carahsoft

True Air Gap Backup & Recovery:

Why the Intelligence Community Definition Matters - and Why Logical Air Gaps Fall Short

---

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASPO ValuePoint, The Quilt and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Bacula Systems, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

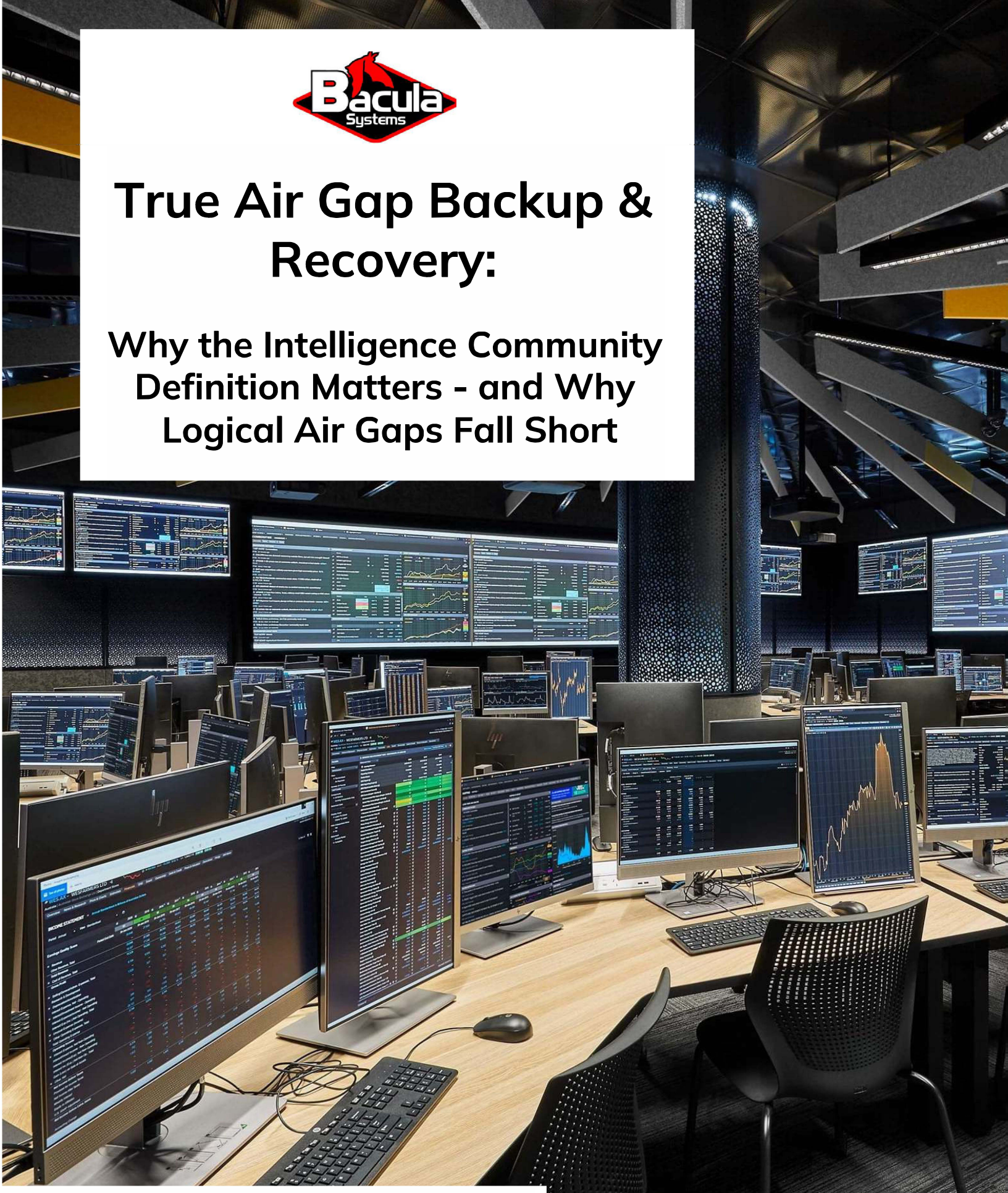
Explore More Resources:
carah.io/BaculaSystemsResources

Join Events & Webinars:
carah.io/BaculaSystemsEvents

Discover Technology Solutions:
carah.io/BaculaSystems

Learn About Procurement:
carah.io/BaculaSystemsContracts

Connect With Our Team:
BaculaSystems@carahsoft.com
571-590-4040



True Air Gap Backup & Recovery:

Why the Intelligence Community Definition Matters - and Why Logical Air Gaps Fall Short

Anchored in CNSSI 4009-2015 / IC Community Standard Authoritative Guidance for DoD, IC, and Critical Infrastructure

Bacula Systems White Paper

Jan. 2026

Table of contents:

1 — Executive Summary

2 — The Authoritative Definition of an Air Gap

3 — What Logical Air Gapping Actually Means

4 — The Risk Profile of Logical Air Gaps

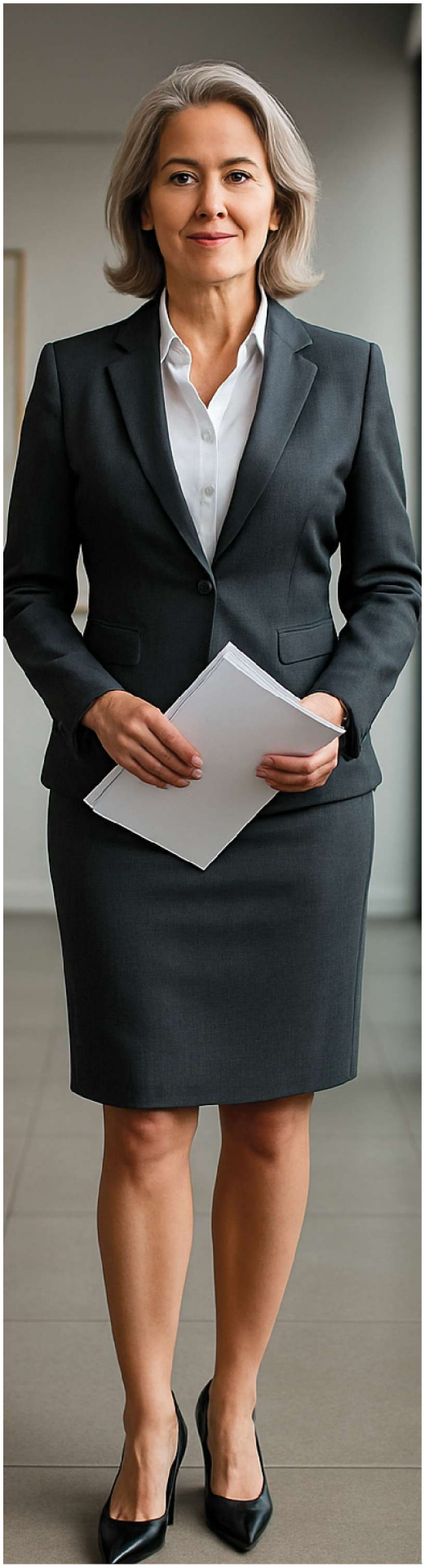
5 — How Bacula Enterprise Satisfies the CNSSI 4009 Standard

6 — Evaluating Vendor Air Gap Claims: A Practical Framework

7 — Industry Context: What Happened to the Air Gap Definition.

8 — Bacula's Advanced Modular Architecture

9 — Conclusion

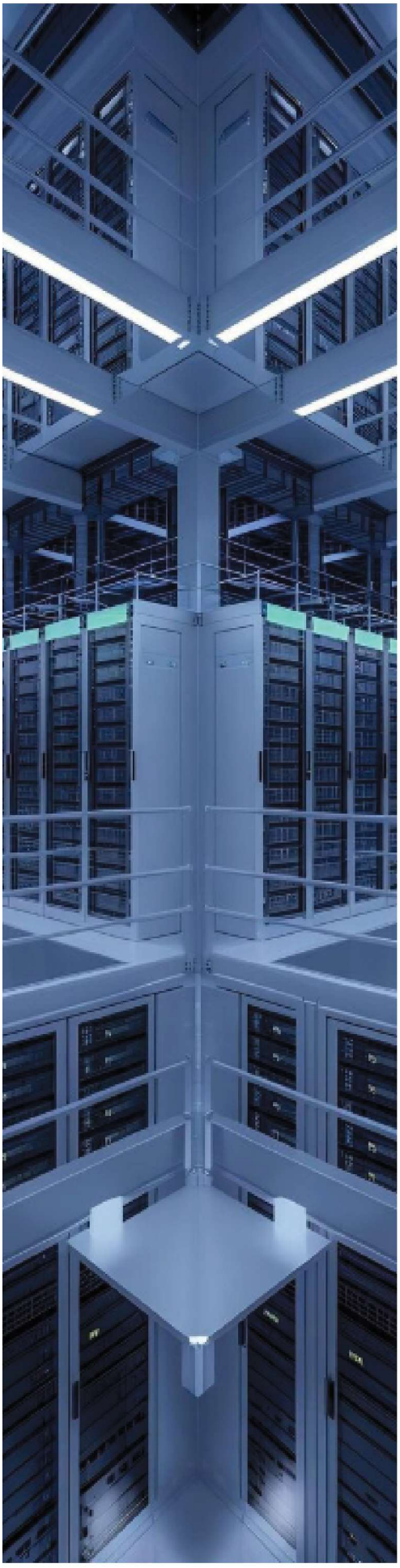


1. Executive Summary

The term 'air gap' has been diluted by marketing claims that conflate physical isolation with software-defined network segmentation. This white paper cuts through that ambiguity by anchoring the definition to its authoritative source: CNSSI 4009-2015, the Committee on National Security Systems Glossary maintained under the Director of National Intelligence (DNI) and used across the U.S. Intelligence Community, Department of Defense, and civil agencies.

Under that standard, a true air gap requires two non-negotiable conditions: (a) no physical network connection between systems, and (b) any data movement must be manual — not automated. Logical air gap solutions, no matter how sophisticated, satisfy neither condition in full. They maintain live network paths, rely on automated transfer mechanisms, and are therefore not air gaps by definition.

Bacula Enterprise is architected to satisfy the CNSSI 4009 definition. This paper explains how, documents the deficiencies of logical air gap approaches, and provides guidance for organizations — including critical infrastructure operators, defense contractors, and intelligence community partners — that must meet the highest standards of data isolation



2. The Authoritative Definition of an Air Gap

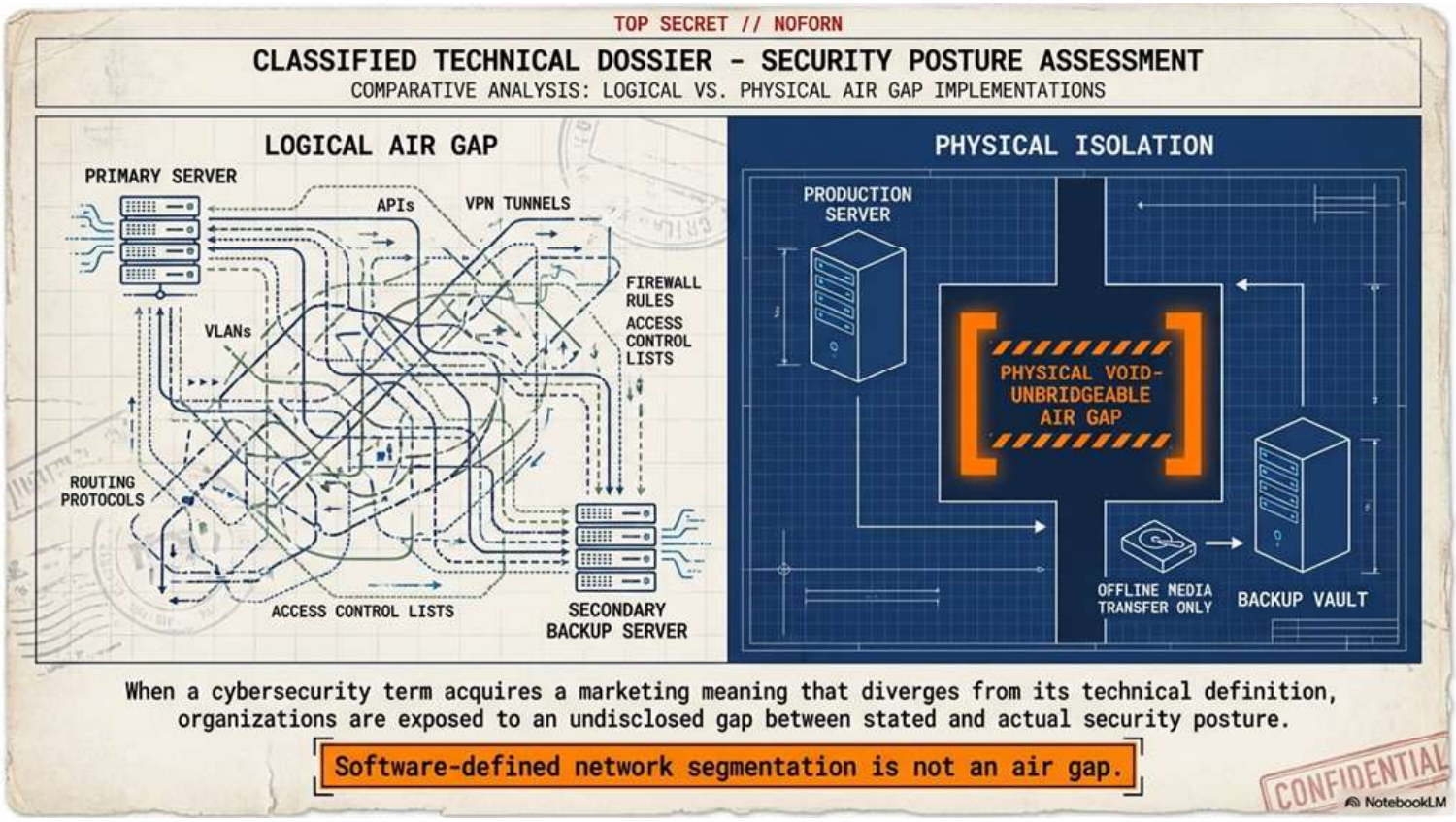
2.1 Market Scale and Explosive Growth

Precise language matters in cybersecurity. When a term acquires a marketing meaning that diverges from its technical definition, organizations that rely on that term in compliance frameworks, contracts, or policy documents are exposed to an undisclosed gap between stated and actual security posture. Nowhere is this more consequential than with the concept of the air gap.

The authoritative definition for national security systems — spanning the U.S. Intelligence Community, Department of Defense, and federal agencies — is established by the Committee on National Security Systems Instruction (CNSSI) No. 4009, published under the authority of the Director of National Intelligence. The 2015 edition of that document, drawing from IETF RFC 4949, defines an air gap as:

> "An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control)."
>
> CNSSI 4009

This definition contains two independent and equally necessary conditions. Both must be satisfied simultaneously. The failure of either condition means the interface does not constitute an air gap under the standard.



Condition A: No Physical Connection

The first condition is absolute: the two systems must not be connected physically. This means no Ethernet cable, no fiber link, no shared SAN fabric, and no wireless interface — not even a management network that is "segmented" by a firewall. A physical wire or wireless signal constitutes a connection regardless of the software policies applied to it. This condition rules out any architecture in which backup data resides on systems that are reachable via a live network path. VLAN segmentation, software-defined networking (SDN) zones, and cloud storage buckets with restrictive IAM policies all fail Condition A because a physical path exists between the production environment and the backup repository

Condition B: No Automated Data Transfer

The second condition is equally demanding: any data movement across the air gap interface must be manual — performed by a human, under human control, and not automated. This requirement exists because automation creates a programmable attack surface. Malware, ransomware, and advanced persistent threats (APTs) can exploit automated transfer mechanisms to traverse the gap even when the physical path is removed.

This condition rules out immutable object storage APIs, automated tape libraries that remain network-accessible, and cloud-based "air-gapped vaults" that receive data through orchestrated replication workflows. If a software process can initiate, schedule, or complete a data transfer without human intervention, Condition B is not satisfied.

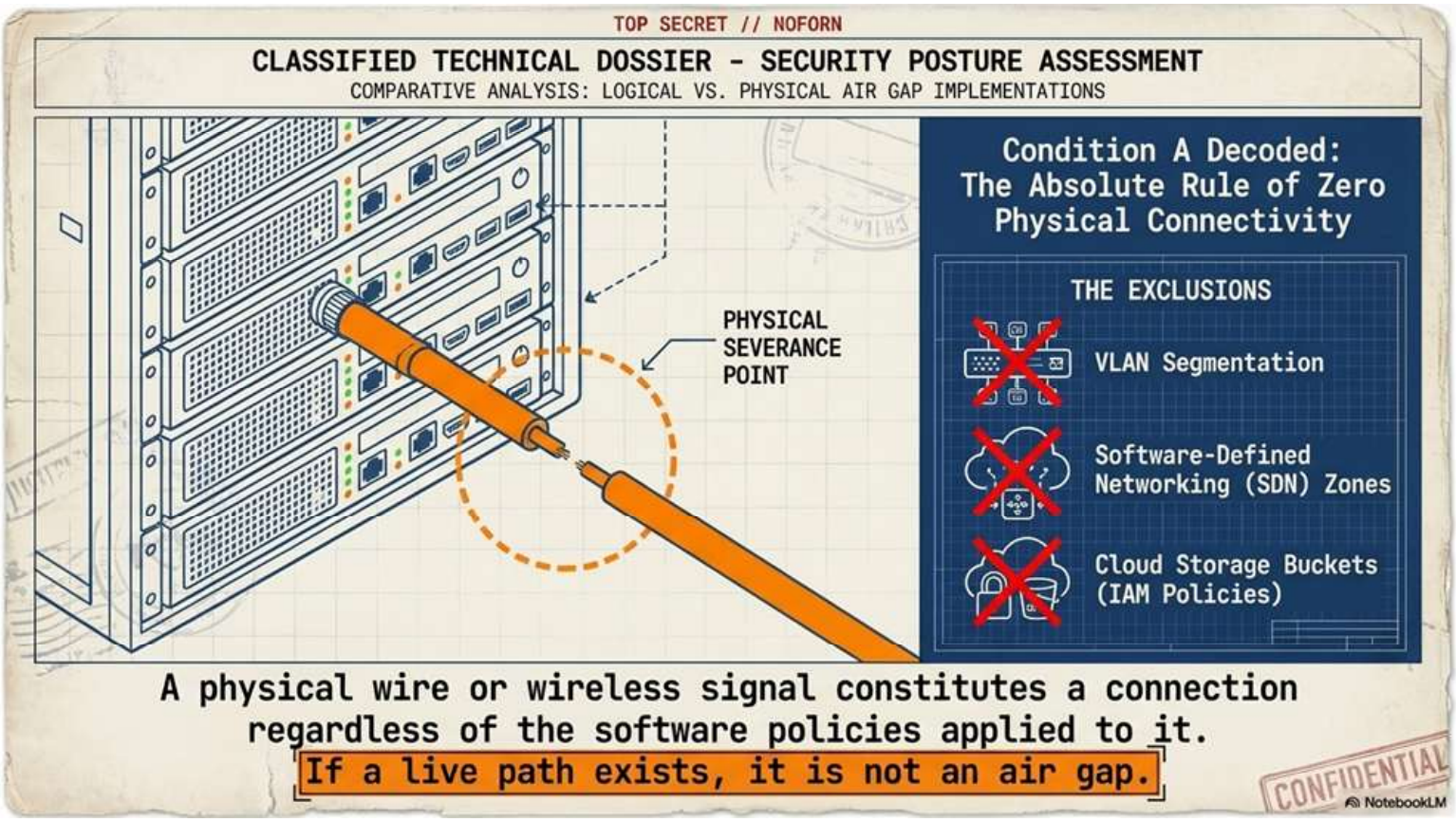
3. What Logical Air Gapping Actually Means

The term "logical air gap" has proliferated in vendor marketing as a way to associate their products with the security assurances implied by the CNSSI definition while delivering a fundamentally different architectural reality. Understanding what logical air gapping actually provides — and what it does not — is essential to evaluating compliance claims.

3.1 Common Logical Air Gap Implementations

Logical air gap claims typically rest on one or more of the following mechanisms:

- **Immutable Object Storage (S3 Object Lock, Azure Blob WORM):** Data is written to a cloud or on-premises object store with immutability flags that prevent deletion or overwriting for a specified retention period. The data remains accessible over a live network; only modification is restricted
- **Network-Isolated Storage VLANs**: Backup infrastructure is placed in a dedicated VLAN accessible only via jump hosts or dedicated management interfaces. Physical connectivity still exists; access is controlled by firewall rules and ACLs.



- **Automated "Vault" Replication**: Vendor appliances or cloud services periodically copy backup data to a secondary zone that is described as "air-gapped." The copy is initiated and completed automatically via software, with no human in the loop.
- **API-Gated Repositories:** Backup data is stored behind a restricted API with strong authentication. The API endpoint is reachable from the network; the "air gap" is the authentication requirement.
- **Data Diodes and Unidirectional Gateways**: Hardware devices enforce one-way data flow between networks. While this narrows the attack surface, the systems remain physically and logically connected; automated transfer still occurs.

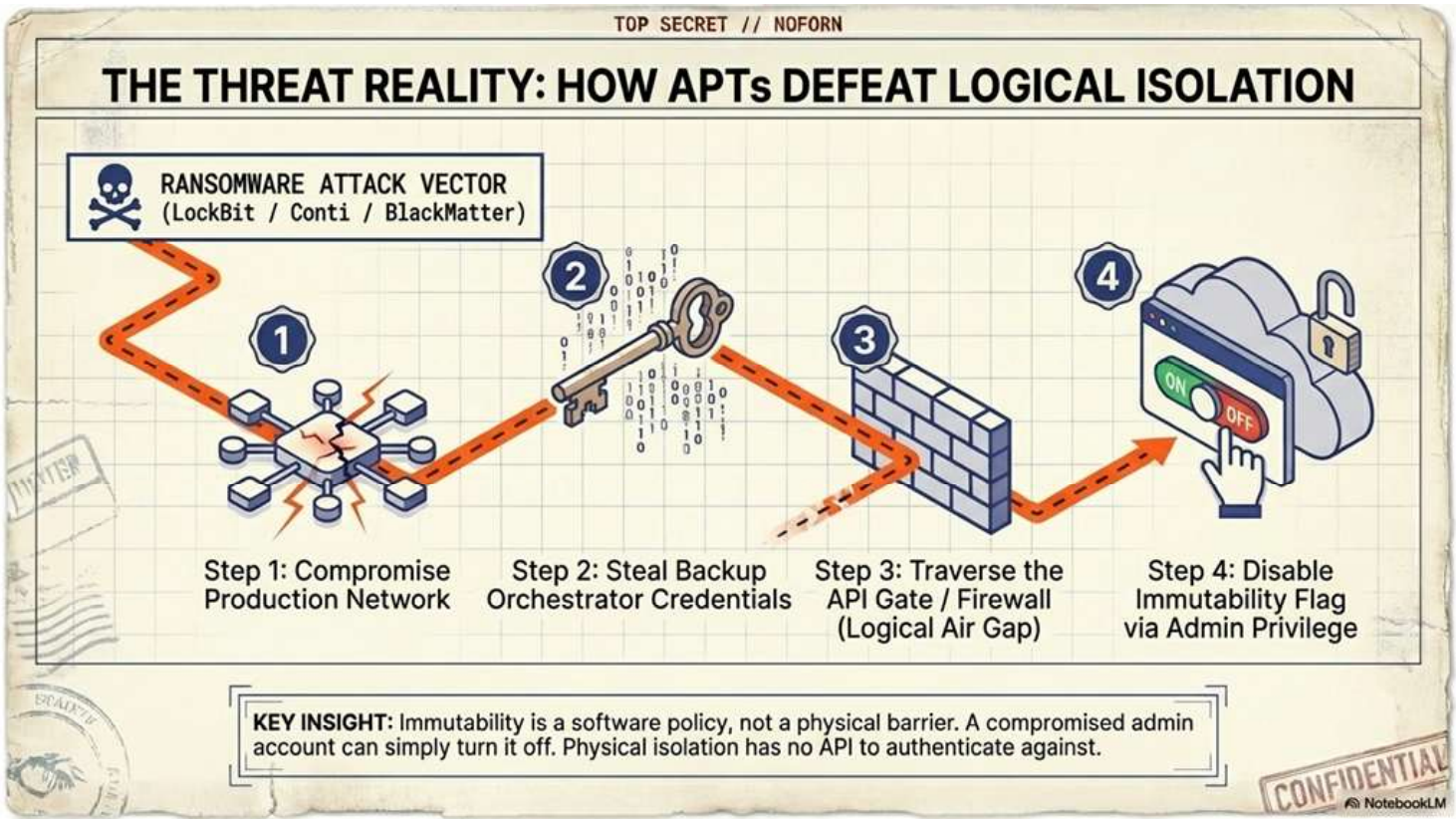
3.2 Why Each Mechanism Fails the CNSSI 4009 Standard

Applying the two-condition test from CNSSI 4009 to each of these approaches reveals consistent non-compliance:

Criterion	True Physical Air Gap (Bacula)	Logical Air Gap (Competitor Claims)
Physical Connectivity	Zero. Backup media (tape, portable drive) removed from all networks after write.	Present. Live network path exists to backup repository, even if segmented.
Data Transfer Control	Manual only. Human physically carries media to isolated environment	Automated. Software-initiated replication, scheduled jobs, or API calls move data without human intervention.
Attack Surface at Rest	None. No network interface active when media is in offline storage.	Present. Storage endpoint remains reachable; immutability flag is a policy, not a physical barrier.
Ransomware Traversal Risk	Near-zero for offline media. Attacker cannot reach isolated storage over a network.	Exists. Compromised orchestration account or zero-day in storage API can defeat logical controls.
Compliance with CNSSI 4009(a)	Satisfied. No physical connection.	Not satisfied. Physical connection or active network interface exists.
Compliance with CNSSI 4009(b)	Satisfied. Manual, human-controlled transfer.	Not satisfied. Transfer is automated by software.
Example Technologies	Bacula tape-out, offline removable media, physically isolated restore nodes.	AWS S3 Object Lock, Cohesity DataLock, Veeam SureBackup cloud tier, Rubrik Cloud Vault.

4 The Risk Profile of Logical Air Gaps

Logical air gap solutions are not without value. They provide meaningful defense-in-depth against opportunistic ransomware campaigns, reduce the blast radius of credential-based attacks, and support compliance with standards that do not require physical isolation. However, when an organization believes it has achieved a true air gap — and communicates that belief to regulators, auditors, insurers, or leadership — the gap between perception and reality creates material risk across several dimensions.



4.1 Ransomware and Sophisticated APTs

Modern ransomware groups and state-sponsored APTs are explicitly designed to defeat logical air gap implementations. Attack techniques documented against logically isolated backup infrastructure include:

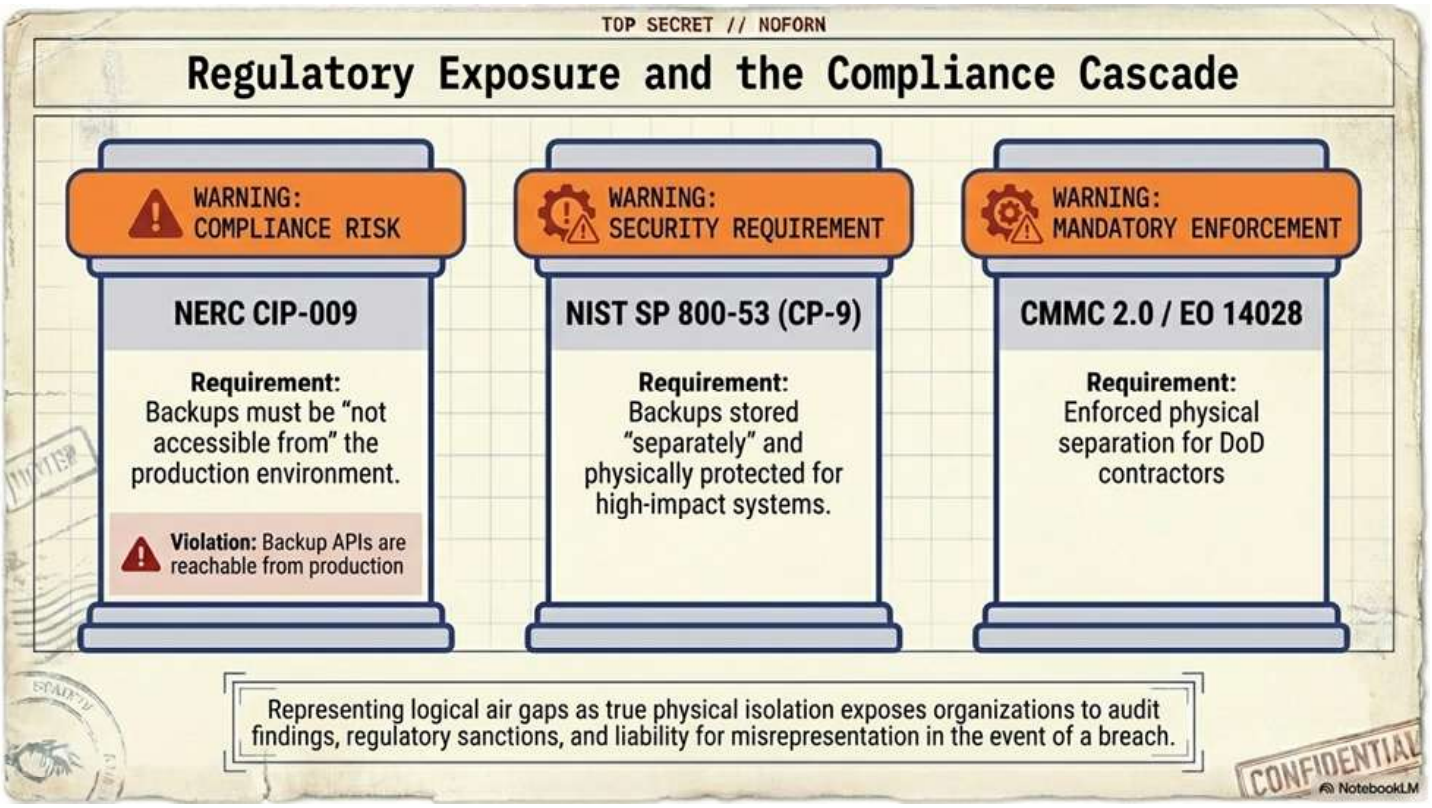
- **Credential Theft Against Backup Orchestrators:** Ransomware such as BlackMatter, Conti, and LockBit specifically target backup software administrative accounts. With valid credentials, an attacker can disable or corrupt data within the "vaulted" repository before triggering encryption.

- **API Exploitation:** Cloud storage APIs that accept authenticated requests to modify retention policies or delete versioned objects are a known attack vector. The immutability feature itself can often be modified by a sufficiently privileged account.
- **Supply Chain and Firmware Attacks:** Logical segmentation provides no protection against firmware-level compromise of network-attached storage devices, which can exfiltrate or corrupt data regardless of VLAN policy.
- **Living-Off-the-Land Techniques**: Attackers who achieve persistent access to a backup orchestration environment can schedule malicious jobs that appear to be legitimate backup operations, silently corrupting or exfiltrating the vault contents over time.

None of these attack vectors can traverse a true physical air gap. An offline tape cartridge stored in an access-controlled vault has no network interface to exploit, no API to authenticate against, and no scheduled jobs to hijack.

4.2 Compliance and Regulatory Exposure

Several regulatory frameworks explicitly require physical isolation or use language that maps directly to the CNSSI 4009 conditions:



- **NERC CIP-009:** Requires recovery plans for bulk electric system cyber assets. Interpretations by regulators increasingly require that backup copies be "not accessible from" the production environment — a condition that logical air gaps do not satisfy if the backup API is reachable from the production network.

- **IEC 62443 (Industrial Automation Security):** Zone and conduit models require that assets in different security levels maintain enforced separation. Physical isolation is the highest assurance tier; logical segmentation is a lower-assurance control.

- **NIST SP 800-53 Rev. 5, CP-9:** Directs that backup copies be stored "separately" from originals and protected from threats. While not mandating physical air gaps for all contexts, the guidance for high-impact systems aligns with physical separation.

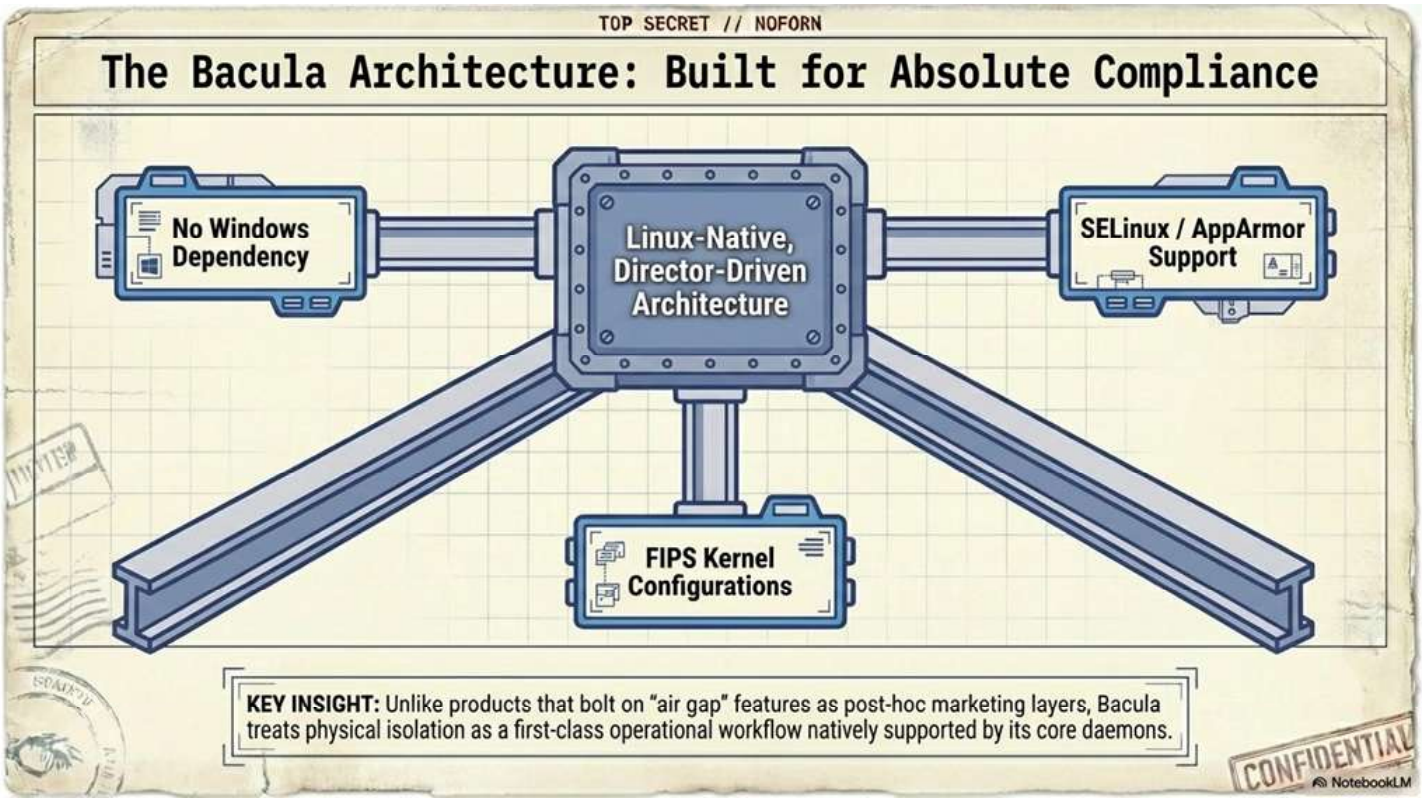
- **NSA/CISA Joint Advisories on Backup Security:** Repeatedly advise that "offline, immutable" backups means physically disconnected — not immutable flags on network-accessible storage.

- **Executive Order 14028 / CMMC 2.0**: Federal contractors are expected to implement data protection controls consistent with NIST 800-171 and, at higher levels, NIST 800-53, which for high-impact systems effectively requires physical air gap capability.

Organizations that represent logical air gap solutions as satisfying these requirements may face audit findings, regulatory sanctions, and — in the event of a successful attack that defeats the logical controls — liability for misrepresentation of their security posture.

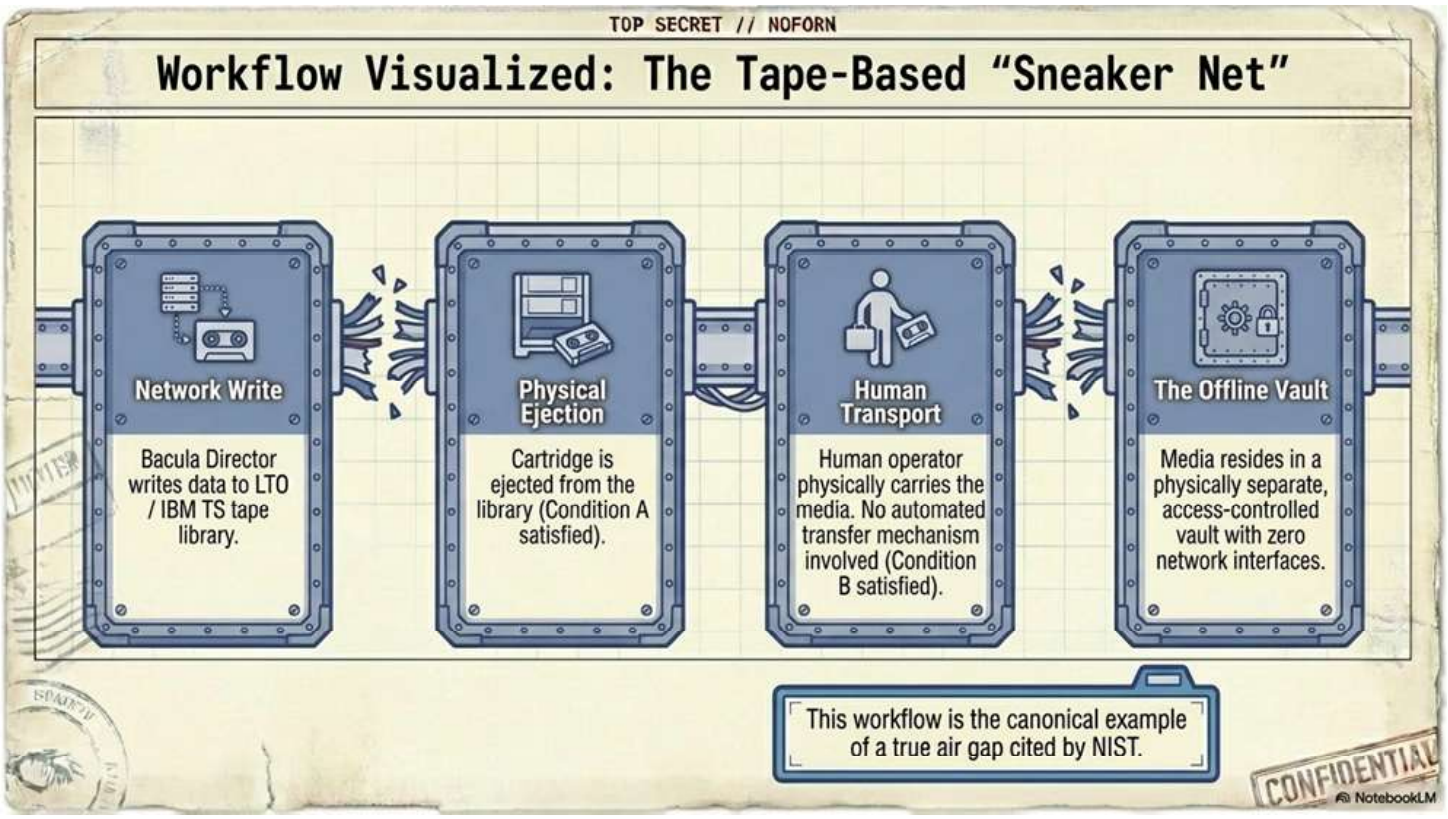
5 How Bacula Enterprise Satisfies the CNSSI 4009 Standard

Bacula Enterprise is designed from the ground up around a Linux-native, director-driven architecture that enables true physical air gapping as defined by CNSSI 4009. Unlike backup products that bolt on "air gap" features as post-hoc marketing layers, Bacula's architecture treats physical isolation as a first-class operational workflow.



5.1 Tape-Based Physical Air Gap

Bacula Enterprise provides native, production-grade integration with tape libraries and standalone tape drives using the LTO and IBM TS tape formats. The workflow satisfies both CNSSI 4009 conditions explicitly:



- **Condition A (No Physical Connection):** After a backup job writes to tape, the tape cartridge is ejected and physically removed from the library. The media is then transported to an offline vault — a physically separate location with no network connectivity. At that point, there is no physical interface between the tape and any network-connected system.

- **Condition B (Manual Transfer):** Moving tape media between the tape library and the offline vault is performed by a human operator. No automated mechanism can initiate or complete the transfer. The cartridge is physically carried; it does not traverse a network.

This workflow is directly analogous to the "sneaker net" model that the NIST Election Terminology Glossary cites as the canonical example of an air gap in operation. Bacula's tape management capabilities — including barcode tracking, slot management, volume pools, and retention scheduling — give organizations the operational discipline to implement this workflow at enterprise scale without sacrificing manageability.

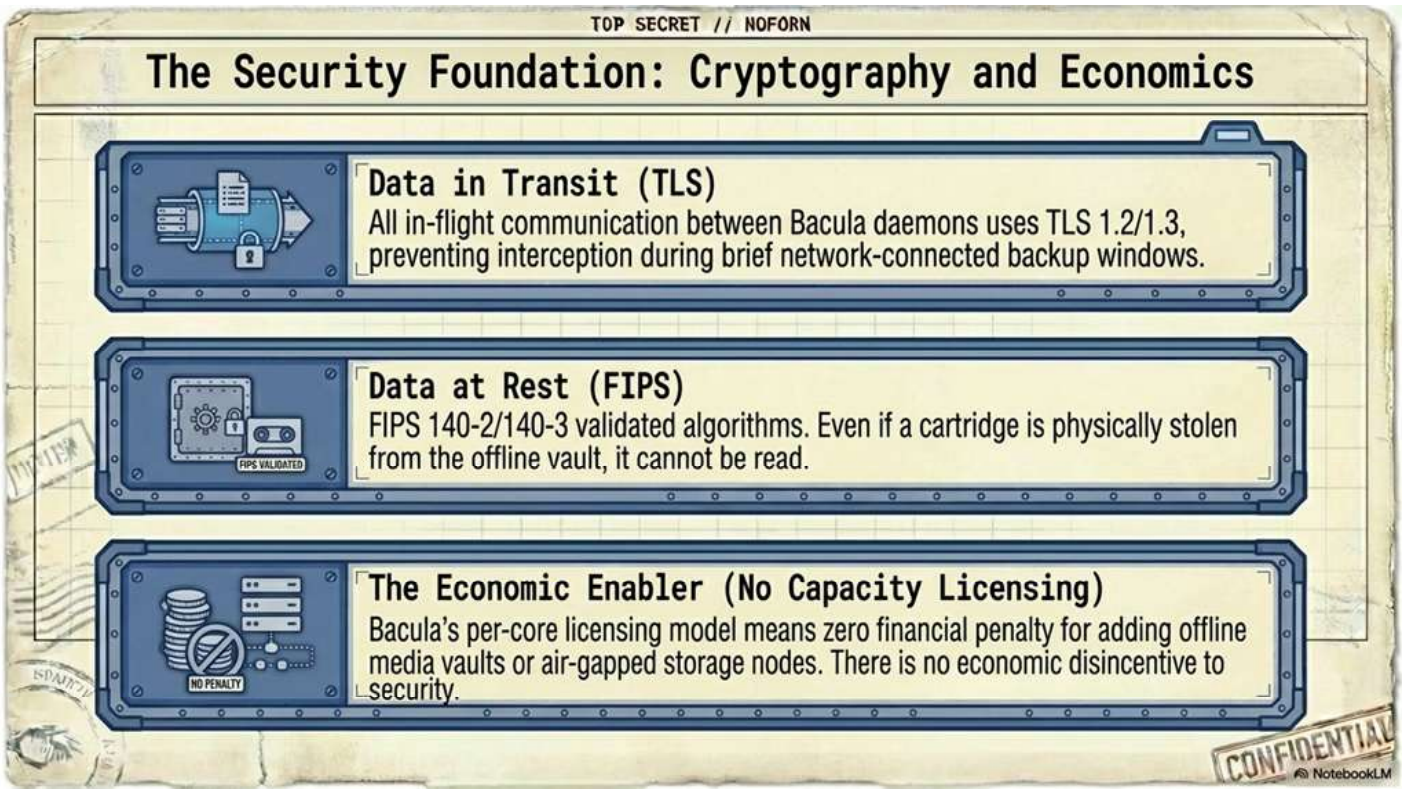
5.2 Physically Isolated Restore Nodes

For organizations that require disk-based backup with physical isolation, Bacula Enterprise supports architectures in which the storage daemon resides on a system that is network-connected only during the backup window and physically disconnected during the retention period. The Bacula director can be configured to execute a pre-job script that enables the network interface, run the backup, and execute a post-job script that disables or physically disconnects the interface — reducing the attack surface to the minimum possible window.

More advanced implementations use out-of-band management (IPMI/BMC) to control power and network connectivity of the storage node entirely separately from the backup data path, ensuring that the administrative control plane for isolation decisions is never co-located with the data plane that an attacker would seek to compromise.

5.3 Security Architecture Supporting True Air Gap Operations

The following Bacula Enterprise security features reinforce the integrity of true air gap workflows:



- **TLS-Encrypted Communications:** All in-flight communication between Bacula daemons uses TLS 1.2 or 1.3, ensuring that data in transit cannot be intercepted during the backup window when the storage node is briefly network-connected.

- **FIPS 140-2/140-3 Validated Cryptography**: Data at rest on tape and disk is encrypted using FIPS-validated algorithms, so media that is physically stolen from the vault cannot be read without the encryption key.

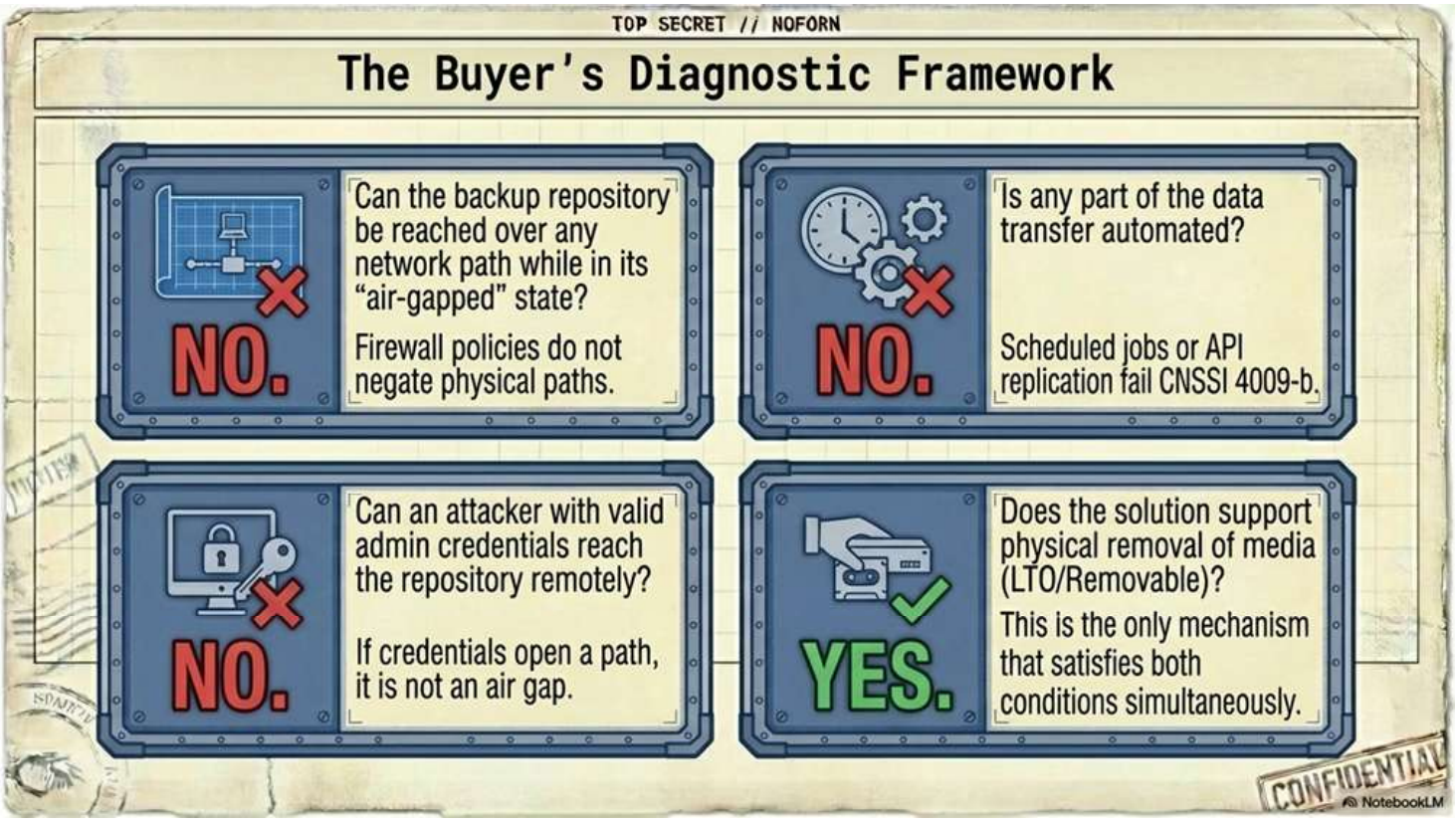
- **Role-Based Access Control and Audit Logging:** All Bacula director operations are logged with full audit trails. Attempts to modify retention policies or access job configurations generate auditable events, supporting forensic investigation if an attempted breach is suspected.

- **No Capacity-Based Licensing:** Bacula's per-core licensing model means organizations are not penalized for adding air-gapped storage nodes or offline media vaults. There is no economic disincentive to implement true physical isolation.

- **Linux-Native Architecture:** The absence of a Windows dependency eliminates a significant attack surface. The Bacula director and storage daemons run on hardened Linux, supporting SELinux, AppArmor, and FIPS kernel configurations that are required in classified and high-assurance environments.

6 Evaluating Vendor Air Gap Claims: A Practical Framework

Security and procurement professionals evaluating backup solutions for environments that require true air gap capability should apply the following questions directly to vendor claims. If any question cannot be answered with a definitive "yes," the solution does not satisfy the CNSSI 4009 definition.



Evaluation Question	What a Compliant Answer Requires
Can the backup repository be reached over any network path while in its "air-gapped" state?	**The answer must be "no".** Any live network path — regardless of firewall policy, VLAN, or authentication requirement — disqualifies the solution under CNSSI 4009(a).
Is any part of the data transfer from production to the isolated repository automated?	**The answer must be "no".** Condition (b) requires that data cross the air gap interface only manually, under human control. Scheduled jobs, API-driven replication, and automated media libraries do not qualify.
Can an attacker with valid backup administrator credentials reach the isolated repository remotely?	**The answer must be "no".** If credentials can open a network path to the repository, it is not air-gapped.
Does the solution support LTO tape or equivalent removable media that can be physically removed from all network-connected systems?)	Yes is required. Physical removal is the canonical mechanism by which both CNSSI conditions are satisfied simultaneously.
Can the vendor provide documentation of physical air gap workflows certified or validated for use in ICS, DoD, or Intelligence Community environments?	Yes is required for regulated environments. Marketing claims are not a substitute for documented technical architecture.

7 Industry Context: What Happened to the Air Gap Definition

The erosion of the air gap definition is not accidental. As cloud and hyperconverged infrastructure reduced the operational burden of managing physical tape workflows, backup vendors sought ways to provide the security assurances associated with air gapping without its operational complexity. The result was a marketing evolution that repurposed the term.

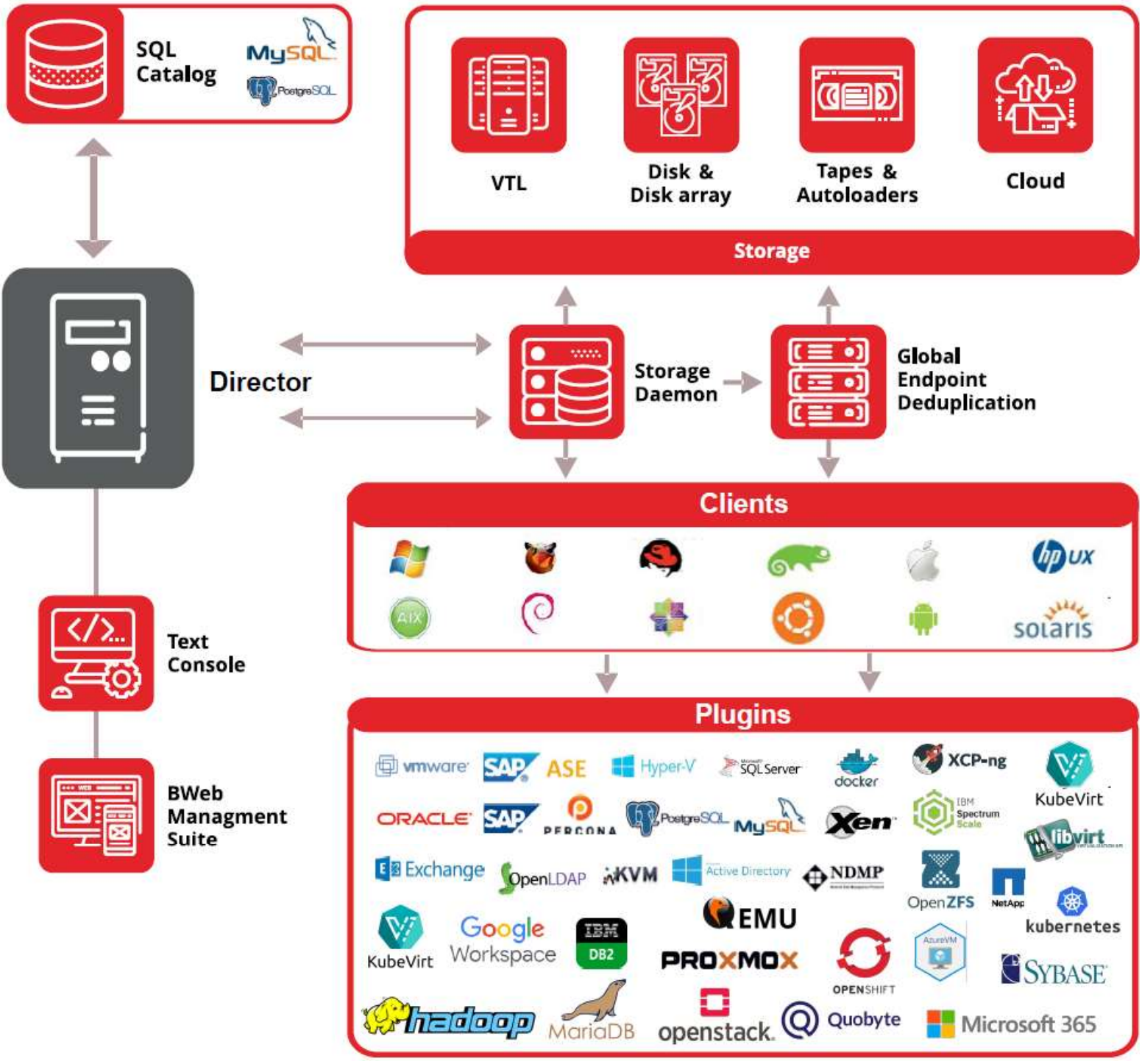
The pattern follows a predictable arc: first, the term is broadened by adding a qualifier ("logical air gap," "near air gap," "cloud air gap"), then the qualifier is dropped in executive summaries and marketing materials, and ultimately the modified term achieves sufficient penetration that buyers begin to treat it as equivalent to the original.

This is not a theoretical concern. Several prominent ransomware attacks in the period 2020–2024 succeeded specifically because the targeted organizations believed their logical air gap solutions provided physical isolation. Post-incident analysis in multiple cases revealed that the ransomware had traversed the "air gap" via the backup orchestration API, encrypting or deleting backup data before triggering payload deployment in the production environment.

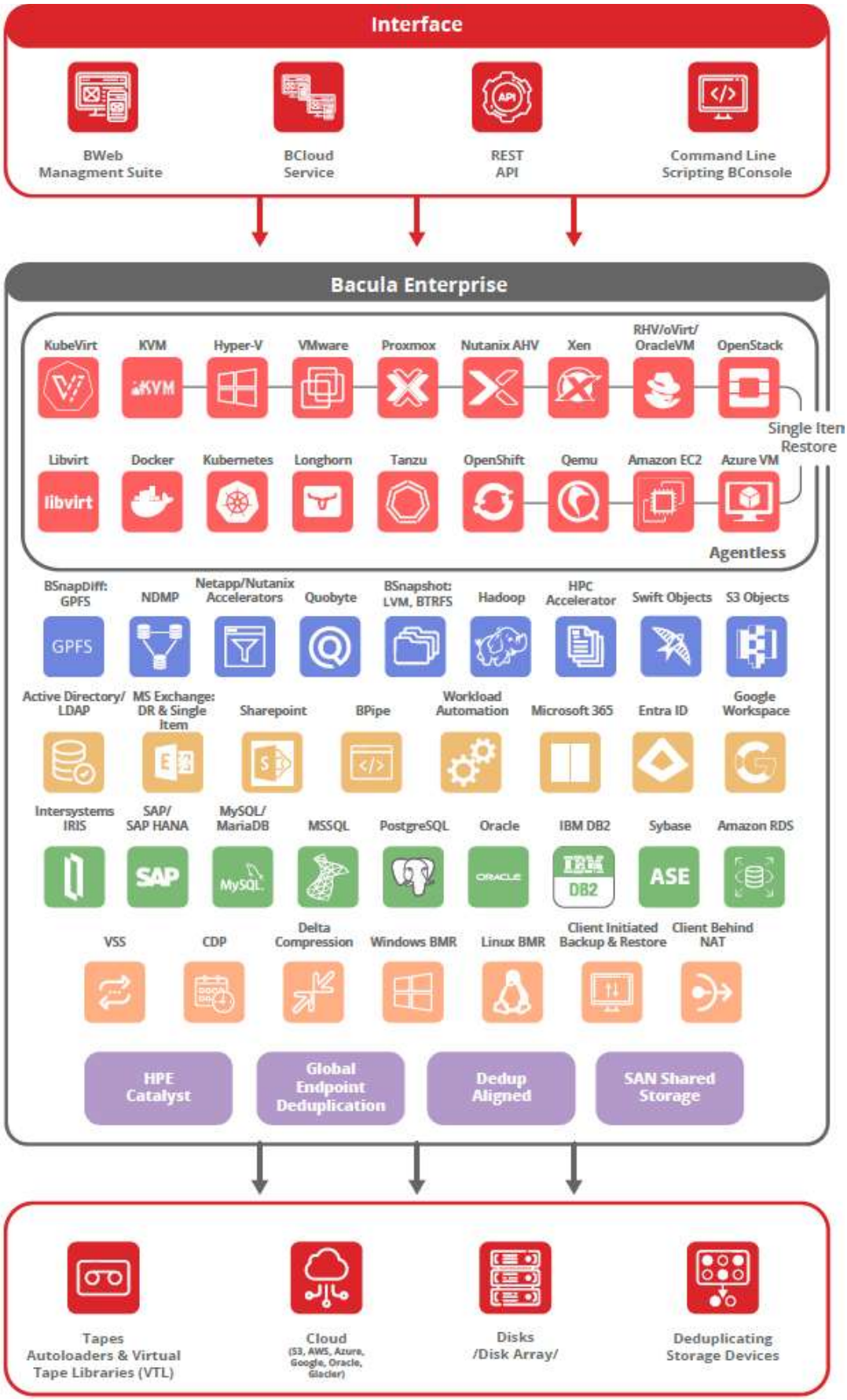
The intelligence and defense communities — who originated the air gap concept and have the greatest operational experience with it — have not changed their definition. CNSSI 4009 continues to require physical non-connection and manual data transfer. Organizations that must meet those community standards, or that aspire to the security assurance level they represent, have only one option: implement true physical air gapping.

8. Bacula's Advanced Modular Architecture

Bacula's modularity enables far higher levels of security and efficiency in AI and HPC infrastructures than any other data protection solution.



Bacula Enterprise has a broader range of technology integrations than any other data protection solution.



9 Conclusion

The Committee on National Security Systems definition of an air gap — physical non-connection combined with manual data transfer — represents the standard that has guided intelligence community, defense, and critical infrastructure security for decades. It is not an aspirational ideal; it is a precise technical criterion that either is or is not satisfied by a given architecture.

Logical air gap solutions provide value as defense-in-depth mechanisms, but they do not satisfy the CNSSI 4009 definition. They maintain live network paths and rely on automated transfer mechanisms. The security properties they provide, while meaningful, are categorically different from those provided by a physically isolated backup copy that has no network interface and can only be accessed by a human being carrying physical media.

Bacula Enterprise is built to satisfy the CNSSI 4009 standard in full. Its native tape integration, support for physically isolated restore nodes, FIPS-validated encryption, Linux-native architecture, and per-core licensing model combine to make it the platform of choice for organizations that need true air gap backup — not a logical approximation of it.

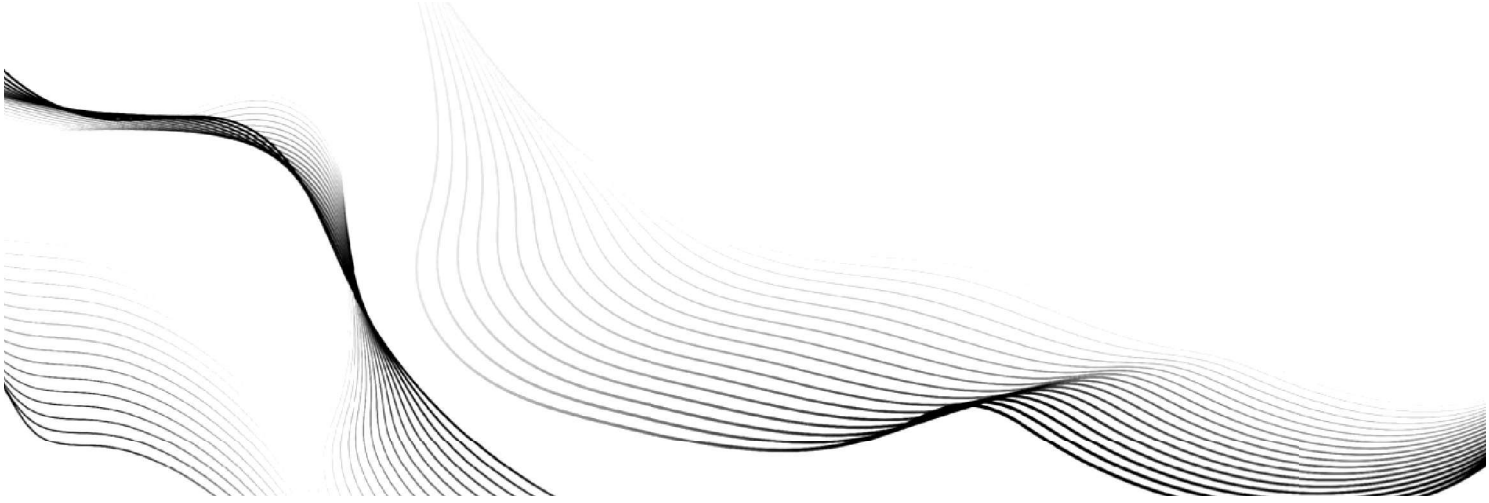
For critical infrastructure operators, defense contractors, intelligence community partners, and any organization whose risk posture demands the highest available assurance of backup data integrity and recoverability, the choice is clear: only a true physical air gap, as defined by the authority that originated the standard, provides the protection the term implies.

About Bacula Systems SA

Bacula Systems SA is an enterprise backup and recovery software company headquartered in Yverdon-les-Bains, Switzerland. Bacula Enterprise Edition is deployed across HPC national laboratories, critical infrastructure operators, financial institutions, healthcare organizations, and defense agencies worldwide.

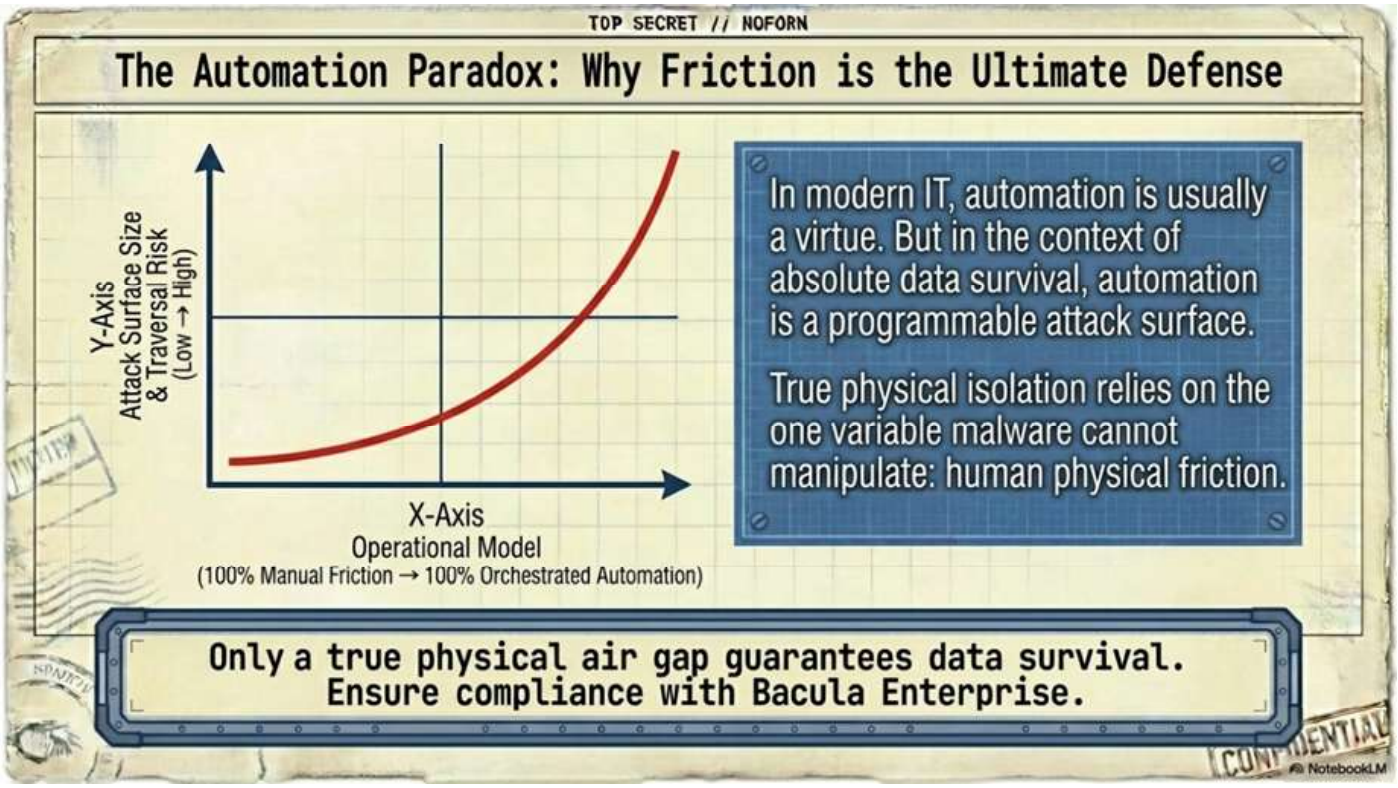
Bacula's Linux-native, director-driven architecture, per-core licensing model, and security-first design — including FIPS 140 cryptography, IEC 62443-aligned zone support, and true tape-based air gap capability — make it uniquely suited for organizations operating in high-assurance and regulated environments.

Don't let backup constraints limit your security. Contact Bacula today and discover how its comprehensive data protection can accelerate your path to higher security levels.



Document Version: 2.0
Publication Date: January 2026

www.baculasystems.com



No Other Data Protection Vendor Can Provide Air Gap Security To The Same Levels As Bacula Enterprise.

References

1. Committee on National Security Systems. CNSSI No. 4009-2015: National Information Assurance (IA) Glossary. Published under authority of the Director of National Intelligence. April 6, 2015.
2. Internet Engineering Task Force. RFC 4949: Internet Security Glossary, Version 2. R. Shirey. August 2007. (Source document cited by CNSSI 4009 for the air gap definition.)
3. National Institute of Standards and Technology. NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. September 2020.
4. National Institute of Standards and Technology. NIST Cybersecurity Practice Guide SP 1800-11: Data Integrity: Recovering from Ransomware and Other Destructive Events. 2020.
5. Intelligence Community Directive 705: Sensitive Compartmented Information Facilities. Office of the Director of National Intelligence. May 26, 2010.
6. North American Electric Reliability Corporation. CIP-009-6: Recovery Plans for BES Cyber Systems. Effective 2016.
7. International Electrotechnical Commission. IEC 62443: Security for Industrial Automation and Control Systems. Various parts, 2011–2023.
8. Cybersecurity and Infrastructure Security Agency. #StopRansomware Guide. CISA, NSA, FBI, MS-ISAC. May 2023.
9. U.S. National Security Agency / CISA. Joint Cybersecurity Advisory: Protecting Against Malicious Use of Remote Monitoring and Management Software. January 2023.