5G'S NEXT TEST: TURNING INFRASTRUCTURE INTO REAL RETURNS | 16

₹100

www.voicendata.com

VOL 33 ISSUE 03 MARCH 2026

VOICE & DATA

Connecting the Digital World

CyberMedia

FROM PILOTS TO PLATFORMS: IIoT GROWS UP

Factory systems are evolving into a layered digital infrastructure where sensors, connectivity, edge computing and AI are driving real-time operational decisions.

"CUSTOMERS TODAY ARE BUYING OUTCOMES, NOT PRODUCTS"

ASHOK SHIVASHANKAR, Cisco India & South Asia

46

76 pages including cover

Special subscription offer on Page 56

"Full physical isolation is rarely practical in modern connected operations, so organisations rely on tightly controlled architectures and continuous monitoring."

VIVEK SRIVASTAVA
Country Manager, Fortinet India

Routine security activities, such as software updates, require carefully controlled procedures involving physical supervision, restricted vendor access, and airlock-style handling. Patch management in particular can become cumbersome and time-consuming. Removable media such as USB drives can become major threat vectors.

Srivastava emphasises that air-gapped systems are not automatically immune to threats. "Operationally, they introduce complexity, especially in patch management, monitoring, and controlled data exchange. Updates must often be performed manually, which can delay remediation if processes are not disciplined." Physical isolation also does not eliminate insider threats, supply-chain risks, or social engineering attacks.

Mishra illustrates the challenge with a simple scenario. When a zero-day vulnerability is discovered, threat actors can begin exploiting it within hours. However, deploying a patch in a physically air-gapped environment may take days or even weeks due to validation procedures, transfer controls, and staged deployment processes. This delay can give attackers a temporal advantage.

A LAYERED APPROACH TO MODERN SECURITY

Air-gapping, therefore, should not be treated as a stand-alone security strategy. Security researchers have demonstrated numerous ways to breach isolated systems, ranging from infected USB drives to acoustic side-channel attacks that transmit data through sound or heat.

Pankit Desai, CEO and Co-Founder of Sequretek, argues that relying solely on air-gapping is no longer sufficient. "Gone are the days when you could simply air-gap systems and consider them secure. Security today must be more sophisticated than just cutting a cable. Physical isolation is not a magic shield." The well-known Stuxnet attack, which infiltrated Iranian nuclear facilities through infected USB drives, illustrates how determined adversaries can bypass isolation mechanisms.

The human factor remains another major vulnerability. With the rise of generative AI, phishing campaigns have become more convincing and scalable. According to Mishra, the increase in AI-assisted phishing attacks highlights a critical reality: the human layer remains one of the most exploitable components of any security architecture.

For most enterprises, therefore, the objective should not be disconnection but secure connectivity. IoT systems are designed to collect, transmit, and analyse data across distributed environments, making full physical isolation impractical.

Srivastava recommends focusing instead on strong network segmentation, Zero Trust access controls, continuous monitoring, threat intelligence, and unified visibility across IT, operational technology, and IoT environments. Platform-based architectures that integrate networking and security can help organisations protect distributed deployments without sacrificing performance.

Vembu also emphasises that air-gapping should be applied selectively. It works best as one layer within a broader security architecture. For sectors such as energy, defence, or certain healthcare systems where compromise could have national or safety implications, some degree of air-gapping may be justified. However, for most enterprise environments, disciplined patching, strict access controls, strong segmentation, and continuous monitoring often provide more practical and scalable protection.

Ultimately, security is about reducing risk rather than chasing absolute isolation. If only air-gaps were as effortless as an invisible cloak rather than as cumbersome as walking through a crowded mall in a PPE suit.

pratimah@cybermedia.co.in