BROADCOM

Executive Summary

Air-Gapped: Isolation in an Always-Connected World

Air-gapped systems have long been considered the gold standard for protecting the most sensitive environments, relying on physical isolation to prevent unauthorized access. In today's interconnected world, however, complete isolation is increasingly difficult to maintain. Organizations face growing pressure to enable data sharing, cloud integration, and operational efficiency, which introduces new pathways into environments once considered secure.

This shift creates a critical challenge: systems designed to be isolated are now partially connected, often without the controls required to manage that exposure. As a result, many environments that are assumed to be "air-gapped" are, in reality, operating within a spectrum of isolation where risks such as removable media, insider activity, and supply chain compromise can bypass traditional defenses.

To address this, organizations must rethink the role of the air gap. Rather than treating it as a standalone control, it should be integrated into a broader defense-in-depth strategy that combines strict boundary enforcement with internal visibility, endpoint protection, and governed data movement. Zero trust principles (i.e., continuous verification, least privilege, and monitoring of all activity) are essential to ensuring that isolation remains effective even as connectivity increases.

The most resilient organizations recognize that isolation is no longer binary. By defining and controlling how data crosses boundaries, enforcing layered protections within sensitive environments, and continuously validating systems and users, they can preserve the intent of the air gap while adapting to modern operational demands.

The Isolation Gap

Many "air-gapped" environments are not truly physically isolated

Logical segmentation (VLANs, firewalls) ≠ physical isolation

Each new connection introduces a potential attack path

Assumed isolation often leads to *unmonitored risk exposure*

Primary Risk Vectors

Removable Media
Primary method for bypassing air gaps

Insider Behavior
Trusted users introducing or exfiltrating data

Supply Chain Compromise
Hardware/firmware introduced into the enclave

Misconfigured "Virtual Gaps"
False sense of security from logical controls

From Air Gap to "Virtual Gap"

- Isolation now exists on a spectrum, not a binary state.
- True air gaps remain essential for highest-risk systems.
- Most environments operate with controlled connectivity.
- Security depends on how well those connections are governed.

Key Practices for Securing Air-Gapped Environments

Enforce Controlled Data Transfer
Use verified, auditable workflows for all boundary crossings

Deploy On-Premises Security Controls
Endpoint protection, logging, and monitoring within the enclave

Implement Hardware-Based Boundaries
Unidirectional gateways (data diodes) for secure data flow

Apply Zero Trust Principles
Continuous verification of users, devices, and activity

Strengthen Governance and Oversight
Formalize processes for patching, access, and change management

Prepare for Offline Incident Response
Pre-stage tools and define physical response procedures

Bottom Line for Executives

Air gaps remain a critical control, but they are no longer sufficient on their own. Organizations must treat isolation as a continuously enforced capability, combining physical separation with layered defenses, visibility, and strict governance.

Those that successfully evolve from static air gaps to managed "virtual gaps" can reduce risk, maintain mission integrity, and enable secure operations in an increasingly connected world.

SANS | Research Program

What's at Stake

Operational Disruption
Loss of control over critical or safety systems

Security Breaches
Malware introduced via removable media or supply chain

Data Exposure
Sensitive or classified data crossing uncontrolled boundaries

Mission Impact
Compromise of national security, critical infrastructure, or sensitive information