance (on primary location).

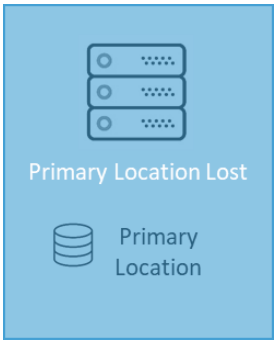


3 – Ensure Clean Data

If, and only if, the Disaster Recovery data is clean of malware, then save the data to a tertiary backup. The third location can be in the same cloud zone, in a second cloud zone, in a second cloud region, or in a second corporate data center.

// ATTACK

When a Ransomware attack happens, production server images and data are encrypted and not available. Often, your backup data is encrypted as well.



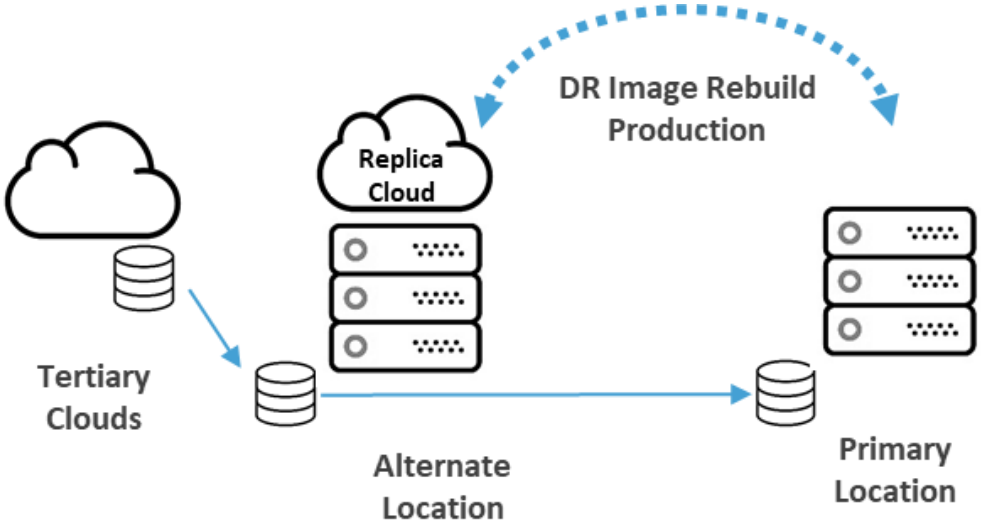
// POST ATTACK

4 - After a ransomware attack

Restore a fresh copy of the data from the tertiary copy into a preserved copy of the systems in DR (operating systems and applications will never be infected)

5 – Final Step. Restore Production

Copy DR OS + App images back into the production environment and replicate DR data in reverse to main systems, and you will have restored production and DR without every paying ransom



<u>Once data is restored, systems are quickly brought back to life in the disaster recovery environment!</u>