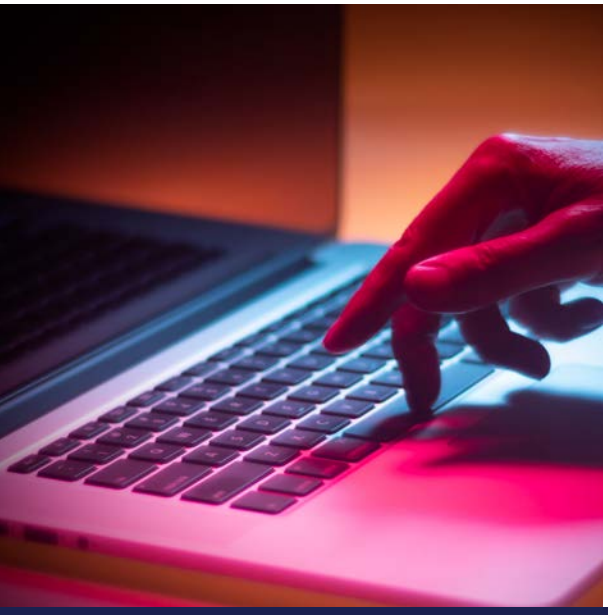
HORISON
Information Strategies

Sponsored by:
FUJIFILM
Value from Innovation

2022 Technology Update Series



TAPE AIR GAP ANCHORS SECURITY ECOSYSTEM

ENCRYPTION, WORM AND AIR GAP CREATE IMMUTABLE DATA STORAGE SYSTEM

Fred Moore, President | **Horison.com**

IN THIS WHITE PAPER

ABSTRACT

No computer system is immune from cybercrime, and new types of threats are being discovered every day. With a cease-fire in the cybercrime war highly unlikely, we are witnessing the rapid convergence of data protection and cybersecurity to counter damaging cybercrime threats and ransomware attacks. Emails deliver most of all cybercrime infections with **96% of phishing attacks arriving by email**, initially landing on your computer's HDDs or SSDs - but not on air gapped (offline) storage devices. In addition to tape's value to online applications such as an active archive, modern tape is clearly the preferred offline storage technology for today's data centers. Though tape has been an air gapped technology since its inception, the growing cybercrime wave has positioned air gapped tape storage squarely in the middle of the cybersecurity ecosystem as data cannot be hacked when stored behind a physical air gap. Today's most effective cybersecurity strategies include air gapped tape.

CYBERCRIME SCENARIO 2022

Cybercrime is more than a $6 trillion annual industry, which would qualify it as the world's third-largest economy after the U.S. and China. The cybercrime ecosystem includes endpoint security, firewalls, VPNs, antivirus software, multi-factor authentication, and most are present on every system. These security layers don't always guarantee the bulletproof levels of security an organization needs before a new breach arrives. Each of these security layers can block hackers on many fronts, but they can leave a backdoor entry directly into your IT organization. The World Wide Web was invented in 1989, the first-ever website went live in 1991, and today there are more than 1.7 billion websites all vulnerable to cybercrime attacks. In addition, there are more than 26.8 million software developers creating new software code, and the highly hyped IoT (Internet of Things) is currently projected to exceed 27 billion endpoints by 2025, all increasing the attack surface while creating an intensifying perfect storm for cybercrime. Digital data has become the highest value resource for most every business and is the single biggest target for cybercriminals.

The World Wide Web was invented in 1989, the first-ever website went live in 1991, and today there are more than 1.7 billion websites all vulnerable to cybercrime attacks.

TAPE AIR GAP PROVIDES CYBERCRIME PROTECTION

A robotic tape library, on premise or in the cloud, or manually accessed tape cartridges in tape racks or vaults are currently the only data center class air gapped storage solutions available. A physical tape air gap is an electronically disconnected or physically isolated copy of data stored in a robotic library or tape rack that prevents cybercriminals from directly attacking a backup, archive, or other data on magnetic tape. Without an electronic connection to the tape cartridge, data stored on tape can't be hacked. Tape cartridges are online and accessible only when the tape cartridge is mounted by a robot or person in the tape drive (see chart below). When tape media is not mounted in a drive, it resides in a library slot or offline rack electronically disconnected and inaccessible from any system and is protected from cybercriminals with the tape air gap. Note that many CSPs (Cloud Service Providers) provide online connections to disk storage for various storage services and air gapped, offline robotic tape connections for archive services.

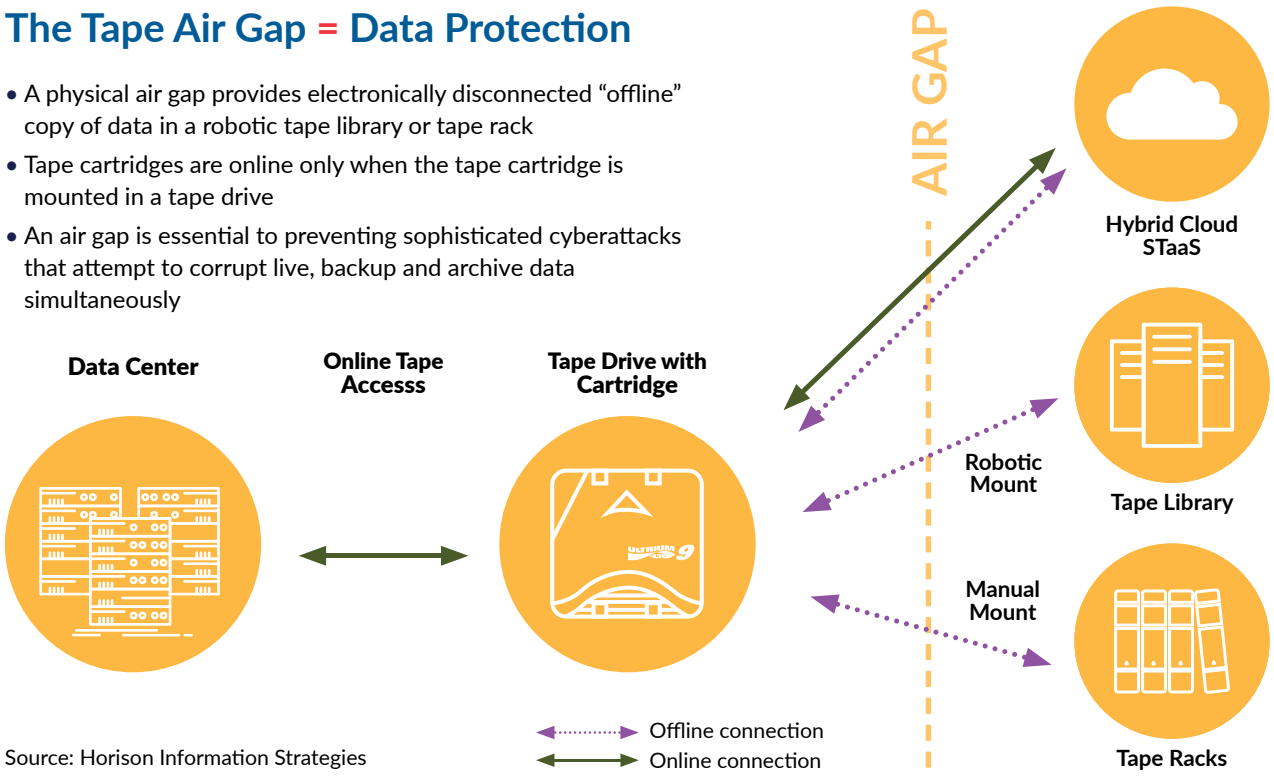
Tape media stored in a robotic library sits in magazines or slots when not in use. To take advantage of this, a variation to the tape air gap strategy is available that can partially eject a specified tape magazine manually so the tapes cannot be picked or retrieved by the robot until an operator physically reinserts the magazine. Although partially ejected, the barcode scanner on the robot can still scan the tape barcodes, allowing system administrators to perform periodic audits of the tape system, ensuring tapes are still present.

HDDs and SSDs are always online and accessible to hackers and are the initial entry point for cybercrime infections. A true, cyber-resilient copy of data must meet additional and more stringent requirements than provided by online systems. As a result, tape "air gapping" strategies are quickly gaining momentum.

Note that data that is offline is either physically or logically air gapped.

The Tape Air Gap = Data Protection

- A physical air gap provides electronically disconnected "offline" copy of data in a robotic tape library or tape rack
- Tape cartridges are online only when the tape cartridge is mounted in a tape drive
- An air gap is essential to preventing sophisticated cyberattacks that attempt to corrupt live, backup and archive data simultaneously



Source: Horison Information Strategies

LOGICAL OR VIRTUAL AIR GAPS

Several tape library vendors are taking air gap protection to the next level by offering logical or virtual air gapped library partitions consisting of dedicated slots that are made invisible to external applications. Logical air gaps rely on network access controls or operator commands to create isolation within a tape library (a cold partition) from production and primary backup environments. Some enterprises wall off the disconnected media via a locked room or cage to prevent manual access. Logically air gapped backups can be brought back online and accessed via operator commands. A logical air gap normally uses a Zero Trust approach, eliminating implicit trust and continuously validating every stage of a digital interaction. HDDs can also create a logical air gap with commands that VARY a hard drive offline or online, preventing application access. Logical air gaps tend to lack full protections against insider attacks that can access user controls as there is still a physical network connection to the data, making it potentially hackable.

THE POPULAR 3-2-1-1 DATA PROTECTION STRATEGY LEVERAGES THE TAPE AIR GAP

Advanced IT data protection strategies are incorporating the tape air gap to further combat cybercrime. Backup creates a copy or multiple copies of data to restore data in case of damage or loss. The original data is not deleted after a backup is made. The widely used 3-2-1-1 data protection strategy states enterprises should have **three** copies of backups on **two** different media types, **one** copy of which is kept offsite and **one** air-gapped offline copy. There are two ways to store a physically offsite data copy, either with an online electronic access (HDD, SSD) to a cloud provider or other location, or with an offline (air-gapped tape library or manual access tape racks) copy. By keeping backup copies both locally and physically offsite or in the cloud (hybrid cloud), you double the protection for your data in the event of any unforeseen circumstance, disaster, or outage at the primary data center. The business consequences of critical data loss by ignoring the 3-2-1-1 rule can be devastating, making the tape air gap a highly valuable component of a successful backup strategy.

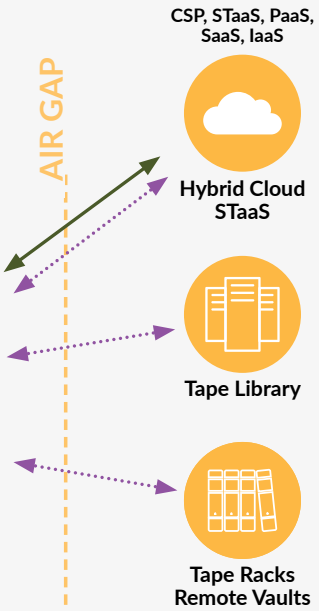
CYBERCRIME SCENARIO 2022

Tape Air Gap Plays Central Role In the Cybersecurity Ecosystem

THE 3-2-1-1 DATA PROTECTION STRATEGY

(for Backup, Recovery and DR)

3 Copies of Data	**2** Different Media Types (SSD, HDD, Tape)	**1** Copy Offsite ... Business Resiliency (SSD, HDD, Tape)	**1** Air Gap Copy Offline (Tape) No Electronic Connection



Offline connection Online connection

- The Zettabyte Era, IoT, Edge, and Shadow Assets Expand the Cybercrime Attack Surface.
- Ransomware attack damages from rose from $11.5 B in 2019 to $20 B in 2021.
- Highest ransom fee was **$70 M**, 82% defaulted to paying the ransom.
- **Cloud** cyberattacks account for 20% of all cyberattacks.
- WW ~3.5 million unfilled cybersecurity jobs in 2021. **Cybersecurity Ventures**.
- Protection solutions *lagging* for emerging technologies like 5G, the edge, IoT, crypto, AI and ML — *all TBD*.

The tape air gap also applies to archival data that may be stored for years awaiting reference or future analysis, which is typically unchanging and is seldom overwritten. Archiving moves the data to another location, typically a lower-cost, highly secure tape storage environment and frees up the space on the source volume. The tape air gap becomes even more important since the archive copy is typically the only copy of data increasing the potential exposure to cybercrime damages.

The Cybersecurity Ecosystem Building Blocks

Physical Tape Air Gap	An electronically disconnected or physically isolated copy of data in a robotic tape library or tape rack preventing cybercriminals from directly attacking a backup, archive, or other data copy on magnetic tape. Data stored behind a physical tape air gap cannot be hacked.
Logical Tape Air Gap	Uses network and user access controls to create additional levels of data isolation from the production and primary backup environments. Since logical air gaps still have an electronic connection and it requires human intervention, it is not as secure as a physical air gap.
3-2-1-1 Backup Strategy	Back up data regularly using the 3-2-1-1 backup strategy. Three copies of data on two different storage media, one offsite copy and one air gap copy. The cloud is often used to store the offsite and air gapped (offline) copies of backup and archive data.
Encryption (Incomprehensible Text)	Encryption translates data into an unreadable format. Only people with access to a secret decryption key or password can read it. One of the most popular and effective security methods available, most organizations use at least 256-bit AES encryption for data at rest and in motion.
WORM (Immutable Copy)	Write-Once-Read-Many provides immutable storage and is used for tape and HDDs. You can write data to a WORM storage device or media exactly one time. After that, no one can legitimately change the data in any way. The data can be read an unlimited number of times.
Multi-factor Authentication (MFA)	MFA is an authentication method that requires the user to provide two or more verification factors beyond the standard username and password, often including a one-time password, to gain access to a resource such as an application or online account.
Antivirus Software	Antivirus (AV) software scans, detects and deletes viruses (malware) from a computer. Most AV software runs automatically in the background to provide real-time protection against virus attacks. Use antivirus software from trusted vendors and only run one AV tool on your device.
Firewalls	A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.
VPNs	A virtual private network allows users to create a private connection over a less private network by creating an encrypted tunnel between your computer and the internet.

A physical tape air gap is an electronically disconnected or physically isolated copy of data stored in a robotic library or tape rack that prevents cybercriminals from directly attacking a backup, archive, or other data on magnetic tape.

ATTACK LOOPS MAKE RANSOMWARE MORE CHALLENGING

Though digital extortion is not new, ransomware malware is a growing crypto-viral digital extortion technique that can get around firewalls and malware protection tools locking the system's screens by encrypting selected files. According to the 2021 IBM Cost of a Data Breach report, the average total cost of a ransomware breach was $4.62 million and ransomware damages reached $20 billion. A ransomware attack typically begins when an end user clicks on a website link or opens a file attachment in a malicious email that is part of a phishing (random) or spear-phishing (targeted) cybercrime campaign. Ransomware attacks can give cyber criminals complete control over a device's online (non-air gapped) files and applications unless the organization pays a ransom.

Ransomware Attack Loops attacks can embed time-delayed, undetected malware into online files and the malware can stay dormant, sometimes taking several months to reactivate. In the meantime, the dormant malware is eventually and unknowingly backed up to a backup device, normally tape or HDDs. After a time-delayed online malware detonation disabling a file(s), the pre-attack generation of the backup file(s) is restored only to realize that the recovery data from tape or HDDs reinserts the ransomware back into the system and re-encrypts the data all over again for a perpetual loop of attacks. The Attack Loops usually continue until a complete recovery occurs or extortion fee is paid, typically into an anonymous bitcoin account in exchange for the deciphering key. An estimated 82% of attacks result in a ransomware payment.

Fortunately, Attack Loop prevention software can identify and quarantines malicious code upon entry into the backup repository and again prior to recovery into the online environment with the malicious code disabled. Advanced Attack Loop prevention software is using automated, AI and ML tools to continually improve detection capabilities and coupled with the tape air gap backup copies, provides the best option to prevent attack loops. Expect significant advancements with backup software as it becomes tightly integrated with air-gapped tape libraries to disarm any ransomware attacks.

THERE ARE SEVERAL ADVANTAGES OF USING TAPE FOR THE HIGHEST DATA SECURITY LEVELS

In addition to the tape air gap, there are several advantages of using modern tape for the highest levels of data security. Media life for LTO is rated at 30 years or more and WORM and encryption add further immutable data protection capabilities. Tape has a better bit error rate (reliability) than any other recording medium. LTO drives have unrecoverable bit error rates (BER) of $1x10^{19}$, which is roughly one unrecoverable error in every 1.25 EB read. Enterprise class HDDs have an error rate of $1x10^{16}$ or an error every 125 TB. Tape capacity has reached 18 TBs native capacity (45 TB compressed) on the latest LTO-9 drives and at 400 MB/sec., tape delivers faster data rates than any HDDs reducing data recovery times, especially for larger files. The enterprise 3592 drives have a 20 TB capacity, 400 MB/sec. data rate and a leading BER of $1x10^{20}$. Robotic tape library capacities have surpassed one exabyte ($1x10^{18}$) capacity becoming the first air gapped exascale storage system. Studies indicate storing cold data on tape has a TCO that is 86% lower than disk and produces 87% less carbon footprint than disk for storing 10 PB of cold data. These features coupled with the air gap have brought tape-based technology back into the forefront as a solid defense to protect data against cybercrime.

SUMMARY

The IT industry no longer considers data security and data protection as separate tasks and actively seeks more stringent integrated solutions. The primary goal for cyber criminals and malicious insiders is to access your high value data. The larger the storage environment, the greater the attack surface for cyber criminals. Clearly the cybercrime threat isn't going away and will take every defense mechanism available to counter its relentless impact. Malware continues to become more sophisticated and increasingly targets weak access points that may exist within an organization's cybersecurity defenses. Organizations must now operate under the assumption that malware or ransomware will one day attack their IT environment.

Though no option is completely impenetrable, the cybersecurity ecosystem is continually improving and has been significantly strengthened with tape air gap storage solutions. Air gapped technologies now serve a critical role in helping organizations neutralize and repel these attacks. They ensure ransomware attacks do not compromise existing backup data and encourage organizations to make the 3-2-1-1 Data Protection Strategy an operational requirement. For some in the security field, the tape air gap can be a minimum requirement in cyber defense. In other segments, such as the military, government or any critical infrastructure, air gaps may be mandated by a security policy. Cyber-insurance underwriters may also require an air gap as a condition of issuing a policy. Unless wireless data sniffers or drones someday arrive to attack offline air gapped data, the tape air gap provides the last line of defense for data protection simply because criminals can't delete or encrypt what they can't access over the network or any other electronic link.

Horison Information Strategies is a data storage industry analyst and consulting firm specializing in executive briefings, market strategy development, white papers and research reports encompassing current and future storage technologies. Horison identifies disruptive and emerging data storage trends and growth opportunities for end-users, storage industry providers, and startup ventures.