Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value

Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value

Has a vendor been talking to you about Isolated Recovery recently? Or have you been thinking about duplicating and air-gapping your infrastructure with scheduled updates to protect against ransomware or cyberattacks? Could there be a less expensive, less complex way to achieve similar benefits?

Recently, we've been hearing these ideas - both from our customers' internal discussions and other vendors' recommendations. Along with that, we've been discussing the real value of these concepts internally with the goal of keeping ourselves technically honest. Let's dive into these ideas to explore the concept of Isolated Recovery, its limitations, and where Rubrik can help.

WHAT IS ISOLATED RECOVERY?

From a network perspective, the concept of air-gapping isn't new. See this overview via Wikipedia if not familiar - https://en.wikipedia.org/wiki/Air_gap_(networking). Simply put, there's physical isolation between two networks - mostly commonly a secured and an unsecured network.

What we're hearing about today from certain vendors as it relates to protecting against cyberattacks and ransomware is not exactly the same thing. While Isolated Recovery shares this "physical isolation" characteristic, it is built on the concept of having a separate datacenter infrastructure that is disconnected from the primary infrastructure via an air-gap. In the case of Isolated Recovery, the air gap is closed on a regular schedule for replication updates. Often large amounts of consulting services are added similar to Business Impact Analysis (BIA) used in Disaster Recovery (DR) planning.

To state the obvious, this can have varying degrees of financial impact, as there's a notable increase in cost and operational complexity any time you duplicate infrastructure; more moving parts means more maintenance, updates, and monitoring. Think of this as being similar to the operational overhead of a DR infrastructure.

More moving parts means more maintenance, updates, and monitoring. Think of this as being similar to the operational overhead of a DR infrastructure.

In an oft-cited document (linked here), the Federal Financial Institutions Examination Council lists air-gap as "another control for consideration" but does NOT list this as a primary or sole recommendation. For better or worse, this document has been selectively quoted at times to focus on air-gapping. We recommend reading the document to be sure - it also lists "periodic read-only data backup" and "other emerging data backup technologies" as worthy of consideration while concluding "The objective of these strategies is to allow financial institutions and TSPs to maintain relatively current data backups without the risk of an attack destroying or corrupting the backup data."

In theory, if your files are encrypted by ransomware, there is complete surety that your "air-gapped" data isn't affected and is available for restore. While this concept has been around in various flavors for years, it's been given new life with the recent explosion of ransomware attacks and the need to "do something, anything!"

IS THERE A REAL BENEFIT?

You might already be thinking about update schedules -- good catch if so. What if the ransomware isn't detected before the scheduled update occurs? At that point, your separate infrastructure hasn't bought you anything despite it's cost and complexity.

> **What if the ransomware isn't detected before the scheduled update occurs? At that point, your separate infrastructure hasn't bought you anything despite it's cost and complexity.**

Even worse, what if the scheduled update happens after a ransomware infection or other attack but before detection? The ransomware may be dormant, specifically to get past regular update windows schedules, and now you have ransomware-encrypted files both places.

On the bright side, what if you do catch the ransomware attack before the scheduled update? You're still dealing with the classic challenge of backup and recovery systems as they relate to ransomware -- the speed of restore. This is due to the time required to hydrate the data, validate that the restore point wasn't infected, and possibly rinse and repeat with a different restore point if so.

In all honesty, we have yet to meet a customer who has experienced real-world benefits with this approach.

WHAT'S THE REAL CHALLENGE?

Based on customer conversations, when considering Isolated Recovery the main challenge people are trying to protect against is undetected ransomware file encryption. Rubrik can help with this challenge in two key areas.

1. Reliability of Data Recovery

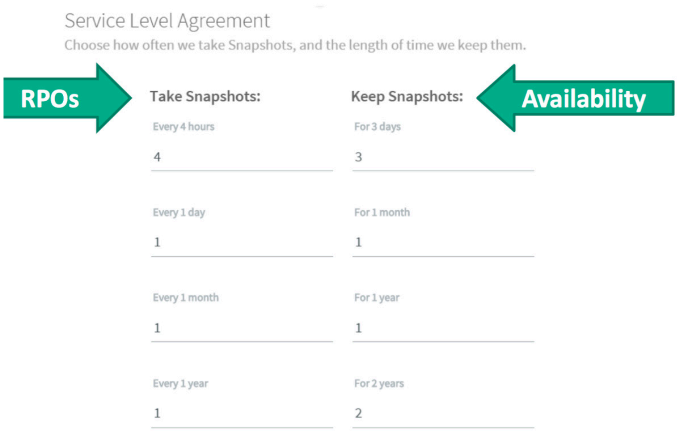
2. Speed of Data Recovery

We recently covered these in depth in the webinar "Ransomware Jail--Is There Any Way Out?" (linked here) but let's explore them briefly.

RELIABILITY OF DATA RECOVERY

While the underlying question is simple - "is my backup data there when I need it?" - the underlying factors are more complex and related to Simplicity of Setup + Day to Day Operations and Immutability of Snapshots.

Simplicity of Setup + Day to Day Operations - this is critical due to the underlying complexity of most backup systems. Any system with many moving parts requires constant inspection to control for the increased likelihood of failure somewhere in the environment - this is the operational life that most backup engineers live each day. Rubrik helps here by being incredibly easy to setup but also simple to run on a day to day basis due to its policy driven nature.



Service Level Agreement

Choose how often we take Snapshots, and the length of time we keep them.

Take Snapshots:		Keep Snapshots:	
Every 4 hours	4	For 3 days	3
Every 1 day	1	For 1 month	1
Every 1 month	1	For 1 year	1
Every 1 year	1	For 2 years	2

Immutability of Snapshots - unlike some other backup systems, Rubrik backups (aka snapshots) are immutable once created. In the words of David Ramos, Security Lead at Rubrik, "no amount of compromise to the machines we back up will cause us to do bad things to existing backups." Regardless of subsequent backups (which may include encrypted versions of previously backed up files), the previous backups are never affected. This was a conscious architectural choice during design of the Rubrik system - more details in this previous blog post.

Additionally, the previous backups are never available in a Read/Write state to the client. Even during a restore of a VM, the underlying backups remain Read Only. This prevents ransomware from being able to access and encrypt backup data.

> **Immutability is critical - it's what allows Rubrik to meet and exceed the benefits of an air-gap environment for your backup infrastructure without the operational complexity and higher cost of Isolated Recovery.**

Additionally, even if someone compromises your production infrastructure and deletes items (VMs, file systems, databases, etc.), we do not delete the related backups. Instead, they are turned into "relics" inside of Rubrik and aged out over time based on the pre-assigned policy.

SPEED OF DATA RECOVERY

This is where the rubber meets the road - if you have your data, can you restore it quickly enough ~~to avoid major financial~~ or reputational impact to your organization? If not, you will be faced with the challenging business decision of choosing to pay the ransom to get online - this is the exact decision Horry County School District and many others have faced.

Rubrik's capabilities apply to this area in two ways.

1. Speed of restore via live mount
2. Automation/API to enhance restore capabilities.

Live mount focuses on the capability to make backup data available instantly without a traditional restore process. This is done by instantiating one or more VM's live from the Rubrik system into the vSphere environment without having to restore or rehydrate the data.

Having a native REST API allows much greater flexibility in restoring to recover from a ransomware attack. As stated by Matthew Day, ICT and Support Manager at Langs Building Supplies, "We were able to write a script to restore files back to the VM from the latest version of the file because of our backup. We had all of our files back to the file server in approximately one hour. No damage done."

See the case study attached to this document for further details as well as a video case study linked below.

Langs Stops Ransomware Attack with Rubrik

FLEXIBILITY VIA API

Despite the commentary above, Rubrik can as well provide options for air gap infrastructure with scheduled updates via integration with the REST API. While we believe the discussion above covers most use cases, an external orchestration engine (such as vRealize Automate or others) can easily be leveraged to trigger Rubrik replication updates. We're happy to discuss this further if worthwhile for your organization.

BUT THERE'S MORE!

This is definitely a large topic - if you're thinking we've left out some pieces, you're right! Please don't hesitate to reach out to your local Rubrik team if you'd like to discuss further how Rubrik's approach can provide much of the benefit of Isolated Recovery at a fraction of the cost.