International Journal of Computer Techniques–IJCT Volume 12 Issue 6, November 2025
Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

The Zero Trust Imperative for 5G and Cloud-Native Telecom Operators

Krishnaveni Palanivelu

krishnavenipalanivelu@gmail.com

Abstract

The evolution of telecommunications networks from hardware-driven infrastructure to cloud- native architectures has fundamentally changed the security landscape. Traditional perimeter- based defense models no longer suffice in a 5G and Telco Cloud environment where workloads, APIs, and network functions are distributed across physical, virtual, and cloud-native domains.

Zero Trust Architecture (ZTA) — based on the principle of "never trust, always verify" — has emerged as a foundational approach for securing modern telco networks. This paper explores the key concepts of Zero Trust in the context of 5G and Telco Cloud, outlines common implementation challenges, and provides practical strategies for integrating ZTA into existing OpenShift- or Kubernetes-based environments. Real-world examples from network slicing, CNF deployment, and multi-cluster orchestration illustrate how operators can build a resilient, identity-driven, and continuously verified telco security posture.

1. Introduction

Telecommunications networks have traditionally relied on perimeter security, assuming that entities inside the network are trustworthy. This model worked reasonably well for legacy systems, where the infrastructure was static and tightly controlled.

However, the introduction of 5G, Network Function Virtualization (NFV), and Cloud-Native Network Functions (CNFs) has dissolved this perimeter. Telco infrastructure is now composed of:

- Multi-vendor CNFs running in OpenShift or Kubernetes clusters
- Dynamic APIs connecting core, transport, and edge networks
- Distributed edge nodes and partner integrations

Each of these elements increases the attack surface, making implicit trust dangerous. Zero Trust Architecture provides a framework to authenticate, authorize, and continuously validate every entity — human, device, or workload — before granting access or connectivity.

2. What is Zero Trust Architecture (ZTA)?

Zero Trust is not a product, but a security philosophy. It assumes that threats exist both inside and outside the network and that no communication or transaction should be trusted by default.

According to NIST SP 800-207, the core principles of Zero Trust are:

1. All entities are untrusted by default.
2. Access is granted based on identity and policy, with the least privilege possible.

3. Continuous monitoring and verification are mandatory.
4. Microsegmentation ensures that lateral movement is restricted.
5. Automation and policy enforcement are integrated across systems.

When adapted to the telco ecosystem, ZTA extends beyond IT boundaries — it governs network slices, control planes, management APIs, CNFs, and inter-cluster communication.

---

3. Why Telco Networks Need Zero Trust

3.1 Expanded Attack Surface

5G introduces a distributed architecture with multiple trust boundaries — from the core network to the edge.

- Network slicing allows multiple tenants and applications to coexist, increasing the risk of cross-slice attacks.
- APIs used for orchestration and service exposure (e.g., NEF, NSSF) are accessible externally.
- Multi-vendor CNFs introduce software supply chain vulnerabilities.

3.2 Dynamic and Ephemeral Components

In cloud-native environments, workloads are ephemeral — pods and containers appear, disappear, and scale dynamically. Traditional IP-based security controls can't track these entities effectively.

3.3 Supply Chain Risks

Telcos increasingly rely on open-source software, external vendors, and CI/CD pipelines. Without verification, malicious or compromised container images can infiltrate production clusters.

3.4 Regulatory Pressure

Regulatory frameworks like 3GPP SA3, GSMA NESAS, and NIST Zero Trust guidelines require stronger isolation, traceability, and encryption across all network planes.

---

4. Key Components of Zero Trust in Telco Cloud

Implementing Zero Trust requires adapting its pillars to the telco ecosystem.

ZTA Pillar	Telco Adaptation
Identity and Access Management (IAM)	Identity-based access for users, APIs, and workloads. Integration with LDAP, OAuth, or OpenID for operators and CNFs.
Network Segmentation	Use of microsegmentation at Layer 3–7 via Kubernetes NetworkPolicies, SDN, or service mesh.
Continuous Monitoring	Centralized logging and real-time behavior analytics using

	Prometheus, Grafana, and AI-based anomaly detection.
Policy Enforcement	Use of Open Policy Agent (OPA), Kyverno, or admission controllers to enforce runtime compliance.
Encryption and Trust Anchors	TLS for all intra-cluster and inter-cluster communication; use of TPM and Secure Boot for hardware trust.

5. Practical Challenges and Real-World Scenarios

5.1 Challenge 1: Legacy Integration

Scenario:
A telco operator runs a hybrid setup — part of the 5G Core on an OpenShift cluster, and legacy EPC functions on bare metal. Legacy nodes lack identity-based authentication, depending only on IP whitelisting.

Problem:
This creates "blind trust" zones where compromised systems can access control-plane interfaces.

Solution:
Implement an identity proxy using API gateways or service mesh sidecars that enforce mTLS (mutual TLS) and JWT-based service identity even for legacy components. Gradually phase out IP-based ACLs.

5.2 Challenge 2: Multi-Cluster Communication in Hub-Spoke Architectures

Scenario:
A telco cloud uses a central hub cluster for orchestration and multiple edge clusters for CNF workloads. These clusters communicate via APIs over WAN links.

Problem:
If the connection between clusters isn't authenticated or encrypted, an attacker could impersonate an API call or inject malicious payloads.

Solution:

- Establish cluster federation using OpenShift ACM (Advanced Cluster Management) or similar tools with mutual certificate-based trust.
- Use service mesh federation (e.g., Istio or OpenShift Service Mesh) for secure service- to-service communication with automatic key rotation.

5.3 Challenge 3: Insecure CNF Supply Chain

Scenario:
A CNF vendor delivers Docker images via an internal registry. There's no validation of image integrity or content.

Problem:
Malicious or outdated images can be introduced into production, leading to runtime exploits.

Solution:

- Implement image signing (using Sigstore, Cosign, or Red Hat Quay) and enforce verification during deployment.
- Integrate software composition analysis (SCA) and vulnerability scanning in CI/CD pipelines.

- Use Kubernetes admission controllers to reject unsigned or unverified images.

5.4 Challenge 4: Lateral Movement Between CNFs

Scenario:
Two CNFs share the same OpenShift namespace and use the same default network.

Problem:
A compromise in one CNF can be used to probe or exploit another, due to flat network connectivity.

Solution:

- Enforce namespace-level isolation with NetworkPolicies.
- Use Service Mesh Authorization Policies to restrict traffic between services.
- Adopt RBAC (Role-Based Access Control) to isolate service accounts and API access.

5.5 Challenge 5: Human Access and Privilege Escalation

Scenario:
Operational users access both management (OneView, SR Linux) and control-plane systems with shared credentials.

Problem:
If one credential is compromised, it can be reused across systems.

Solution:

- Centralize authentication using LDAP/Active Directory + SSO (Keycloak, RHSSO).
- Apply least privilege access (e.g., "break-glass" emergency accounts).
- Enable MFA (Multi-Factor Authentication) and session monitoring for privileged operations.
- Audit all changes using SIEM integration.

---

6. Implementation Framework for Zero Trust in Telco Cloud

Step 1: Identity Foundation

- Define identities for all entities — users, CNFs, APIs, and infrastructure components.
- Implement strong authentication mechanisms using certificates and tokens.
- Manage lifecycle via IAM systems (Keycloak, RHSSO).

Step 2: Network Microsegmentation

- Define trust boundaries: control plane, data plane, and management plane.
- Apply NetworkPolicies in OpenShift for each CNF namespace.
- Use service mesh to implement mTLS between services.

- Separate customer-facing CNFs from internal components via VLANs or SDN overlays.

Step 3: Continuous Verification

- Monitor every access event and flow using telemetry (Prometheus, Loki, ELK).
- Implement behavioral anomaly detection using AI models trained on normal traffic baselines.
- Feed alerts into Security Orchestration, Automation, and Response (SOAR) tools.

Step 4: Policy Enforcement and Automation

- Apply Open Policy Agent (OPA) or Kyverno for runtime policy checks.
- Example policy: block deployment of any container image not signed by a trusted key.
- Automate compliance audits via Ansible + OpenSCAP.

Step 5: Data Protection

- Encrypt all communication (TLS 1.3+).
- Use etcd encryption at rest in OpenShift.
- Implement secure key management (Vault, KMS).
- Protect backup and DR data with integrity verification.

---

7. Real-World Example: Zero Trust in a 5G Core Deployment

Architecture Overview

A Tier-1 telco deployed its 5G Core (AMF, SMF, UPF, PCF) on OpenShift across two clusters — control plane (hub) and user plane (edge).

Challenges

- Mixed vendor CNFs with different security maturity levels
- Legacy NMS systems without identity-based access
- API communication across WAN links

Implementation

1. **Identity and Certificates:**
   Each CNF received an x.509 certificate issued by an internal PKI, managed via OpenShift cert-manager.
2. **Microsegmentation:**
   Each CNF namespace implemented network policies limiting traffic only to approved services (e.g., AMF ↔ SMF).
3. **Service Mesh:**
   Deployed Istio for encrypted service-to-service communication using mTLS.

4. **Continuous Monitoring:**
   Integrated Prometheus and Grafana with SIEM (Splunk) for anomaly detection.
5. **Policy Enforcement:**
   Admission controller rejected unsigned CNF images.
6. **Human Access Control:**
   All administrative access via Keycloak with MFA.

Outcome

- Reduced blast radius from potential CNF compromise
- Unified visibility across clusters
- Compliance with GSMA NESAS security baseline

---

8. Measuring Success: KPIs for Zero Trust Adoption

Metric	Description	Goal
Authentication coverage	% of services using mTLS or token-based auth	>95%
Segmentation coverage	% of namespaces with NetworkPolicies	>90%
Image verification rate	% of workloads using signed images	100%
Privilege access reduction	# of shared credentials eliminated	Target: 0
Detection-to-response time	Mean time to detect/respond (MTTD/MTTR)	<5 min

---

G. Overcoming Common Pitfalls

Pitfall	Recommendation
Treating Zero Trust as a single product	Design a framework with multiple integrated controls
Over-segmentation causing performance	Balance security with network throughput; validate issues latency
Manual certificate management	Automate via cert-manager or Vault
Ignoring runtime visibility	Deploy continuous security monitoring with anomaly alerts
Lack of executive sponsorship	Tie Zero Trust to compliance and business risk reduction

---

10. Future Outlook

As telco networks evolve toward 6G, AI-driven orchestration, and quantum-resilient encryption, Zero Trust will become the default design principle rather than an add-on.
Future systems will leverage:

- AI-based identity scoring for adaptive access control
- Confidential computing for workload isolation
- Post-quantum encryption for long-term data integrity

The journey to Zero Trust is continuous, but early adopters are already achieving measurable security and operational benefits.

---

11. Conclusion

Zero Trust is not a one-time deployment but a **strategic transformation** in how telco networks are designed, deployed, and operated.
By eliminating implicit trust, enforcing strong identity verification, and continuously monitoring every connection, operators can secure dynamic, distributed 5G and Telco Cloud environments against evolving threats.

As telcos embrace cloud-native architectures, Zero Trust offers a **unified, scalable, and standards-aligned approach** to protect their most critical infrastructure — ensuring resilience, compliance, and customer trust.

References

1. NIST Special Publication 800-207 — *Zero Trust Architecture*, 2020.
2. 3GPP TS 33.501 — *Security architecture and procedures for 5G system*, Release 17.
3. GSMA NESAS — *Network Equipment Security Assurance Scheme*, 2023.
4. Red Hat — *Securing Cloud-Native 5G Networks*, Technical Whitepaper, 2024.
5. ETSI NFV-SEC 003 — *Security; Security and Trust Guidance for NFV Architectural Framework*, 2022.
6. CNCF — *Cloud Native Security Whitepaper*, 2023.
7. Gartner — *Zero Trust Security for 5G and Edge Computing*, 2024.
