WINDVAL

technology solutions

Windval Advisory Services and Technical Solutions

Air Gap: A Modern Approach to Data Security

Windval Solution Guide – April 2020

Accelerate IT Transformation

with a modern approach to disaster recovery and data security.

Introduction

What is Backup and Recovery?

"Backup and Recovery" describes the process of creating and storing copies of data that can be used to protect organizations against data loss such as hardware / software failure, physical event (such as a fire), human error, or a cyber event (ransomware). This data backup and restoration is sometimes referred to as operational recovery and an element of broader organizational disaster recovery strategies.

Backing up data requires an IT organization to copy and archive computer data so that it remains accessible in cases of data deletion and/or data corruption. Storage replication and data snapshots are not proper enterprise backup methods.

Recovery from a backup typically involves restoring the data to the original location, or to an alternate location where it can be used in place of the lost or corrupted data.

Data can only be restored from an earlier point in time if it has been backed up properly.

A Reliable Backup and Recovery Strategy

3-2-1 Backup Strategy: The 3-2-1 backup approach is a reliable recovery methodology for ensuring that data is protected adequately, and backup copies are available when needed.

The basic concept of the 3-2-1 backup strategy is that three (3) copies of the data are made and protected; the data copies are stored on two (2) different types of storage media; and one (1) copy of the data is sent offsite.

"3-2-1" Backup Strategy Rules

3	Three (3) Copies of Data – This includes the original data and at least two backup copies.
2	Two (2) Different Storage Types – Both backup copies of the data should be kept on two separate storage types to minimize the chance of failure. Storage types could include an internal hard drive, external hard drive, removable storage drive, or cloud backup environment.
1	One (1) Copy Offsite – At least one data copy should be stored in an offsite or remote location to ensure that natural or geographical disasters cannot affect all data copies.

Solution Review

Current Challenges and Threats

Experts forecast that cybercrime is the biggest threat to businesses today and that the total costs of attacks will skyrocket to $6 trillion by 2021[1]. Companies need to find new solutions to proactively address the growing cybercrime / ransomware threat and mitigate the risk of loss in their data protection strategies.

Successful strategies require comprehensive planning and the application of multiple security and data protection techniques.

A Modern Approach

One method, in particular, that been discussed and promoted recently is "Air Gap".

While Air Gap is not a new topic or technique, it seems that it is still an interesting area of conversation. Globally, critical systems are typically protected with Air Gap techniques. Examples include military / government computer networks and systems, stock exchange systems, life-critical systems such as Nuclear Power Plant Controls, and journalists working with sensitive information.

What is Air Gap?

Air Gap is an important technique to keep your systems secure, and your files and folders free of malware. Imagine having data on your laptop that is infected with a virus. If that laptop is connected to the network, and those backups are stored on a file server inside of the network that your laptop has access to, there is a very real possibility that your infected laptop will infect the backup copy sitting on the file server, and in turn corrupt everything.

Air Gap Strategy: An air gap backup and recovery strategy means ensuring that, at any given time, one copy of your organization's data is offline (disconnected) and cannot be accessed. If a file or system of files has no connection to the Internet or a LAN, it can't be remotely hacked or corrupted. This enables storage of a secondary copy that is immutable. Cloud backups are becoming a virtual, modern equivalent of air-gapped tape backup, but only if they are truly disconnected.

As discussed earlier, reliable backup and recovery strategies recommend a "3-2-1 Backup Plan". The one (1) is a copy of your data that is stored offsite in a cloud or remote media location. This copy can be made offline if and when required, creating an air gap, disconnected and protected from external hacks.

Is Air Gap Effective?

An Air Gap, or offline strategy, ensures that a copy of your data is physically separate from the primary network.

Unfortunately, there is no guarantee that the air-gapped copy cannot be corrupted during the copy process.

As an illustration, let’s say every evening a backup of your data is created. The next morning, your organization is attacked by ransomware and the data on your device is encrypted by an outside predator. If this ransomware corruption is not caught before the next backup cycle, the encrypted files will simply be replicated and become part of the backup set.

Assuming your backup strategy included an air-gapped copy stored offsite or in a cloud destination, the timing of such replication becomes important. If the ransomware corruption was still undetected at the time when the air-gapped copy was created, the backup set is rendered useless for recovery purposes. Alternatively, if the ransomware attack was detected prior to the creation of the next scheduled air-gapped copy, you would be able to temporarily halt further replication. You could then clean out the ransomware, restore data to a known-good state from backups, and then resume creation of a clean air-gapped copy.

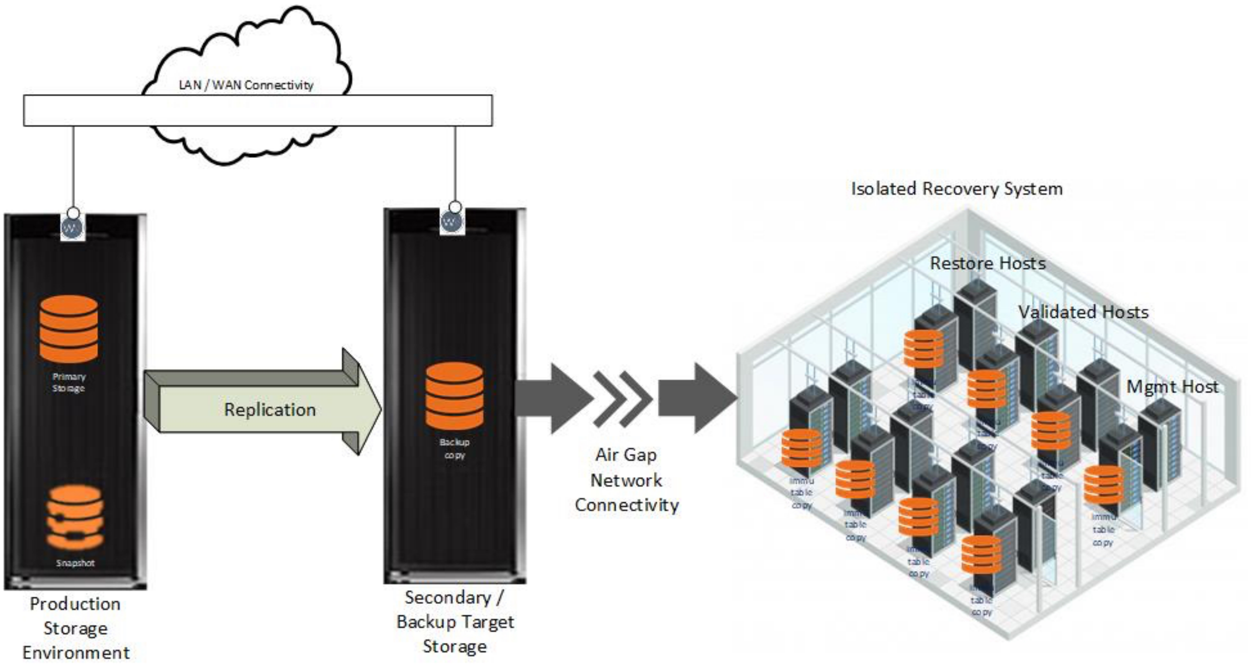
Backup and Recovery Solutions

Backing up data to tape may be a viable approach for data recovery, but is an antiquated approach and and may not be a practical enterprise level component of a modern risk mitigation strategy. Slow restore times from tape may result in missed recovery time objectives.

Alternatively, storing data in the cloud is a modern, cost effective solution, making it an attractive approach. It is important to note however, most cloud providers typically charge for reads rather than writes and retrieving cloud data runs the risk of quickly become a very expensive solution.

Solution Architecture

Air Gap – Array Based Architecture

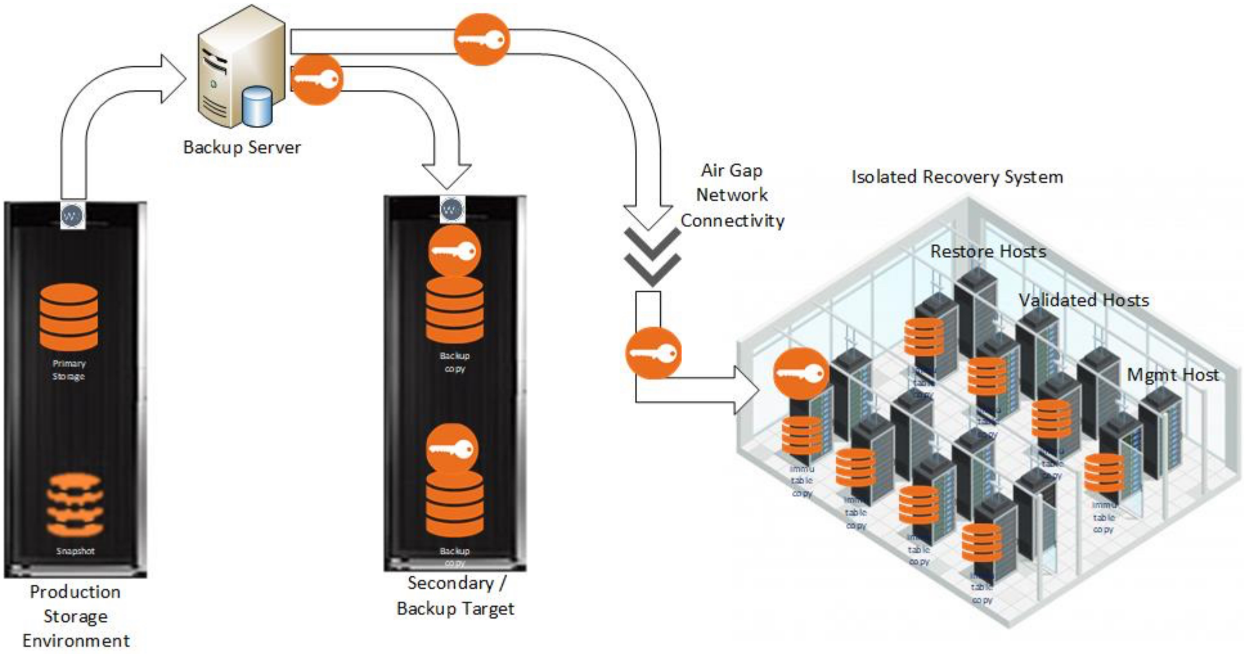


In this traditional, highly capital-intensive model, two disk arrays are configured for replication between them. Replication is scheduled to run at certain times and a network connection between the two systems is opened only during those windows. During the rest of the time, the second array is offline.

Typically, this approach is paired with snapshots to provide the ability to roll back.

The benefit of this approach is fast recovery; however, the cost is typically extreme as two production quality disk arrays are required.

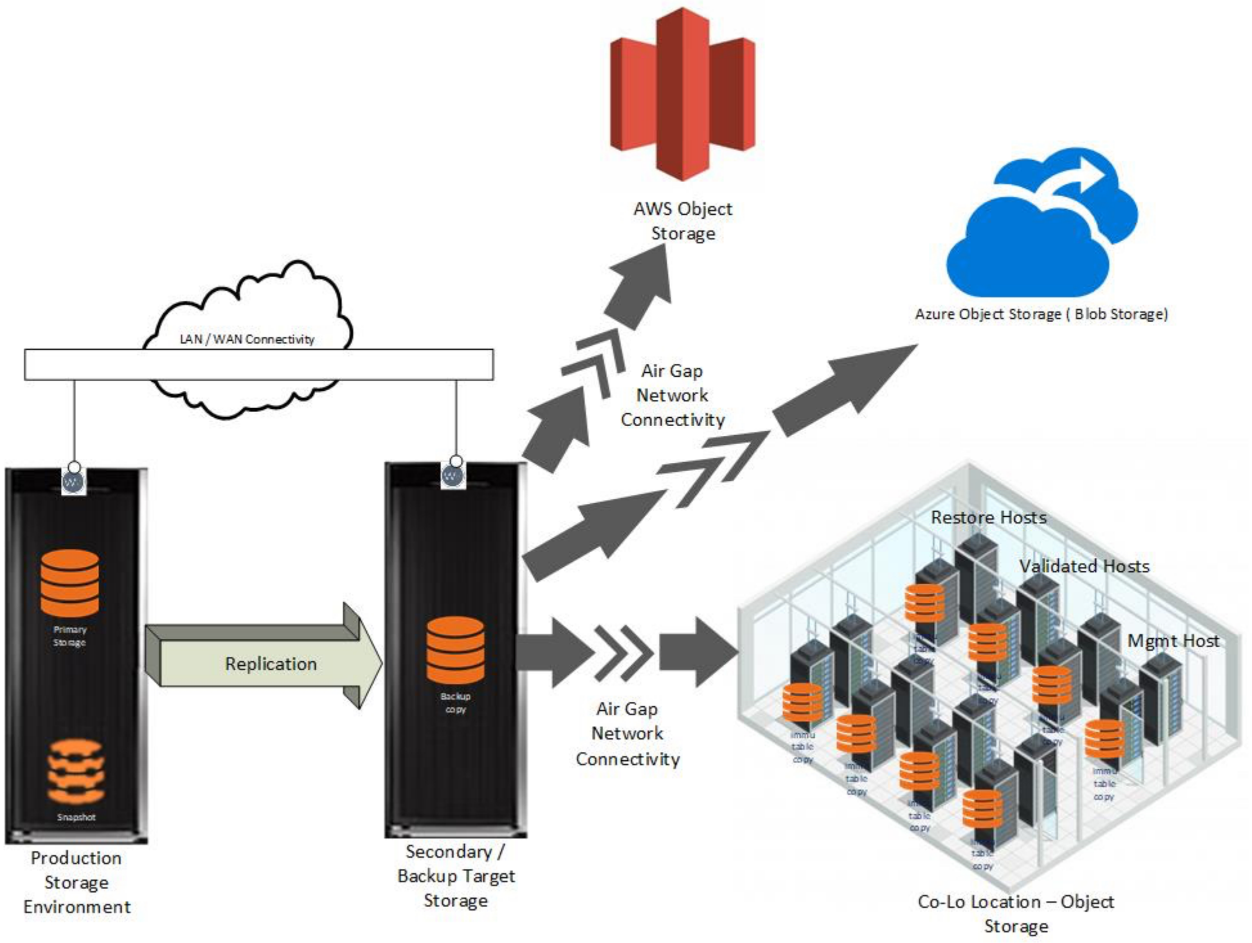
Air Gap – Backup Based Architecture



In this approach data is backed up and then replicated between a primary and secondary backup appliance. Like the array-based offering, the replication pipe is opened and closed based on predefined schedules.

The downside of this strategy is that it is still expensive and recovery times from the air-gapped copy can be lengthy.

Air Gap – Object Storage Based Architecture


AWS Object Storage
Azure Object Storage (Blob Storage)
LAN / WAN Connectivity
Air Gap Network Connectivity
Primary Storage
Snapshot
Replication
Backup copy
Air Gap Network Connectivity
Restore Hosts
Validated Hosts
Mgmt Host
Immu table copy
Production Storage Environment
Secondary / Backup Target Storage
Co-Lo Location – Object Storage

With this architecture, object storage is relied on for replication to create the air gap. Like the other options, the network connection to the object storage system may be opened and closed periodically to create the air gap.

However, many on-premises object storage systems and cloud offerings (i.e. Azure Object Storage and Amazon Glacier) include a WORM option which can enforce retention and prevent data deletion / corruption, and this may be sufficient to remove the need to open and close the network pipe.

The benefit of this approach is the low cost and massive scalability of object storage. The challenge of this approach is that it leverages traditional technologies and recovery from object storage can be lengthy.

Bottom Line

There is no doubt that in order to reduce risk to your data, an Air Gap approach should be incorporated in modern backup, recovery, and data security methodologies where all possible threat routes are proactively accounted and planned for.

Schedule a discovery consultation with Windval today and learn more about how we help address and solve common data management challenges through a holistic and client-centric approach.

contact@windval.com
312.801.6282
https://www.windval.com/contact

About Windval

As used in this document, "Windval" means Windval Technology Solutions LLC.

Windval is a technology consulting organization delivering advisory services and custom technical solutions that enable enterprise organizations to optimize legacy investment, integrate modern technologies, and deliver new capabilities that transform their business.

[1] Josh Fruhlinger. March 2020. Top cybersecurity facts, figures and statistics for 2020. CSO Online. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html.