'PHYSICAL' AND 'VIRTUAL' AIR-GAP DATA PROTECTION

Introduction

In the digital age, cybersecurity is of paramount concern for organizations and individuals alike. With the ever-increasing threat of malware, employing secure & reliable backups and robust disaster recovery capabilities are critical components of any holistic cyber risk reduction plan.

At the same time, a 2024 study reports that 94% of organizations hit by ransomware say that cybercriminals attempted to compromise their backups.[i]

The financial and operational implications of having an organization's backup compromised in a ransomware attack are immense.

When attackers succeed in compromising backups, an organization is almost twice as likely (67% vs. 36%) to pay the ransom and incur an overall recovery bill that is eight times higher than those whose backups were not impacted.

Further, according to a survey by Sophos Ltd, of 2,974 IT/cybersecurity professionals across 14 countries whose organizations had been hit by ransomware in 2023,

organizations whose backups were compromised, are 63% more likely to have their data encrypted and received ransom demands that were, on average, more than double that of those whose backups were not impacted.[ii]

Properly air-gapped backups provide the last line of defense against data loss, corruption, and unauthorized access in the event of network intrusion, such as a ransomware attack, compromised software applications, system failure, or human error.

To address this need, the EchoLeaf SafeRoom Suite™ with its true physical air-gapped storage management and recovery system, has emerged as a powerful strategy to securely and reliably protect and rapidly recover essential data.

What is an Air-Gap?

Air-gapping backups involves creating an isolated environment for data storage to reduce the risk of data compromise significantly. Air-gapped environments may be on-site, remote, or both.

Two 'air gap' approaches are frequently discussed - physical and virtual (aka logical) - and it can be confusing and risky when vendors offer "Air Gap" backup without specifying whether they are referring to "physical" or "virtual" air gaps.

Understanding the distinctions between physical and virtual air-gap storage is vital to achieving optimal data protection and enabling rapid recovery.

This white paper discusses the differences between physical and virtual air gaps, their strengths, and weaknesses, and their roles in protecting against malware and ensuring effective disaster recovery.

'Virtual' Air Gap Backups

A 'virtual' air gap, also known as a 'logical' air gap, is a security measure that leverages software and network segmentation to create a logical separation between the production network and the backup repository. This approach uses virtualization and network segmentation technologies to attempt isolation without physical separation.

A virtual air gap is considered more complex to implement & maintain, limited in scaling, more vulnerable to malware, and susceptible to network-based attacks than physical air-gaped systems.

Complexity: Setting up and managing virtual air gaps can be highly complex, requiring specialized knowledge in network segmentation and virtualization.

Virtual air gaps require sophisticated automation tools to manage disconnection schedules, network isolation, access controls, and encryption.

Regular monitoring and adjustments are required to prevent configuration errors, and the complexity increases with the size

of the organization and data requirements.

Software patches, firmware updates, and system reconfigurations add complexity to maintenance. Staff need to be trained to manage automated processes and ensure they work properly.

A 2024 IBM Data Breach Study[iii] reported more than half of the breached organizations interviewed faced severe security staffing shortages, a skills gap that increased by double digits from the previous year.

This lack of trained security staff is growing as the threat landscape widens, putting complex systems at higher risk as they are difficult and costly to implement and manage.

Network Dependence: Although logically isolated, virtual air gaps operate within the same physical network infrastructure. If the system fails to isolate properly, it can expose the entire network to threats.

If malware breaches the network and exploits vulnerabilities in the backup software or configuration, it could compromise the backups.

Potential for Misconfiguration: The effectiveness of a virtual air gap depends on, among other things, the proper configuration of applications and networks.

Misconfigurations and weaknesses in virtual air gap applications can lead to vulnerabilities that could be exploited by cyber threats leaving them susceptible to sophisticated cyberattacks.

Network Configuration: Implementing and maintaining secure network segmentation requires significant technical expertise. Virtual air gaps require staff with more specialized skills related to network management, automation, and cybersecurity.

Use of Cloud: Given that most "virtual" air gap applications utilize cloud storage, it is worthwhile to note that IBM recently reported[iv] that the number three ranked attack vector for data breaches is Cloud Misconfiguration. Further exposing virtual air-gapped systems vulnerabilities.

Recovery Delays with Cloud: While cloud access to the first byte of data can be rapid if the data is stored in the most expensive standard storage level (seconds to minutes), longer with near-line (hours), and very long/undetermined (10's of hours) with archive, data still must then be transferred to the on-site data center.

Cloud also introduces multiple variables that delay the download of data. Even with a fast connection, high network latency, network congestion or bandwidth throttling (common with cloud providers or ISPs during high-demand periods) can cause delays in establishing secure connections or negotiating data transfers resulting in a slow and unpredictable retrieval.

Human Error: With the increased complexity and reliance on human interaction, misconfigurations in the virtual air gap setup are more likely and could create pathways for malware to infiltrate the backup environment.

Total Cost of Ownership: Virtual air gap backups may initially appear to have a lower entry cost however they are almost always tied to complex multi-purpose software packages that increase ongoing short and long-term costs, lengthen implementation time, create system disruption, add complexity, and result in a higher TCO. If (when) a system is breached, recovery costs will also significantly affect ROI and TCO.

Secondary and Ongoing Costs: Storing data needed for rapid recovery and business continuity in the cloud or on local spinning disks also includes high and often unpredictable costs. Cloud storage incurs storage costs, transport costs, dependency on overall network quality and availability, and typically variable egress charges. Local spinning disks require electricity/cooling, system maintenance, hard drive or SSD replacements, operational management costs, and increased complexity.

Limited Long-Term Archival: While not part of rapid recovery, it is worthwhile to note that virtual storage solutions do not offer the same long-term archival cost effectiveness as LTO media.

The ten-year storage cost of LTO compared to 'all disks' systems is over 86% lower, and for 'all cloud' is over 66% lower. Add the extra egress costs, data retrieval latency, and unpredictability with cloud storage, and it is clear that LTO is an easy choice for long-term archive and defense against ransomware, with rapid and effective recovery.

'Physical' Air Gap Backups

The EchoLeaf SafeRoom™ physical air-gap data protection solution leverages storing backup data on LTO tape media that are physically disconnected from ANY network.

With the EchoLeaf solution, LTO tapes are held in an automated robotic library with the ability to create multiple append-only copies and automatic synchronization with remote off-site locations, typically a geographically separate facility.

High Security & Resilience: By definition, true physical air gap storage provides the highest level of security and the strongest defense against cyberattacks, including ransomware, as they completely isolate systems from potential cyber threats. The complete separation makes it immune to malware, ransomware, or network-based attacks. Malware cannot directly infiltrate an air-gapped system.

This configuration combined with other EchoLeaf patents enables drive virtualization, roll-back to a previous file version, compartmentalization,

encryption, fast access to stored data, and rapid recovery, along with numerous other advantages.

Traditional Cyber Security Protection Solutions are Not Enough: Referencing the IBM study noted earlier that identifies, Phishing, Compromised Credentials, and Cloud Misconfigurations as the top three attack vectors for data breaches, it is clear that traditional cyber security preventative methods are insufficient in dealing with a breach from these modern attack vectors, and makes having a physical air-gapped and immutable backup, combined with an effective & efficient recovery methodology more important than ever.

Simplicity: With the EchoLeaf SafeRoom™, physical isolation is straightforward and easy to understand, deploy, and scale, making it a reliable method for securing sensitive systems sized from small to large. The solution requires staff with basic IT and common physical storage management skills.

Ease of Implementation: The EchoLeaf SafeRoom™ solution is non-disruptive to existing IT systems and workflows appearing as a simple drive location, making it compatible with any backup operation that can read/write to an NFS target.

Scalability: The EchoLeaf SafeRoom™ solution is easily and cost-effectively scalable from 10's of Terabytes to 11+ Petabytes and beyond, and addresses a variety of use cases, by adding LTO media (both within and outside the library), adding library modules, adding LTO drives, and scaling the EchoLeaf Sentry server.

Meeting Legal Compliance Standards: Ransomware and other cyber-attacks can have a severe impact on legal compliance standards across various industries, especially those that handle sensitive data, and/or need longer-term data retention. The extent of the impact depends on the nature of the industry and the regulatory requirements it faces. HIPAA, GLBA, SOX, FISMA, CPRA & GDPR, FERC, SO/IEC 27001, FERPA, COPPA, and ABA Cybersecurity Model Rules are just a few where fines, penalties, and regulatory audits or investigations can result from business interruption due to ransomware.

The Immutable EchoLeaf SafeRoom™ solution helps organizations meet these compliance standards by providing a reliable and secure method for long-term data preservation, and by the nature of its design, provides a reliable audit trail, which is crucial for industries that require accurate records management and data authenticity.

Data Replication: Aside from creating multiple copies within a single environment, EchoLeaf Gemini™ Auto Synchronization with a remote facility, protects against data loss in the case of the physical destruction of the primary site.

Dramatically Fast Restore: Being local to the facility provides almost immediate access and high-speed retrieval of backed-up data, without the associated costs of spinning disks, network problems/delays, or the penalty of storage and egress costs for data stored in the cloud.

Long-Term, Immutable LTO Storage: The patented EchoLeaf SafeRoom™ manages tape so you don't have to, by leveraging and adding value to Linear Tape-Open (LTO) technology, which has been a mainstay in data storage for decades, renowned for its reliability, longevity, and cost-effectiveness.

The LTO format is backed by the most respected names in the storage industry, providing an open format to enable interoperability between drives and media from multiple licensed vendors.

With a well-defined roadmap stretching to generation 14, LTO Ultrium offers a safe investment and the scalability to manage fast-growing data volumes in organizations large and small.

EchoLeaf's use of Immutable LTO tape storage adds a crucial layer of security by ensuring that data, once written, cannot be altered, or deleted. This feature makes LTO an ideal choice for secure archival storage, compliance, and protection against ransomware and other cyber threats.

Extremely cost-effective and portable, LTO media can be easily stationed in remote, active, or offline locations for superior protection from natural or manmade threats. Since EchoLeaf Sentry™ tracks assets both within the library and those moved to other storage locations, the ability of users to easily find and retrieve all assets long-term is effectively unlimited.

Lowest Cost per Terabyte: LTO technology is unrivaled as a low-cost, high-capacity, reliable, portable, and secure solution for data protection. LTO tape complements disk, flash, and cloud solutions in tiered storage architectures, providing a low-cost, last line of defense against ransomware and effective disaster recovery.

Energy Efficiency: Unlike active storage systems that require continuous power, LTO tapes do not consume power when not in use. This significantly reduces energy costs, making them a green and cost-effective storage solution. This cost efficiency makes it an attractive option for organizations looking to store large volumes of data without incurring high expenses.

Sample Use Cases and Considerations

Disaster Recovery

Physical Air Gap: the EchoLeaf SafeRoom Suite™ delivers robust and rapid disaster recovery capabilities. Even in the case of a widespread network-based disaster where the server hosting the EchoLeaf Sentry™ orchestration engine is compromised, EchoLeaf provides for fast bare-metal restore of the Sentry server and uniquely allows (enabled by one of the central parts of the EchoLeaf patents) restoration of the SafeRoom data from tape, making the

EchoLeaf SafeRoom quickly ready to restore data to other servers/systems.

EchoLeaf Sentry™ software combined with local immutable LTO storage provides a drastically faster and lower cost recovery while physical Air-Gap backups offer a robust defense against cyberattacks, especially ransomware, by isolating the backups from online access.

Malware Protection

Physical Air Gap: Ideal for environments where the risk of malware infection must be minimized, such as commercial operations, education, healthcare, military systems, critical infrastructure, and financial systems. Physical disconnection provides extremely strong protection against remote attacks.

Summary

Effective and Secure backups are a critical part of a holistic cyber risk reduction strategy, and true physical air-gapped backups to immutable storage provide the last line of defense against data loss and corruption.

Investing in secure and efficient physical air gap backup protection from EchoLeaf elevates your ransomware resilience while also lowering your overall Total Cost of Ownership.

The EchoLeaf SafeRoom™ Physical Air Gap Solution delivers unparalleled security and the strongest defense against malware and ransomware through complete data isolation, dramatically fast disaster recovery, and rapid non-disruptive deployment providing a cost-effective and scalable solution for organizations of all sizes concerned with cyber threats and disaster recovery.

Echo Your Data Today™!

To learn more, please visit www.echoleafsystems.com.

Contact:
EchoLeaf Systems, Inc.
Douglas Korte | CSO
+1 661-250-0649 (o)
Dkorte-ic@echoleafsystems.com
www.echoleafsystems.com

[i] Sophos Ltd survey. 2024, The Impact of Compromised Backups on Ransomware Outcomes
[ii] Sophos Ltd survey. 2024, The Impact of Compromised Backups on Ransomware Outcomes
[iii] IBM, Annual Cost of a Data Breach Report, 2024
[iv] IBM, Annual Cost of a Data Breach Report, 2024