

5G & TELECOM NETWORK SECURITY.



5G's shared, software-defined core turns network slicing and inter-carrier signaling into the new attack surface — **isolation between slices** and **trust between carriers must be continuously verified, not just assumed by design.**

- SIGNALING INTERCONNECT SECURITY
- NETWORK SLICE ISOLATION
- SUBSCRIBER IDENTITY PROTECTION
- OPEN RAN SUPPLY CHAIN

01 THE MECHANISM

Signaling Protocol Exposure

SS7 and Diameter, the protocols carrying interconnect signaling between carriers, were built for a small, closed club of trusted telcos — **they barely authenticate which carrier a message claims to come from**, letting a connected party query location or intercept SMS.

Network Slice Isolation Failure

5G's core innovation — separate logical networks for IoT, enterprise, and consumer traffic on one shared virtualized infrastructure — means **isolation is enforced by configuration, not physical separation**, and a gap there lets traffic cross between slices.

Disaggregated RAN Supply Chain

Open RAN splits radio access components into open interfaces across multiple vendors instead of one vendor's closed stack. **Every new open interface is a boundary needing its own security review**, widening the equipment trust surface.

02 THE FLOW

The Segmented Carrier Network

CONTAINED

- Interconnect signaling (SS7/Diameter/5G HTTP-2) is filtered at the network edge, with firewalls validating message origin against a subscriber's actual serving network and session state.
- Network slices for IoT, enterprise, and consumer traffic run under **resource and traffic isolation verified at the orchestration layer**, not just declared in a slice template.
- An attacker who compromises one roaming partner's link or one slice's workload is contained to that scope — **unable to reach subscriber data or other slices.**

The Trust-by-Default Network

EXPOSED

- Interconnect messages from any peer carrier are accepted as though every roaming partner is equally trustworthy, since SS7/Diameter assumes a closed circle of carriers.
- Slices share the same virtualized infrastructure without enforced isolation, so **a compromised workload in one slice can reach another** through a shared hypervisor or misconfigured API.
- An attacker with basic interconnect access can **track subscriber location, intercept SMS passcodes, or pivot across slices** the network never expected to be reachable from each other.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Signaling Firewalling	Filters SS7, Diameter, and 5G HTTP/2 interconnect traffic at network borders, rejecting messages inconsistent with a subscriber's known location or session state.
Network Slice Isolation	Enforces resource, traffic, and management-plane separation between slices sharing the same virtualized 5G core, verified at the orchestrator rather than assumed from configuration.
Subscriber Identity Protection	Encrypts the permanent subscriber identifier (SUPI) into a concealed identifier (SUCI) before it leaves the device, closing the classic IMSI-catcher exposure for 5G-native connections.
RAN & Core Supply Chain Assurance	Validates the provenance and configuration of radio, edge, and core network functions across a multi-vendor Open RAN and cloud-native core.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Carrier-to-Carrier Trust Agreements Alone	No	Contractual trust between roaming partners doesn't stop a compromised or malicious partner network from sending valid-looking signaling traffic.
Perimeter Firewalling of the Core Only	No	Protects the core network boundary but leaves east-west traffic between slices and network functions unmonitored.
SUCI Identity Concealment Alone	No	Stops classic radio-layer IMSI catchers but does nothing against signaling-layer location tracking via SS7/Diameter, which never touches the radio identifier.
Vendor Security Self-Attestation	No	Vendor claims about equipment security aren't independently verified and miss vulnerabilities introduced after initial certification.
Signaling Firewalls + Slice Isolation Enforcement + Independent Equipment Assurance (NESAS)	Yes	Combines interconnect-layer, infrastructure-layer, and supply-chain-layer controls so no single failure exposes the whole network.

5G & TELECOM NETWORK SECURITY.

SEGMENT · VERIFY · CONTAIN

05 PROGRAM OPERATIONS

The interconnect trust model predates today's threat landscape. SS7 and Diameter were designed for a small, closed set of trusted carriers — not the hundreds of operators and resellers online now.

Network slicing is a logical boundary on shared physical infrastructure. Isolation must be continuously verified at the orchestration and hypervisor layer, not just declared in a template.

5G's cloud-native core inherits cloud-native risk. Containerized network functions and Kubernetes orchestration bring the same misconfiguration and lateral-movement exposure as any cloud workload.

Open RAN trades a single-vendor black box for a documented, multi-vendor attack surface. Every open interface between radio components is a boundary needing its own ongoing review.

06 CONTROL MAPPING

3GPP TS 33.501

The core 5G security architecture standard, defining SUPI/SUCI concealment, mutual authentication, and inter-network security requirements.

GSMA FS.11 / NESAS

Network Equipment Security Assurance Scheme — independent security testing and accreditation for telecom vendor equipment and development processes.

0-RAN ALLIANCE W611

Security specifications for disaggregated RAN, addressing the open interfaces between multi-vendor radio components.

CISA 5G SECURITY EVALUATION PROCESS

U.S. government framework for assessing 5G architecture risk across standards, supply chain, and deployment choices.

07 WHAT THIS DOES NOT SOLVE

Device & Endpoint Security

Network-layer controls don't protect a handset or IoT endpoint whose **own credentials or firmware** are already compromised.

Application-Layer Fraud

Encrypting signaling and isolating slices doesn't stop fraud carried out through **legitimate, already-authenticated application sessions**.

Legacy 2G/3G Fallback Exposure

Devices and networks that fall back to older generations for coverage **inherit those generations' weaker signaling and encryption**, regardless of how hardened the 5G core is.

Physical Site Security

Cell site and edge compute hardware theft or tampering sits **outside any protocol-level control** and needs its own physical security program.

08 MYTHS VS. REALITY

MYTH

"5G is inherently more secure than 4G, so legacy interconnect risks don't apply."

REALITY

Most live networks run 5G non-standalone on a 4G/LTE core, or interwork with 2G/3G for coverage — **the older signaling protocols' exposure carries forward** until standalone 5G fully replaces it.

MYTH

"SUCI encryption solves subscriber location tracking."

REALITY

SUCI protects the permanent identifier over the air, but **SS7 and Diameter signaling can still expose location** through interconnect-layer queries that never touch the radio identifier.

MYTH

"Network slices are as isolated as physically separate networks."

REALITY

Slices share the same underlying compute, storage, and transport — isolation is **enforced by configuration, not physics**, and a misconfiguration can bridge slices.

MYTH

"Open RAN is less secure than traditional single-vendor RAN by design."

REALITY

Disaggregation adds interfaces to secure, but it also **ends reliance on any one vendor's undisclosed internals** — the net effect depends on how well those interfaces are governed.

MYTH

"Telecom network security is the carrier's problem, not the enterprise's."

REALITY

Enterprises using private 5G, network slicing for OT/IoT, or SMS-based authentication **inherit the carrier's signaling and slice-isolation posture** as part of their own attack surface.

09 SPEAK THE PROGRAM — KEY TERMS

SS7 (SIGNaling SYStem NO. 7)

The legacy inter-carrier signaling protocol for call setup, SMS, and roaming — built on an **implicit trust model between carriers** with no message-origin authentication.

DIAMETER

The signaling protocol used in 4G/5G interconnect, replacing SS7's role for newer networks while **carrying forward much of the same inter-carrier trust assumption**.

SUPI / SUCI

SUPI is a subscriber's permanent identifier; SUCI is its **encrypted form transmitted over the air** in 5G, designed to defeat classic IMSI-catcher interception.

NETWORK SLICING

Running multiple logical, isolated networks — each tuned for a use case like IoT or enterprise — **on one shared physical 5G infrastructure**.

OPEN RAN (0-RAN)

An industry initiative to disaggregate radio access network components into **open, interoperable interfaces across multiple vendors**, rather than one vendor's proprietary stack.

IMSI CATCHER

A rogue base station that tricks nearby devices into connecting so it can **capture identifiers or intercept traffic**; largely mitigated for 5G-native connections by SUCI, but not for 2G/3G fallback.