DCIG

Leverage Air-gap Technologies to Stop Ransomware Attacks and Meet Operational Objectives

By DCIG President & Founder, Jerome Wendt

DCIG

TECHNOLOGY REPORT

Leverage Air-gap Technologies to Stop Ransomware Attacks and Meet Operational Objectives

Contents

2 Ransomware's Pervasiveness

2 Backups Under Attack

3 The NIST Cybersecurity Framework for Combating Ransomware

3 Air Gaps

4 Five Challenges of Managing Air-gapped Technologies

4 Four Strategies for Effective Air Gap Management

5 Strategy #1: Authenticates user access.

5 Strategy #2: Manages multiple air-gap technologies.

6 Strategy #3: Manages immutable storage

6 Strategy #4: Monitors and scans backup data for ransomware

6 The Arcserve Product Portfolio

7 Leverage Air-gapped Technologies to Stop Ransomware and Meet Operational Objectives

Ransomware's Pervasiveness

Ransomware represents one of the largest, most pervasive threats to business operations that many organizations have ever encountered. Hackers actively target organizations of all sizes with ransomware in hopes of encrypting data to extract a ransom from them.

This tactic works well. A 2021 survey found that 37 percent of organizations across 30 countries were hit by ransomware in the last year. Further, of those that were hit, 54 percent reported cybercriminals encrypted organizational data.

While alarming, good news exists. 96 percent of these same organizations got their data back.[1] To get it back, many used backups as a source to recover production data.

Backup's effectiveness has made it a popular option to recover from ransomware attacks. Should ransomware encrypt, corrupt, or make production data unusable, backups provide unaltered copies of production data to use for recoveries.

The effectiveness of backups for recovery negates the need to pay ransoms helping to thwart ransomware attacks. However, as backup assumes this broader role, hackers now more frequently seek to compromise backups and backup software.

> ***"Ransomware represents one of the largest, most pervasive threats to business operations that many organizations have ever encountered."***

Backups Under Attack

Hackers increasingly recognize backups and backup software represent a deterrent to a ransomware attack succeeding. In response, ransomware more frequently attempts to compromise backups and backup software as part of its attack.

For instance, one ransomware strain attempts to log into backup software as a privileged backup user. Once logged in, it attempts to lock the victim's backup software and remove the backups.

Other ransomware strains first scan shared corporate network drives for existing backup archives. Some backup software programs use ".bak" as a file name extension when naming backups stored on network drives. If the ransomware discovers them, it attempts to encrypt or delete these backup archives before encrypting production data.

Still other ransomware strains first infect an organization's production IT environment over time before initiating an attack. This infected production data then gets backed up and stored in the backups. Then, when the ransomware attacks, organizations use their backup data to recover. As they do, the recovery reintroduces the ransomware back into the production environment.

These and other methods represent insidious ways ransomware may compromise backup software and data. This puts the onus on organizations to select and deploy solutions that protect their backup software and data from ransomware.

The NIST Cybersecurity Framework for Combating Ransomware[2]

Knowing where to get started to combat ransomware may represent a hurdle to some organizations. To help, the National Institute of Standards and Technology (NIST) provides a cybersecurity framework. The five functions of this framework explain how organizations can get started.

1. ***Identify.*** Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2. ***Protect.*** Develop and implement the appropriate safeguards to ensure delivery of services.
3. ***Detect.*** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4. ***Respond.*** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Air Gaps

Air gaps represent a practical and cost-effective step that organizations may take to secure their backup data from ransomware attacks. Organizations may utilize physical, logical, or both types of air gaps.

> ***"Air gaps represent a practical and cost-effective step that organizations may take to secure their backup data from ransomware attacks."***

Using a physical air gap, organizations store backup data on storage media such as tape. They can then disconnect this media from their production IT environment. In contrast, a logical air gap remains connected in some form to the production IT environment. However, it relies upon network and user access controls to isolate the backup data from the production environment.

Ransomware cannot see or access the backup data using either of these two techniques. This makes it impossible for ransomware to compromise it. The availability of multiple, proven, and economical technologies to implement these air gap methods adds to their appeal.

To create physical air gaps, organizations may use media such as tape or removable disk. To create logical air gaps, they must first put in place the appropriate network and user access controls. Once in place, they have multiple storage options from which to choose.

If they need or want to keep backup data on-premises, they may use storage systems that store backup data in an immutable format. Organizations may alternately choose from multiple cloud storage providers. These include general-purpose cloud providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure. They may also look to purpose-built cloud storage providers as well as private clouds offered by backup providers.

The affordability of physical and logical air-gapped storage solutions makes them attractive options. Storing backup data with cloud storage providers starts at a few pennies per GB per month with lower cost options available. If using physical storage such as tape, the cost can approach pennies per TB.

This combination of affordability, availability, and effectiveness make the use of air-gapped storage technologies a practical choice. However, using air-gapped storage solutions create a specific challenge for organizations. They must identify and use a backup solution that secures user logins and can manage the different air-gapped technologies.

> ***"Organizations must identify and use a backup solution that secures user logins and can manage the different air-gapped technologies."***

Five Challenges of Managing Air-gapped Technologies

Organizations may secure their backup data by using backup software that leverages air-gapped technologies. However, not every backup software manages every air-gapped technology or may not manage it well. Five challenges they may encounter include:

1. ***No support for physically air-gapped storage.*** Newer enterprise backups solutions may only support disk or cloud storage. They may have limited or no support for physical, removable media, such as tape.
2. ***No support for bucket or object lock.*** Most general-purpose and purpose-built cloud storage providers now offer a bucket or object lock feature. This feature makes backup data immutable to prevent data deletions or changes. However, effectively utilizing these immutability features requires the backup solutions to recognize and manage it. Some may not yet support this functionality.
3. ***Unacceptable performance.*** Storing data on or retrieving data from an air-gapped storage solution may result in lengthy backup or restore times. Organizations may find they cannot back up or restore data in a time that meets their recovery objectives.
4. ***Cost creep.*** Storing backup data on air-gapped storage solutions may create an “out of sight, out of mind” situation. However, backup data stores may grow quickly. This creates scenarios where air-gapped storage costs also swiftly grow. Cloud storage costs recur and may increase monthly. If using removable media, it may have recurring offsite storage costs plus transportation costs.
5. ***Policy creation and management.*** Storing data on air-gapped storage in an immutable format dictates that organizations develop and create policies that manage data retention. These policies must align with business and regulatory requirements and delete data at the end of its useful life. They must also set policies that expire and release physical media or cloud storage once they no longer need it.

Four Strategies for Effective Air Gap Management

The best backup software helps organizations identify, repel, and recover from ransomware attacks. Backup software must support multiple air gap technologies to deliver on these requirements. The better it manages these technologies, the better it positions organizations to fend off ransomware attacks. Four strategies that today’s backup software should effectively implement, deliver, and manage include:

Strategy #1: Authenticates user access.

The integrity of the entire backup process – the backup data, jobs, and users – starts with the backup software itself. Backup software must secure these three components as part of its management of the overall backup process.

Organizations should not assume all backup software adequately performs this task. Some backup software still utilizes default user logins and passwords. Hackers may uncover these logins and passwords by reading backup user administration guides found online. Once discovered, they may attempt to access and compromise the backup software using this information. Hackers may hinder and negate any air gap measures implemented if they access the backup software using them.

Verify a backup solution minimally requires the creation of complex user passwords when first used or installed. Enterprise backup software should also offer multi-factor authentication (MFA) and an option to integrate with Active Directory (AD).

Some backup software even requires role-based access control (RBAC) with a second individual needed to approve performing certain tasks. These may include updating existing backup policies or changing or deleting backup data before it is scheduled to expire.

Key Backup Software Authentication and Access Features

- Requires creation of complex user passwords
- MFA
- AD integration
- RBAC

Strategy #2: Manages multiple air-gap technologies.

The number of air-gap technologies an organization has available to it will depend on the backup software it uses. All backup software supports one or more air-gap technologies. However, the number each one supports can and does vary. The more air-gap technologies a backup software supports, the more options it gives organizations to secure their backup data.

Robust backup software will support both logical and physical air-gap technologies. To create a logical air gap, the backup software should support cloud storage. That support may extend to supporting cloud storage from general-purpose and purpose-built cloud storage providers. Its support may also extend to managing the cloud storage's bucket or object lock functionality. It may even place and manage backup data across multiple storage tiers available from some cloud providers.

Since not all organizations can or want to store data in the cloud, the backup software should support removable storage media. This removable media may take the form of disk or tape. Robust backup software offerings will even offer support for tape libraries.

Finally, the backup software must support creating policies for backup data management. While all enterprise backup software use policies, they differ in how they deliver them.

For instance, some include default policies for backup data placement and retention to expedite faster implementations of its product. Others provide options to create policies based on business rules that the backup software then implements and places backup data accordingly.

Key Air-Gap Technology Manageability Features

- Logical Air Gap
  - Public and private clouds that support immutable data stores
  - Bucket and/or object lock
- Physical Air Gap
  - Removable media such as disks or tape
  - Manages tape libraries
- Policies
  - Default backup policies
  - Automated data placement and management based on business rules

Strategy #3: Manages immutable storage

Many organizations will find it impractical from an operational perspective to logically or physically air gap all their backup data. Storing backup data on air-gapped technologies may slow backup and retrieval times. Since production backup and recovery jobs demand higher levels of performance, organizations look to local disk to meet these requirements.

To keep backup data residing on this media secure from ransomware, organizations may turn to immutable, on-premises storage systems. These storage systems provide a local disk target to facilitate fast backups and recoveries. More importantly, from a data protection perspective, they store backup data in an immutable format to prevent changes and deletions.

Immutable On-premises Storage Benefits

- Local disk target
- Facilitates fast backups and restores
- Stores backup data in an immutable format

Strategy #4: Monitors and scans backup data for ransomware

No organization may assume its production cybersecurity defenses is foolproof due to how ransomware constantly evolves. During these evolutions, it finds ways to elude firewalls, spam filters, and antivirus software defenses.

Organizations cannot discount the possibility that undetected strains of ransomware reside in their production IT environment. If it resides in their production environment, their backup data may also contain it. This becomes problematic since using a backup for a recovery could reintroduce the ransomware back into production.

Backup software should help ensure organizations only recover uninfected data. To do so, backup software may take one or more of the follow steps. It can monitor itself for abnormal user activity as well as the backup data for abnormalities or unusual change rates. It can do scans on backup data to examine it for any latent forms of ransomware. It should ideally scan any data it recovers for ransomware. This helps mitigate the possibility of reintroducing ransomware back into production.

Advantages of Monitoring and Scanning Backup Data

- Leverage exploit prevention technology to stop common hacker tricks and methods that may compromise backup data.
- Use behavioral analysis to stop previously unseen ransomware attacks
- Incorporate analysis of backup data into extended detection and response (XDR) to secure the entire environment and understand the impact of security incidents.
- Stop both local and remote unauthorized file encryption by malicious software

The Arcserve Product Portfolio

The Arcserve product portfolio includes multiple offerings that deliver on these four strategies to effectively manage air-gapped technologies. Arcserve's available offerings position organizations to:

- ***Authenticate user access and secure data.*** Arcserve's enterprise backup software, Unified Data Protection (UDP), supports both MFA and RBAC for administration. This functionality ensures only authenticated and trusted users may access UDP and change or delete backup jobs and backup data. It may further secure the data by encrypting data at-rest with AES encryption and encrypting data in-flight with SSL.
- ***Manage multiple air-gapped technologies.*** Arcserve provides solutions for every currently available logical and physical air-gapped technology. To create logical air gaps, Arcserve may send backup copies to cloud stores that use object lock which it manages through the UDP console. It may use immutable cloud storage such as Amazon AWS S3 Object Lock. It may also use S3-compatible cloud storage systems such as Nutanix Object Lock and Wasabi Object Lock. Arcserve supports their respective bucket or object lock technologies to store data in an immutable format. Regardless of the immutable cloud storage offering, they protect backups from deletion or alteration by malware and hackers. On the physical side, it supports removable media such as disk and tape.

- ***Manage immutable storage.*** To accelerate backups and recoveries, Arcserve UDP supports many storage systems that offer data immutability. Arcserve also offers OneXafe, its own immutable storage system that can host backups. It can then facilitate moving backup data off-premises or to the cloud using either replication or Arcserve UDP's RPS Jumpstart feature. RPS Jumpstart replicates data from a local storage system, such as OneXafe, to an external storage device such as a USB drive. Once copied, they can send that device to another location or the cloud.
- ***Monitor and scan backups for ransomware.*** Arcserve's Secured by Sophos services proactively analyzes backup data for the presence of ransomware. Sophos Intercept X Advanced cybersecurity software detects both known and unknown ransomware strains without relying upon signatures. This software positions organizations to detect and respond to ransomware before it attacks.

> ***"The Arcserve product portfolio positions organizations to implement and manage these four strategies for effective air gap management while still meeting their day-to-day operational objectives."***

Leverage Air-gapped Technologies to Stop Ransomware and Meet Operational Objectives

Organizations must now operate under the assumption that ransomware will one day attack their IT environment. Further, ransomware continues to become more sophisticated and increasingly targets weak links that may exist in organizational cybersecurity defenses.

Air-gap technologies serve a critical role in helping organizations neutralize and repel these attacks. They ensure ransomware attacks do not compromise existing backup data and position organizations to respond. However, organizations must properly implement and manage these air-gapped technologies to ensure they get the benefits they expect.

The Arcserve product portfolio positions organizations to implement and manage these four strategies for effective air gap management while still meeting their day-to-day operational objectives. They may quickly back up, secure, and analyze their data knowing they have reliable, clean backups. Equally important, they may recover their data wherever they need it in the time and manner that they need it. ■

Sources

1. https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf. *The Sate of Ransomware* 2021. Referenced 1/30/2022.
2. https://csrc.nist.gov/csrc/media/Publications/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final/documents/quick-start-guide–ransomware.pdf. Referenced 3/3/2022.

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of TOP 5 Reports and Solution Profiles. Please visit **www.dcig.com.**