Air Gap Technology on the Mainframe

James Ash

Wentworth Institute of Technology

Author Note

First paragraph: Introduction of Air Gap Technology

Second paragraph: Data Movement in Air Gap Backups

Third paragraph: Regulatory Compliance with Air Gap Technology

Fourth paragraph: Conclusion

In today's enterprise computing environment, saving critical data is more important than ever. With rising threats from ransomware, data breaches, and system failures, organizations must adopt secure and reliable backup solutions. One such solution is gaining popularity, especially in mainframe environments, is air gap backup technology. This method physically or logically backs up data from the system, ensuring it remains untouched and uncompromised in the event of a cyber attack.

What is the Air Gap?

Air gap technology is incredibly relevant in mainframe environments that deploy the use of z/OS mainframes, such as banking, government, and healthcare. These industries process large volumes of sensitive data and have mission critical availability requirements. These industries also have incredibly strict regulations on their data. An air-gapped backup is stored offline or on a separate network, the backup has no direct path from the production environment. In mainframe environments, this can be implemented using tape storage systems, WORM drives (write once, read many) drives, or cloud storage platforms with air gaps. Having these backups physically or logically separated creates an 'air gap' preventing malicious actors from accessing or altering the data located on the drives (IBM, 2021).

Data Movement in Air Gap Backups

Data movement is critical in air gap backups. Typically, the data on the mainframe is moved to the backup environment through scheduled jobs, using secure file transfer protocols. The jobs create a snapshot of the data either synchronously or asynchronously while maintaining

data integrity and minimizing the chances of data corruption. For physical air gaps the data is moved to the external tape or WORM drive and then disconnected from the network entirely. For logical air gaps the backup is stored online but is disconnected directly from the mainframe, isolating the drive, while maintaining secure access controls (TechTarget, 2022).

Regulatory Compliance with Air Gap Technology

Air gap backups offer traditional reliability against modern cyber attacks. As enterprise environments evolve to include cloud and distributed architectures, the mainframe still serves as the stable backbone for enterprise environments. Integrating air-gapped backup solutions ensures that legacy systems for enterprise environments remain protected against modern cyber attacks while maintaining compliance to regulatory protocols like HIPAA, SOX, and GDPR. These regulations demand data retention, protection, and recovery protocols. By using air gap technology enterprises can have immutable and isolated backup copies that meet these regulatory requirements (NIST, 2020).

Conclusion

In conclusion, air gap technology has become an integral component of data protection in mainframes. It ensures data integrity enhances security prevention against cyber attacks like ransomware, and supports regulatory compliance. As data has become increasingly valuable threats to said data has become more sophisticated, creating the need for technologies like air gap backups.

References

IBM. (2021). Mainframe Data Protection: Enhancing Cyber Resilience. IBM Redbooks. https://www.redbooks.ibm.com/

TechTarget. (2022). *Air Gap Backup: What It Is and How It Works*. SearchDataBackup. https://www.techtarget.com/searchdatabackup/definition/air-gap

NIST. (2020). *Guide for Cybersecurity Event Recovery*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

IDC. (2021). *The Importance of Cyber-Resilient Mainframe Strategies*. IDC Analyst Brief. https://www.idc.com/