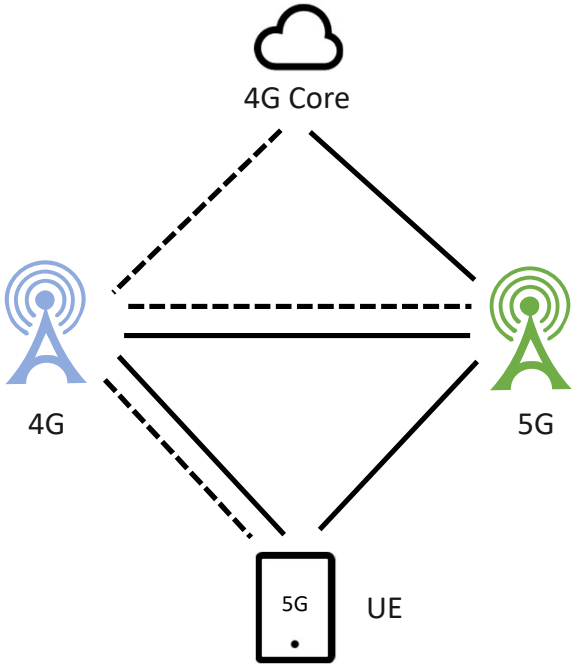
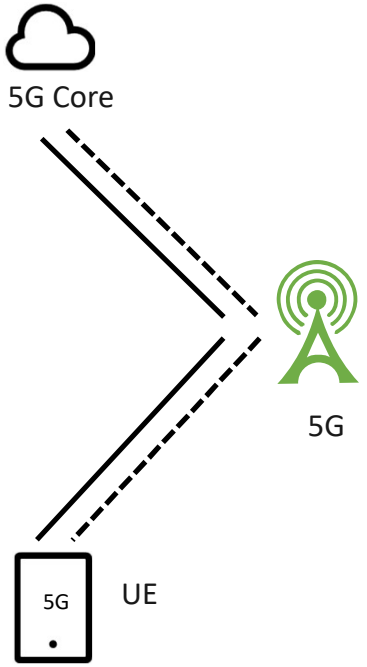
5G Networks and Security

5G | SA & NSA Architecture



NSA (*Non-Standalone*)

- Leverage existing 4G core network
- 5G Signaling dependency on 4G Anchor layer
- Dual data connectivity with 4G & 5G radio



SA (*Standalone*)

- New 5G core deployment
- No dependency on 4G N/w for signaling.
- Data Connectivity with single 5G radio

Signaling

Data Traffic

5G Network | Global landscape

Almost all Operators have launched 5G NSA First

243	41	4	8
Operators have launched 5G networks	Operators with 5G NSA & SA both	Operators Launched 5G SA Only	Operators Launched VoNR

Source GSA May 2023

5G SA Drivers in different Markets

- Greenfield Operators
- Limited SA deployment on a need basis
  - Enterprise Use cases
  - Sports Events

VoNR Challenges

- VoNR Performance not at par with VoLTE
- VONR required features and IRAT maturity
- Device ecosystem readiness

Key Area	NSA	SA
Global Adoption	>98%	<20%
Device Ecosystem	Wider & Matured	Emerging
Core Network	Use the existing 4G Core No complexities of 4G & 5G Core Interworking	Need new 5G core
Voice	No impact to existing Voice Experience	VONR - Emerging 4G Fallback - Higher Setup time
Coverage	Higher by Leveraging Dual Connectivity	Restricted to 5G Uplink Coverage Availability
Slicing	Possible in NSA with new features introduced by RAN, Core and Device Vendors	Possible

5G Security | Network & Architectural Evolution

Adoption of new technologies

Appliance to applications on standard OS , Cloud/Virtualization, Digitization , Automation ,Open network interfaces, Network Perimeters extension

Increased threat actors

Nation states, Hacktivists, Terrorists, Cyber Criminals, Insider Threats, Competition

Highly Sophisticated Attacks

Military-grade Malware, Refined Zero Day Attacks, Phishing Attacks, Exploits

G-Evolution

Closed to Open Network

2G – 4G – 5G

Continuous transformation in Networks

Increased threats landscape

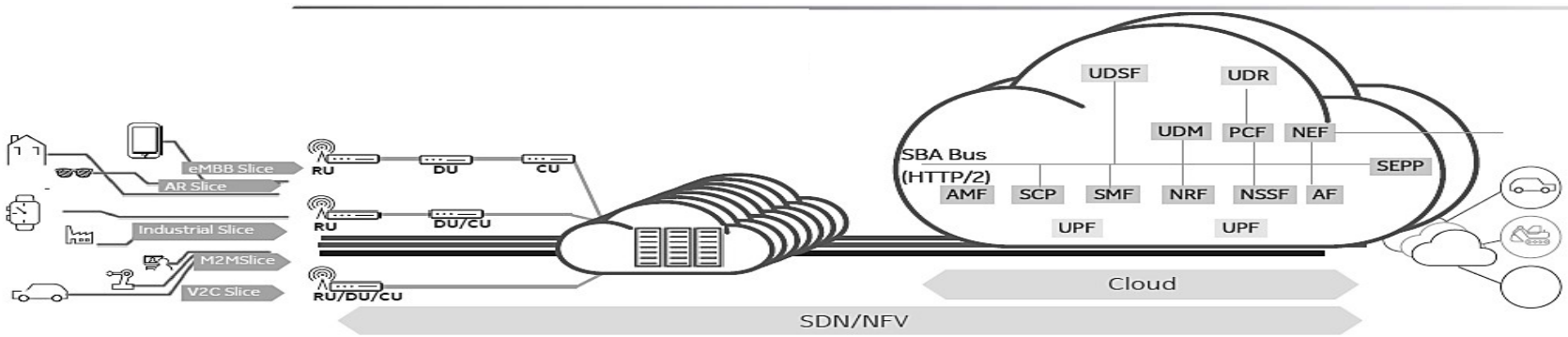
- Lack of real-time awareness
- IoT evolution increasing possibility and attack volumes of DDOS attack
- Consumer privacy protections against interception /misuse
- Regulatory requirements becoming more stringent with increased liabilities
- Thinning of Network perimeter
- Network Access to multiple stakeholders

Disaggregated, function-based, and cloud hosted mobile network

5G Network –Key Changes

- ✓Business Changes
- ✓Network Architecture Changes
- ✓Technology Changes

5G Network Threat Landscape



Air Interface	Internet	Roaming	EMS	Transport	Slicing	MEC	5GC	Cloudification
Theft/Tampering of user data	Lekage/temperin g of user data during transmission	Leakage/tamperi ng of data during transmission	Unauthorized operations by auauthorized users	Data Eavesdropping	Resource abuse among slices	Perimeter attcaks	Perimeter attcak	NFV threats
Fake BTS	Denying data services due to DDOS attack on internet	Exploitation of signalling connectivity - Cat1/2/3 messages	Malicious operations by authorized users	Data Tampering	Data leakage among slices	Attacking of MEC /UPF by malicious App	DDOS attacks	Container threats
Malicious Interference	Unauthorized access to exposed APIs						SBA threats	MANO threats
Deny user access -DDOS Attack								

Three Key Principles –Design of 5G Security

Zero trust

Strong Access control and refined authorization of telecom users and applications to reduce the attack surface .

In-depth Defense

Build four lines of defense to establish an all-round in-depth defense system for 5G networks which include:

- Deploy firewall for building network boundaries
- Configure service proxies at interconnects hiding network topology and enabling message filtering .
- Implement NE protection with TLS and Oauth 2.0 and
- Implement VM isolation and strong network segmentation for preventing lateral movements

Adaptive Security

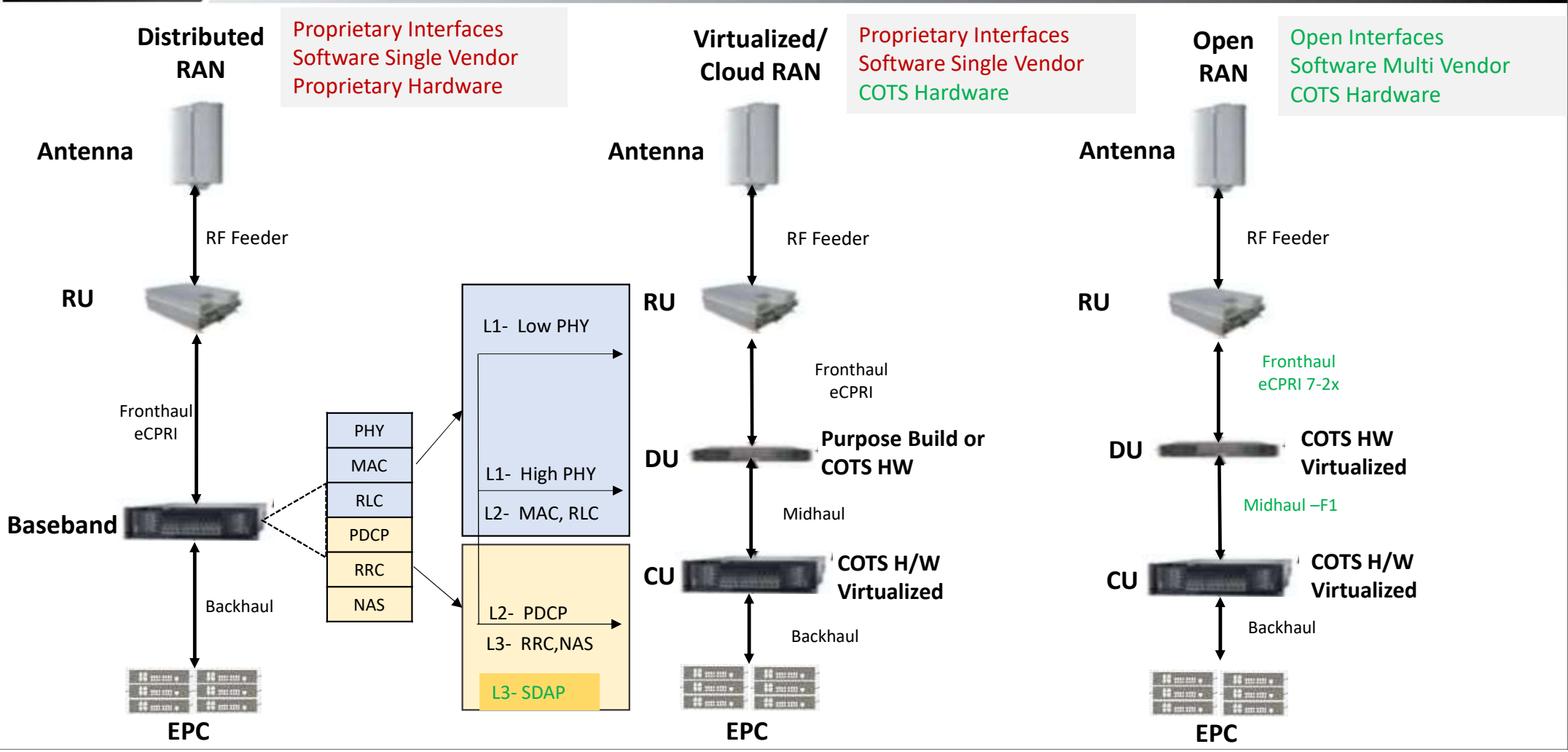
Develop dynamic security solutions that are continuously optimized in terms of

- Reducing risk exposure
- Reducing threat detection time
- Preventing damage from spreading
- Enabling quick recovery

5G Security | Security controls at Different layers

Orchestration	• Securing Orchestration management & interfaces, security Policy enforcement, and enhancing visibility within Orchestration and between Orchestration and Network components.
User	• Segmentation, User Access based on Zero Trust principles, DNS protection
Network	• Segmentation, Policy enforcement, Securing Network Interfaces, Security Cloud integration, and workloads, Securing peering & roaming interface.
Applications	• Securing 3rd Party Application Interfaces, DDoS Protection, Application Security, DevSecOps practices, Segmentation, Cloud application policy sync and enforcement, security API
VNFs and CNFs	• Securing VNF / CNF, Securing Software Lifecycle, Isolation between VNFs/CNFs, detecting malicious virtual functions and vulnerabilities
Infrastructure	• Hardening of NFVI, DDoS protection, securing -E-W traffic

RAN Architecture – DRAN/vRAN/ORAN



5G Security | 3GPP Security Enhancements in 5G

S. No.	3GPP release 15	3GPP release 16
1	**Subscriber authentication**: secure mutual authentication using 5G AKA, Home Control of authentication for roaming devices and non-SIM card-based authentication for IoT devices	Inter-PLMN User Plane Security (IPUPS): The role of the User-Plane Function (UPF) is expanded to include traffic protection with a "common firewall" between two roaming PLMNs.
2	**Subscriber privacy**: Stronger False Base Station (FBS) protection and SUPI/SUCI for encrypted long-term subscriber identifiers.	Full-rate User Plane Integrity Protection
3	**Secure service-based architecture (SBA)**: TLS and OAuth 2.0 on all mandatory functions	Network Slice Specific Authentication and Authorization (NSSAA): provides separate authentication and authorization per network slice.
4	**Secure roaming interconnects**: introduction of the Security Edge Protection Proxy (SEPP) at the application layer	Non-Public Networks (NPN): 5G Private networks to provide security and privacy on dedicated resources that are independently managed.
5		Use case specific security enhancements for cellular IoT and URLLC services.

5G Security | Summary

- Build 5G networks with a ZTA, in-depth defense and adaptive security to protect from both internal and external threats.
- Implementation of security controls at different layers of overall 5G Network and Services Ecosystem
- Use industry approved, supported, secure and current versions of APIs, protocols, and cipher suites.
- Ensure third party vendor security by implementing Supply Chain Risk security controls include Third-Party Risk Management (TPRM) programs which includes:
  - ✓ Clear visibility of the full supply chain including global partners and upstream suppliers
  - ✓ Institute Software Bill of Materials (SBOM)
  - ✓ Implement comprehensive test, metrics, and audit processes.
- Ensure OEMs, including Open RAN suppliers implement a shift-left philosophy using a Secure Product Life Cycle, CICD and DevSecOps
- Implement mature GRC framework and conduct regular risk assessment –internal and External.

Thank you