BROADCOM

Air-Gapped: Isolation in an Always-Connected World

Air-gapped systems were designed for complete isolation—but modern connectivity demands have transformed them into continuously managed environments.

Key Topics

Why This Matters → The Isolation Gap → Isolation Spectrum → Key Security Practices → Zero Trust Alignment → Bottom Line

Why This Matters

Air-gapped environments were once physically isolated by design. Today, cloud adoption, IT/OT convergence, and real-time data sharing introduce new pathways into systems that were never meant to be connected.

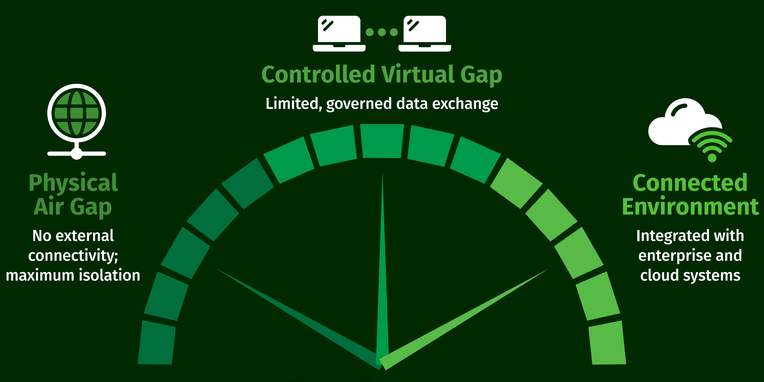
Many organizations now operate with ***assumed isolation—not actual isolation—creating unseen risk.***

The Isolation Gap

Not all "air gaps" are equal.

- Logical segmentation ≠ physical isolation
- Hidden connections create unintended access paths
- Security controls often stop at the boundary
- Internal activity lacks visibility and monitoring

Core Concept: The Isolation Spectrum



Key Security Practices

To secure air-gapped environments, organizations must:

- **Control Data Movement**
  Enforce strict, auditable transfer processes
- **Deploy On-Premises Security Controls**
  Enact endpoint protection, logging, and monitoring within the enclave
- **Implement Hardware-Enforced Boundaries**
  Use unidirectional gateways where possible
- **Apply Zero Trust Principles**
  Verify users, devices, and activity continuously
- **Strengthen Governance and Oversight**
  Formalize patching, access, and change management
- **Prepare for Offline Incident Response**
  Enable physical and manual response capabilities

Zero Trust Alignment

Air-gapped security aligns with zero trust:

- Validate every user and device
- Monitor all activity within the boundary
- Limit lateral movement through segmentation

"Never assume isolation—always verify."

Bottom Line for Executives

Air gaps are not obsolete—but they are no longer sufficient on their own. Organizations must evolve from static isolation to actively managed, layered security, ensuring that even when boundaries are crossed, risk is controlled and contained.

BROADCOM

SANS | Research Program