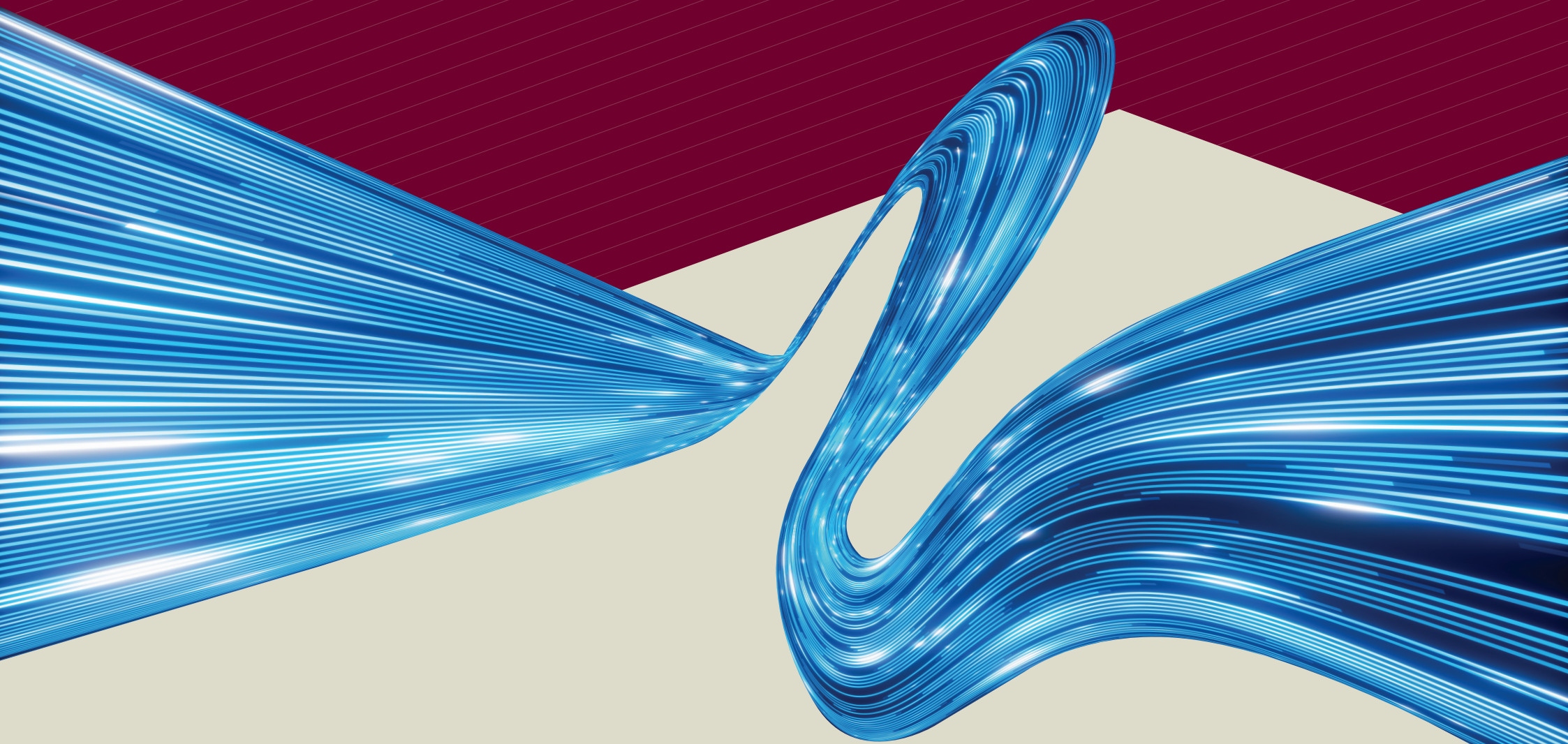
TECH mahindra

WHITEPAPER

# **Securing the Future of Telecommunications:** Implementing Zero Trust Security Architecture



## Executive Summary: Moving from Concept to Culture

Zero Trust is not a product. It is an operating stance that requires verifying every connection every time. While this principle sounds simple, it's a relentless discipline that most telecom programs fail at. Despite years of exposure, the telecom industry has broadly misunderstood what genuine Zero Trust implementation demands. The terminology is ubiquitously used. But the discipline to implement it is still missing across many operators, and this disconnect is becoming a critical liability.

The security concerns are constantly compounding. With the expansion of 5G, large-scale IoT, and cloud acceleration, the number of entry points has multiplied. In this new reality, relying on perimeter defenses is not just outdated; it's dangerous. This whitepaper discerns the operational shifts required to move from strategy to execution.

## Table of Contents

# Introduction: The Current State of Security in Telecom

The telecom sector is facing a critical security juncture. 5G rollouts, IoT at scale, cloud migration, and edge computing are actively reshaping networks and are also rewriting the rules of security. While attackers have kept pace with this evolution, most security programs have not. Consequently, Zero Trust has become the industry's default mandate. Governments enforce it, vendors sell it, and boards demand it. Yet, many leaders still underestimate what this approach requires in practice. Currently, Zero Trust is confined to strategy documents and vendor pitches. To make it an operational reality, the industry must shift from strategic intent to relentless execution.

At its core, Zero Trust is simple: never assume anything is safe until verified. Every user, every device, and every connection must be validated every time. The model breaks when organizations treat this principle as a one-time project. Zero Trust is not a rollout. It is a permanent cultural shift in how access and risk are managed. Most implementations fail precisely here. Organizations often choose the appearance of adoption over the substance of defense, reducing Zero Trust to a mere compliance exercise.

To build a resilient defense in telecom operations, organizations must adopt an integrated architecture that enforces verification across every layer of the network. Here's a rundown.

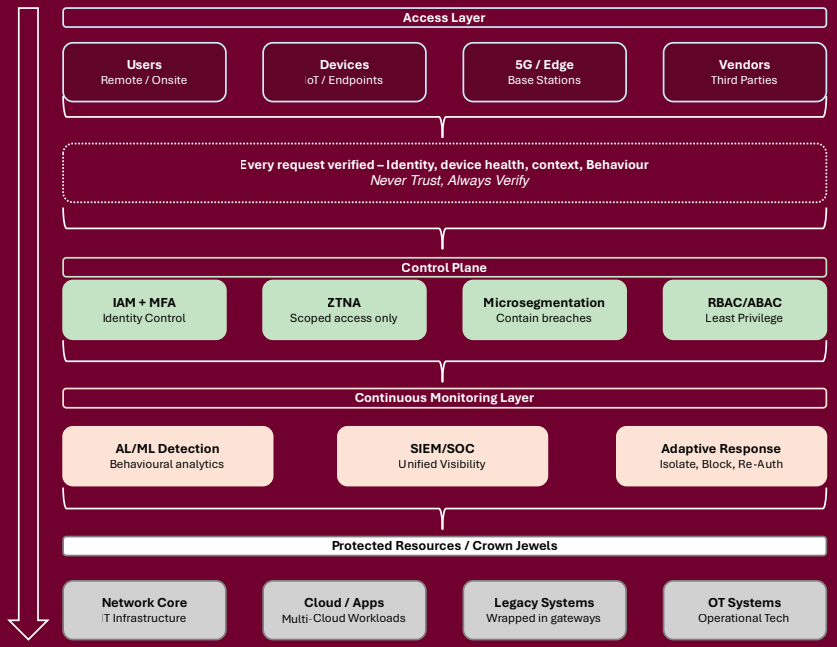



Figure 1: Four-Layered Zero Trust Security Architecture

## Perimeter Thinking, IT/OT Gaps, and Nation-State Threats

Most operators are still defending with a perimeter that stopped working years ago. The reality is, users now access networks from everywhere. Applications typically run outside traditional data centers, and vendors and contractors require recurring access to critical systems. Static boundary controls such as firewalls, VPNs, and perimeter tooling were not designed to handle this level of complexity. As a result, when an attacker slips past the outer layer, many networks still offer too little resistance to lateral movement. In practice, a single compromised credential can become a multi-system incident, quietly and quickly.

The boundary between IT and OT has effectively disappeared, but many operators have not aligned ownership, tooling, or response. Virtualization, cloud-hosted core functions, and remote management have connected these domains without security as a primary design constraint. If IT and OT are not treated as a single security ecosystem, Zero Trust remains strong in theory and weak in practice.

Above all, telecom faces patient adversaries with strategic objectives. Since 2021, government-backed cyberattack campaigns have targeted telecommunications providers.[1] Public reporting describes adversaries embedding quietly, subtly modifying configurations, and maintaining access for extended periods. In such scenarios, perimeter defense fails to offer value or protection.

## Core Zero Trust Principles and Implementation Gaps

Many telecom companies talk about Zero Trust. But only a few enforce it. While tools and policies change, the underlying trust model remains the same, repackaged in a newer language. The following principles define Zero Trust and reveal where implementations break down.

## Continuous Verification

Continuous verification is not a login prompt, and access is not a one-time event; it is a continuous security responsibility. Yet many providers still rely on one-time authentication to approve logins and validate sessions. When credentials are stolen or devices are compromised, traditional defense mechanisms fall apart. In a Zero Trust environment, identity, device health, and access patterns are constantly validated. If the risk changes, the access decision is re-evaluated automatically. Without this verification loop, it is not Zero Trust. It's a front door on a building with no internal locks.

## Micro segmentation

Micro segmentation divides the network into smaller, controlled zones to contain breaches. What most operators get wrong about the approach is that they stop halfway, creating broad zones and calling it segmentation. This partial implementation is not enough and creates a false sense of safety. Real defense, in contrast, requires granular enforcement and strict traffic paths to prevent attackers from moving freely between systems. When implemented effectively, it contains incidents and limits their impact.

## Least Privilege

Least privilege ensures users and systems have only the access required, no more and no longer than necessary. Typically, permissions accumulate over time, people change roles, vendors cycle in and out, and accounts outlive projects. Each overprivileged identity provides attackers with leverage, enabling lateral movement, privilege escalation, and data extraction without detection. Least privilege prevents abuse, and through sustained discipline, it supports governance and continuous review.

## Continuous Monitoring and Adaptive Response

Most operations centers face the same reality: more logs, more tools, and more alerts than humans can triage. Individual events are visible; the pattern connecting them often isn't. When monitoring pairs with adaptive responses, the system acts before humans can, restricting access, isolating workloads, and forcing re-authentication. At telecom scale, this automation makes continuous verification operationally viable.

# Implementing Zero Trust Security Architecture in Telecom

Adopting Zero Trust in a live telecom environment is challenging, not because the principles are complex, but because most networks are vast, interconnected, and built on infrastructure designed before identity-based access and continuous verification became practical. Relabeling existing tools does not change trust behavior. To be credible, every user, device, and connection must earn access each time, with no exceptions. This shift is cultural as much as technological, and tools only work when the organization enforces them consistently.

## A robust Zero Trust security architecture includes:

### IAM, MFA, and ZTNA

A credible Zero Trust implementation starts with effective identity and access management. When location cannot be trusted, identity becomes the control plane for all access decisions. Therefore, every user, device, and service must be verified before accessing critical resources. MFA is the most direct way to reduce the impact of stolen credentials, especially for privileged access. Strong role-based access control limits permission sprawl and reduces the blast radius of compromise.

ZTNA plays a critical role too. It replaces broad VPN connectivity with tightly scoped, session-based access to specific resources. Access is verified at connection time and ends when the session ends. For many operators, replacing legacy VPNs is a practical step that delivers measurable risk reduction by limiting lateral movement.

### Micro segmentation for 5G and IoT

5G and large-scale IoT have changed the arithmetic of telecom security. The attack surface is no longer a limited set of systems; it now includes millions of distributed endpoints, virtualized functions, and workloads across multiple clouds. Micro segmentation addresses this scale by creating workload-specific security zones governed by strict policies. When a compromise occurs, segmentation prevents it from turning into service-wide disruption by containing the incident

### AI and ML for Real-Time Threat Detection

Data volumes in modern telecom networks exceed what human teams can monitor effectively. AI-powered detection becomes necessary to identify subtle deviations that traditional rule-based systems miss, such as unusual access timing, anomalous traffic spikes, and unexpected data movement patterns. ML adds the behavioral layer, learning normal baselines and triggering action when risk crosses thresholds. When paired with adaptive response, these systems enable rapid containment without waiting for manual triage.

## Overcoming Legacy and Operational Barriers

Zero Trust isn't just a technology problem; it requires addressing legacy practices. Often, enterprises are contending with decades of infrastructure built on a single, flawed premise: once access is granted, it is implicitly trusted. This outdated assumption is still hard-coded into telecom environments, creating a fundamental barrier to modern security enforcement.

Moreover, in telecom, tearing everything out is not a strategy. The workable path is protective layering: wrapping legacy systems with secure access gateways and enforcing authentication, session controls, and monitoring at the boundary, without disrupting operations. As a result, each added layer increases security coverage without risking uptime.

Consistency in implementation across regions, vendors, and inherited systems is as important to governance as it is to engineering. Leadership must own Zero Trust not only in strategy but also in funding, accountability, and operating mechanisms. Without this approach, Zero Trust becomes fragmented along organizational seams even when technology is in place.

On the performance front, security concerns are also addressable when verification is engineered intelligently. Validation can be pushed closer to the edge, and analytics can calibrate scrutiny by risk: familiar, low-risk patterns pass with minimal friction, while anomalies trigger stricter checks. Security and performance do not have to be trade-offs; when approached diligently, they can be designed together.

Finally, bridging IT and OT security operations is essential. Many OT systems prioritize reliability over adaptive authentication, and their behavior differs fundamentally from that of typical IT assets. When connected without unified control, implicit OT trust extends into risky IT pathways, increasing exposure. Closing this gap requires unified governance, shared visibility, and coordinated response across both domains, supported by a security operations center (SOC) capable of analyzing cross-domain signals to detect multi-stage attacks.

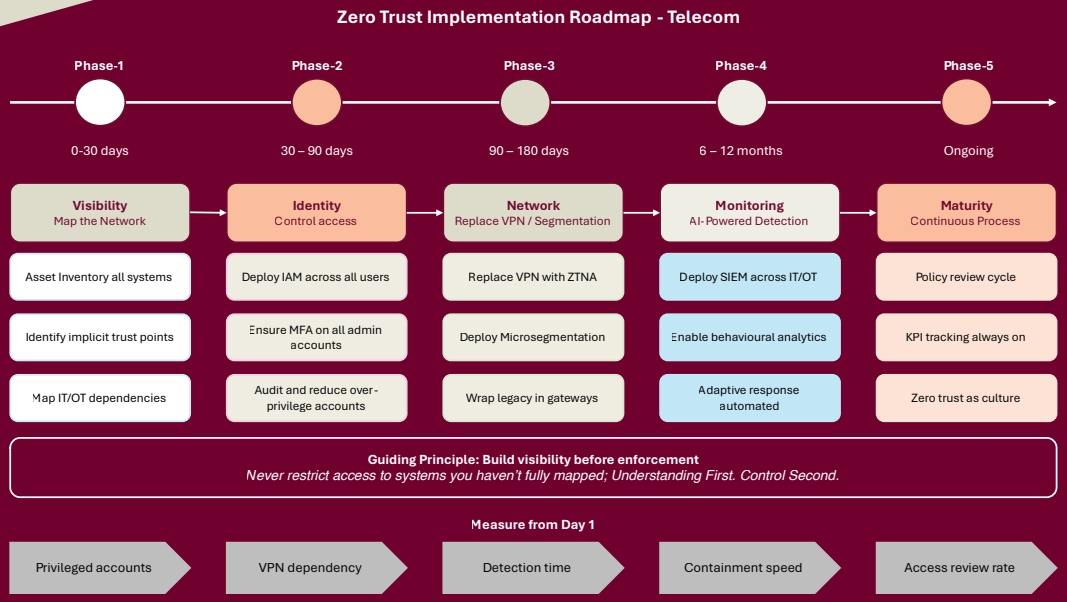



*Figure 2: Zero Trust Implementation Roadmap, From Visibility and Mapping to Ongoing Maturity*

## KPI Panel: Metrics to Prove Progress in the First 180 Days

A Zero Trust program that cannot demonstrate measurable progress is of no value. The following metrics, tracked from day one, give leadership a clear picture of outcomes in the first six months.

- **Reduction in Overprivileged Accounts:** Identify and deactivate dormant accounts or those with excessive access to shrink the blast radius quickly.
- **Decrease in VPN Dependency:** Track the shift from VPN to ZTNA to reduce broad network exposure
- **Mean Time to Detect (MTTD):** If detection is not improving, visibility and monitoring are not functioning as intended. Therefore, focus actively on improving detection quality.
- **Access Review Closure Rate:** Missed reviews are where permission drift begins; consistency in oversight brings back control and equips security teams with visibility.
- **Incident Containment Time:** Faster containment means reduced impact, both operationally and financially. Hence, reduce containment time for active incidents.

## Conclusion

Zero Trust is not a far-fetched concept. It is already here and is the only security model that structurally fits the telecom landscape operators manage today. For years, Zero Trust has been treated as a product to deploy rather than a practice to sustain. The old model of defending the edge and trusting traditional security measures is ineffective in the wake of 5G, IoT, cloud services, and global interconnectivity.

To thrive in this environment, organizations need to actually operationalize Zero Trust rather than treating it as a compliance checkbox. Going forward, Zero Trust must be built as an ecosystem: identity-driven access control anchored by IAM and MFA; ZTNA replacing broad VPN connectivity; microsegmentation that actively contains damage; and AI-powered monitoring that detects and responds in real time. Trust, on the other hand, can't be assumed anymore. It must be earned, every time, by everyone, across every connection. This approach is not a policy preference. It is the only realistic foundation for telecom security in the decade ahead.

## About the Author

### Ashish Mishra

**Group Manager - Service Delivery, CSRM, Tech Mahindra**

Ashish Mishra is a seasoned IT professional and author with over 20 years of experience in the industry. He has a strong grasp and command of the IT (Information Technology), IS (Information Security), and Cyber Security domains. Ashish is also experienced in managing large IT and IS operations, strategy building, transformation journeys, project and program management, and service delivery. His expertise includes Public Cloud, Private Cloud, Cloud Security, Network Security, SASE, and Zero Trust.

With the thought process of 'continuous learning is the key to success,' he has obtained more than 150 professional certifications across various technologies and platforms related to public and private cloud, cloud security, information security, cybersecurity, compliance, infrastructure management, leadership, project management, and many more.

## End Notes:

1. Australian Signals Directorate's Australian Cyber Security Center. (2025, August 28). Countering Chinese state-sponsored actors' compromise of networks worldwide to feed the global espionage system.

https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/countering-chinese-state-sponsored-actors-compromise-of-networks-worldwide-to-feed-global-espionage-system

## About **Tech Mahindra**

Tech Mahindra (NSE: TECHM) offers technology consulting and digital solutions to global enterprises across industries, enabling transformative scale at unparalleled speed. With 147,000+ professionals across 90+ countries helping 1100+ clients, Tech Mahindra provides a full spectrum of services including consulting, information technology, enterprise applications, business process services, engineering services, network services, customer experience & design, AI & analytics, and cloud & infrastructure services. It is the first Indian company in the world to have been awarded the Sustainable Markets Initiative's Terra Carta Seal, which recognizes global companies that are actively leading the charge to create a climate and nature-positive future. Tech Mahindra is part of the Mahindra Group, founded in 1945, one of the largest and most admired multinational federation of companies. For more information on how TechM can partner with you to meet your Scale at Speed™ imperatives, please visit https://www.techmahindra.com/.

TECH mahindra

www.techmahindra.com
www.linkedin.com/company/tech-mahindra
www.x.com/tech_mahindra