
SCTE®
CABLE-TEC EXPO®
FAST FORWARD 2021
ATLANTA, GA
OCTOBER 11-14
SCTE
a subsidiary of CableLabs®
UNLEASH THE POWER OF LIMITLESS CONNECTIVITY
2021 Fall Technical Forum
SCTE® • NCTA • CABLELABS®

SCTE
a subsidiary of CableLabs

Security & Privacy

5G Security Challenges & Protection Framework

Vasu Dalal

NOKIA

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

SCTE CABLE-TEC EXPO FAST FORWARD 2021

VIRTUAL EXPERIENCE
OCTOBER 11-14

Security in 5G: Key Aspects

Stringent requirements & Scale

"Physically, low-cost, short range, billions of small-cell antennas deployed throughout urban areas become new hard targets" – Brookings Institute

"The number of cellular IoT connections is expected to increase at an annual growth rate of 27 percent, reaching 4.1 billion in 2024." – CSO Magazine

"The threat model for identifying suspicious activity in the context of a human subscriber will not work for IoT devices, which are the majority of 5G users" - GSMA

"In order to meet the challenges of billions of connected devices, gigabit connection speeds, and ultralow latencies service providers must now rapidly increase edge network capacity" – CSO Magazine

Multi-vendor, Diversity & Complexity

- *New 5G use cases*
  - *Autonomous vehicles*
  - *Smart homes (Gaming, IOT, …)*
  - *Network slicing (5G sliced FWA, Private LTE)*
  - *SDN & NFV*

"The network has moved away from centralized, hardware-based switching to distributed, software-defined digital routing" – Brookings Institute

"…Volumetric DDoS attacks, signaling protocol-specific hacks, advanced persistent threats, lateral propagation, web application layer vulnerabilities, API security, and more" – CSO Magazine

"An increased exposure to attacks and more potential entry points for attackers" – EU NIS Group

"As SDN and NFV are implemented for network slicing in 5G, administration will become even more difficult" – GSMA

"Distributed edge opens up new attack surfaces. Network slicing and virtualization bring new risks" - Infradata

People, Processes & Regulation

"One out of every three successful attacks on 4G networks was resulted from incorrect configuration of equipment" – GSMA

"The 5G cyber realm needs to adopt leading indicator methodology to communicate cyber-preparedness" – Brookings Institute

"…industry-developed best practices are a step in the right direction, they are only as strong as the weakest link in the industry" - EU NIS Group

"…unfilled cybersecurity jobs is expected to grow by 350 percent, from one million positions in 2013 to 3.5 million in 2021" – MIT Technology Review

"…GDPR fines jump 39% to $332 million in 2020" – DLA Piper

5G Security & Potential Threats

UE

The number and types of UE´s are rapidly increasing

5G Radio

5G RAN introduces distributed RAN, CloudRAN and ORAN

Transport & Network

distributed computing power closer to the UE and more locations with specific security demand

5G Core & Cloud

5G with many firsts like CUPS, SBA, open API´s, containers and Eco-Systems (NEF)

THREATS

- UE compromised
- Signaling storms
- Malicious SW
- Bot hijacking
- IMSI catching

- Man-in-the-middle attack
- Configuration hacks
- IP-Spoofing
- Scanning attacks

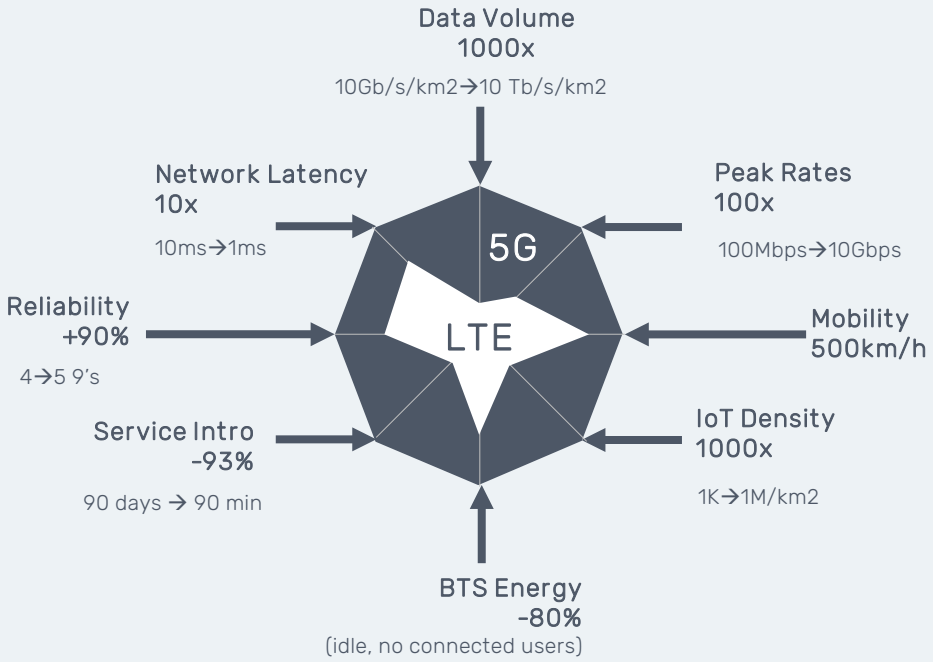
Distributed architecture raises number of entry point!
- Hijacking attacks
- TCP level attacks

Service based architecture & slice resource sharing increases security complexity!
- DoS attack on signaling plane
- Side Channel Attacks
- Saturation attacks
- User identity theft
- Active/passive eavesdropping
- Capability exposure API attack

Stringent requirements

Security implications

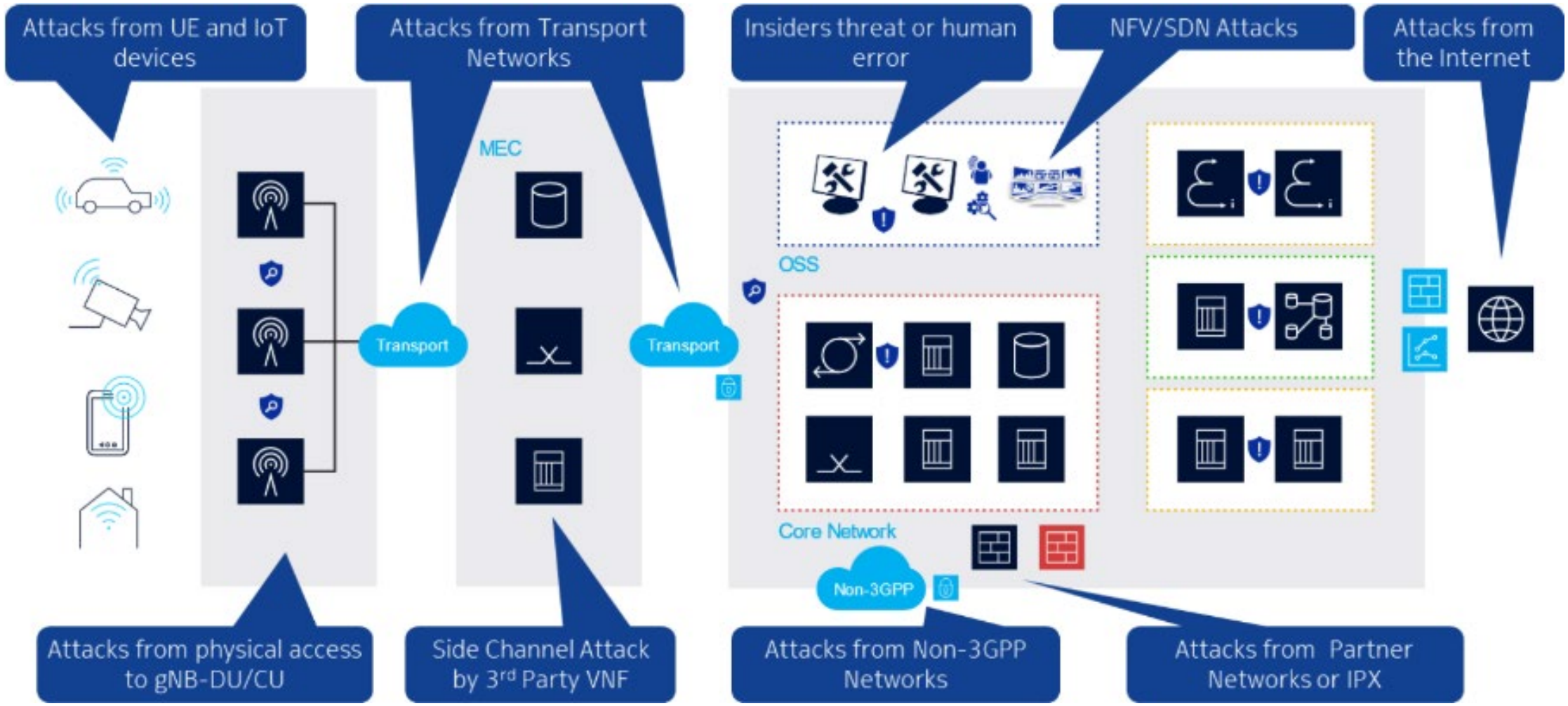
	Use case	DL	UL	Network Latency	Reliability	Cost Sensitivity	Security
Consumers	Mobile Broadband	100-300M	10-50M	15-25ms	Medium	Medium	Medium
	Fixed Wireless Access	1-5G	100-200M	1-20ms	High	High	Medium
	Event experience	1-100M	1-5G	1-5ms	Medium	Medium	Medium
	In-vehicle Infotainment	5-100M	1k-1M	1-20ms	Medium	Medium	Medium
Industries	Critical automation	1M	1-10M	1-5ms	Very high	Low	Very High
	Tele-operation	1M	1-10M	1-25ms	Very high	Low	Very-High
	Highly interactive AR	5-100M	1-100M	1-10ms	High	Medium	High
	Mass sensor arrays	1k-1M	1k-1M	200-500ms	Low	Very High	Medium-High



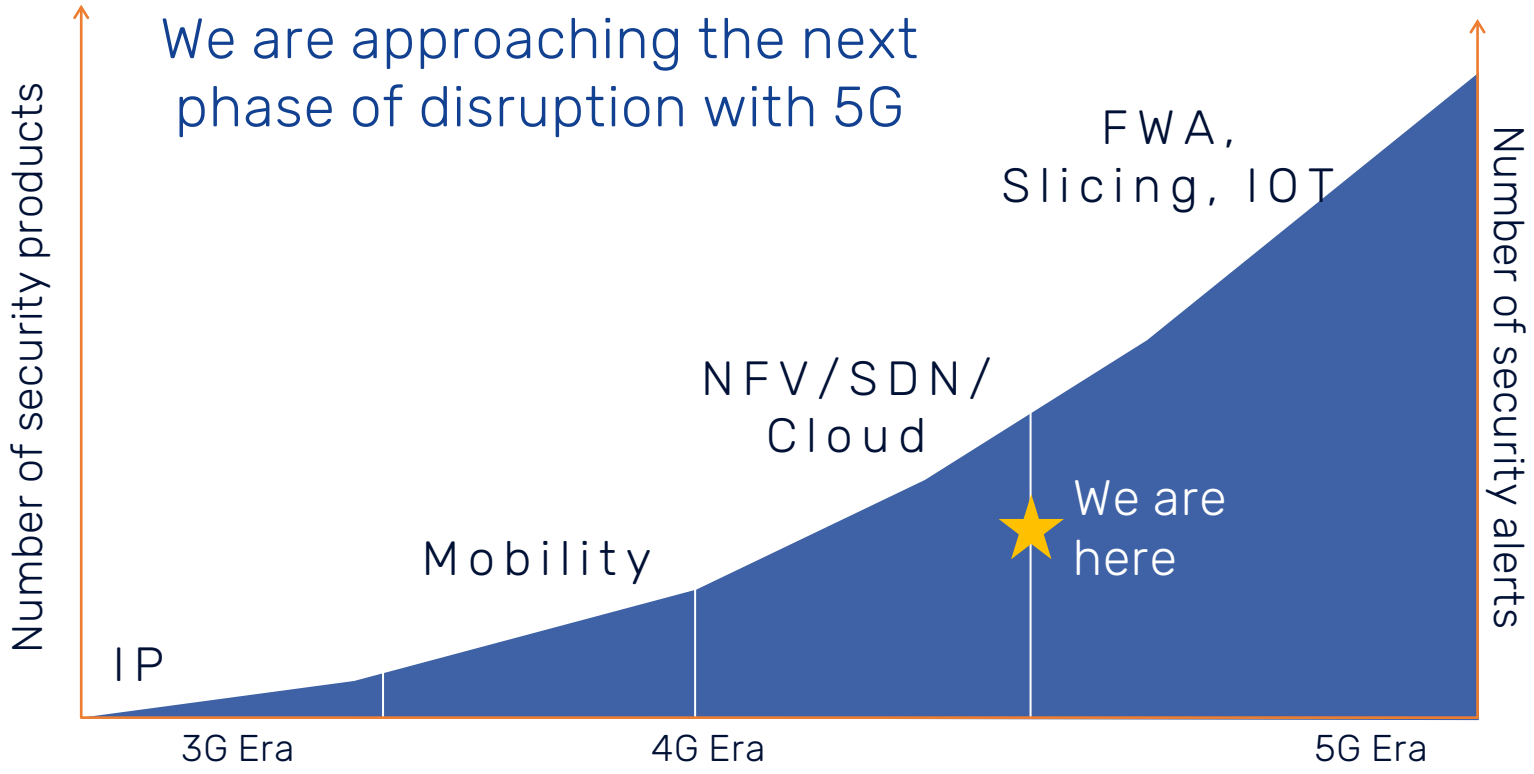
Scale challenges in a 5G network – at a glance

	Users & Endpoints	Radio & Transport	Network, Core & Edge	Cloud	People, Processes & Regulations
Services & Use cases	*Smart home (Gaming)* *Smart home (slicing)*	*Wi-Fi* *FWA*	*5G data* *5G voice*	*Autonomous vehicles* *IOT* *Private wireless* *CBRS* *APIs*	*Cloud* *Distributed* *Regulations*
Now	Subscribers & Devices 10s of millions	Radios & Base stations Cellular eNodeB millions	Bandwidth 10s of Mbps	Network & Servers *Centralized* thousands	Complexity Manual Compliance (Limited)
	100X-1000X	1000X	10X-100X	10X-100X	many X
Future	10s of billions	billions Cellular gNodeB	100 Mbps – 10 Gbps	100s of thousands *Distributed* *(Edge, SDN, & NFV)*	Automated, AI/ML Compliance (GDPR, CA Consumer Privacy Act, Clean Network (US Dept. of State), …

Multi-vendor, Diversity & Complexity



People challenges in a 5G network - Volume & Scale

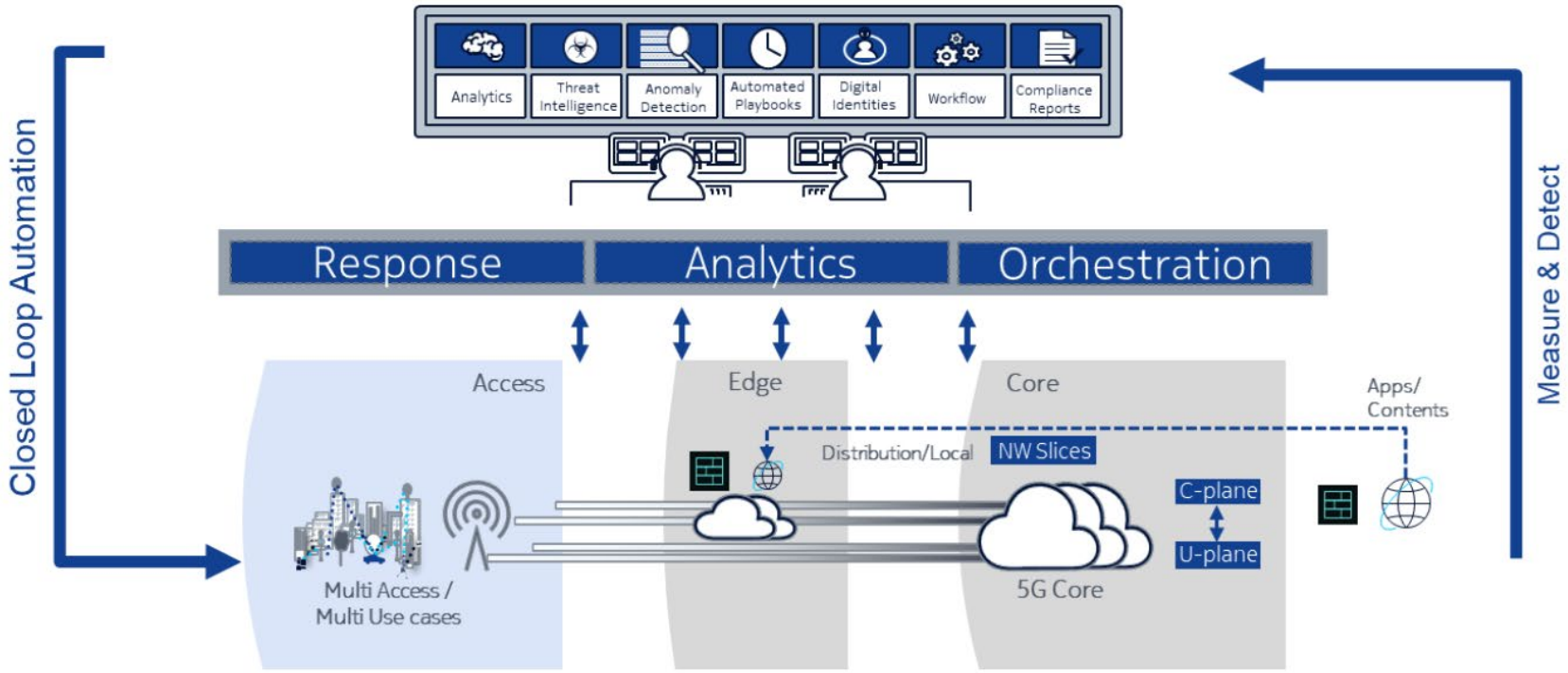


Sources: Ponemon, Cisco, HPE, ESG

- Security becomes unmanageable by conventional means
- Security Operations Must become Adaptive & Automated
- Only 56% of alerts are investigated
- 72% of investigated alerts are false
- 49% of legitimate alerts are not remediated
- 53% of time is spent on detection

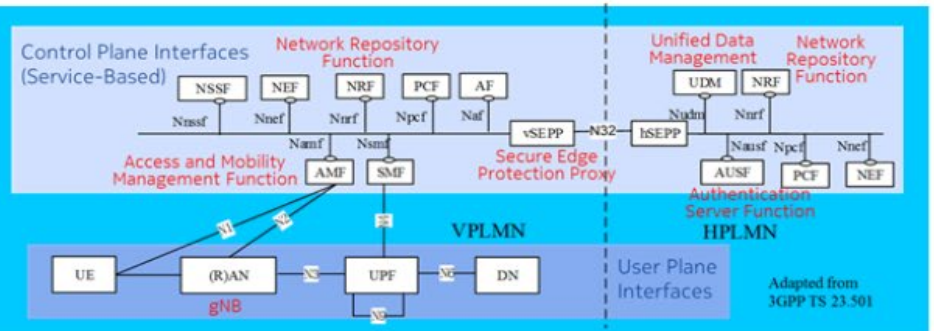
Security Orchestration, Automation & Response (SOAR)

5G E2E Network Security – Security Orchestration, Automation & Response



- Centralized security command-and-control structure with a fusion of threat intelligence, analytics, machine learning & automated response
- Automated access governance and management
- Analytics and machine learning (ML)
- Security operations workflow automation and orchestration: awareness of business processes, regulations, customer-specific policies & access management/governance

Defense in Depth

Security architecture specified by Standards (e.g. 3GPP)	Nokia Products are 3GPP compliant and implement the 3GPP security architecture. 	3GPP specified
Network element security measures	**Design for Security (DFSEC)** : *VNF Hardening, OS Hardening, Hypervisor Hardening, Secure Boot, Root of Trust, Software Integrity Protection, Secure Key & file storage, Memory Protection, Account Management*	Vendor & Network dependent
Network security unspecified by Standards	① **Radio Transport Security** ② **Cloud Infrastructure Security** ③ **Packet Core Security** ④ **IoT Security** ⑤ **Security Operation** ⑥ **Security Services**: *Security Risk Assessment, Security Consulting, Security Architecture, Managed Security Operation*	Vendor & Operator dependent

How should operators address each security domain

Proposed E2E Approach to 5G Security

1 Radio & Transport

- Unified cryptographic authentication
- IPsec encryption of traffic in Midhaul
- Authentication of all NEs w/ digital certs
- Automated Cert. Life Cycle Mgt
- C-Plane & U-Plane Confidentiality & Integrity protection
- M-Plane encryption with TLS or IPSec

2 Network & Cloud

- Multi-layer cloud security
- Secure NFVI
- Micro-segmentation
- Virtualized Security
- Physical Security Components
- Security Management
- Cloud Security Orchestration

3 Devices & UEs

- Manage endpoints to establish trust – 2 way authentication;
- Analyze traffic pattern and detect anomalies using AI analytics
- Endpoint profiling - alert and mitigate any deviation e.g. send SMS, firmware update or traffic throttling

4 Security Operations

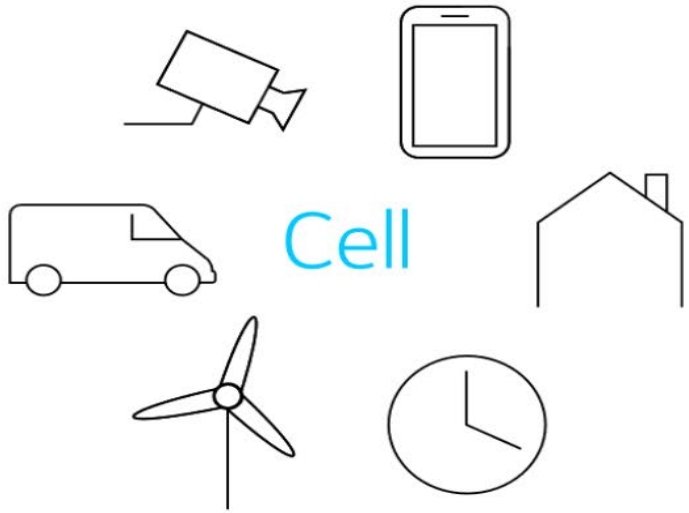
- Automated holistic security orchestration and management will be crucial in 5G networks
- E2E security needs will have to be managed through a central point of control
- Smart security controls required to cope with escalating threats to NEs

5 Slicing Security

- Isolation is a crucial security aspect in network slicing security
- Network Slice Isolation = Resource Isolation + Security Isolation
- by equipment-specific mechanisms on (non virtualized) RAN equip.
- in the transport by VPNs created via SDN
- in the cloud by NFV mechanisms in the (central/edge) cloud

AAA | PKI | Zoning | Zero Trust | Data hiding | Encryption | DFSEC | Automation | AI/ML

Device & UE security



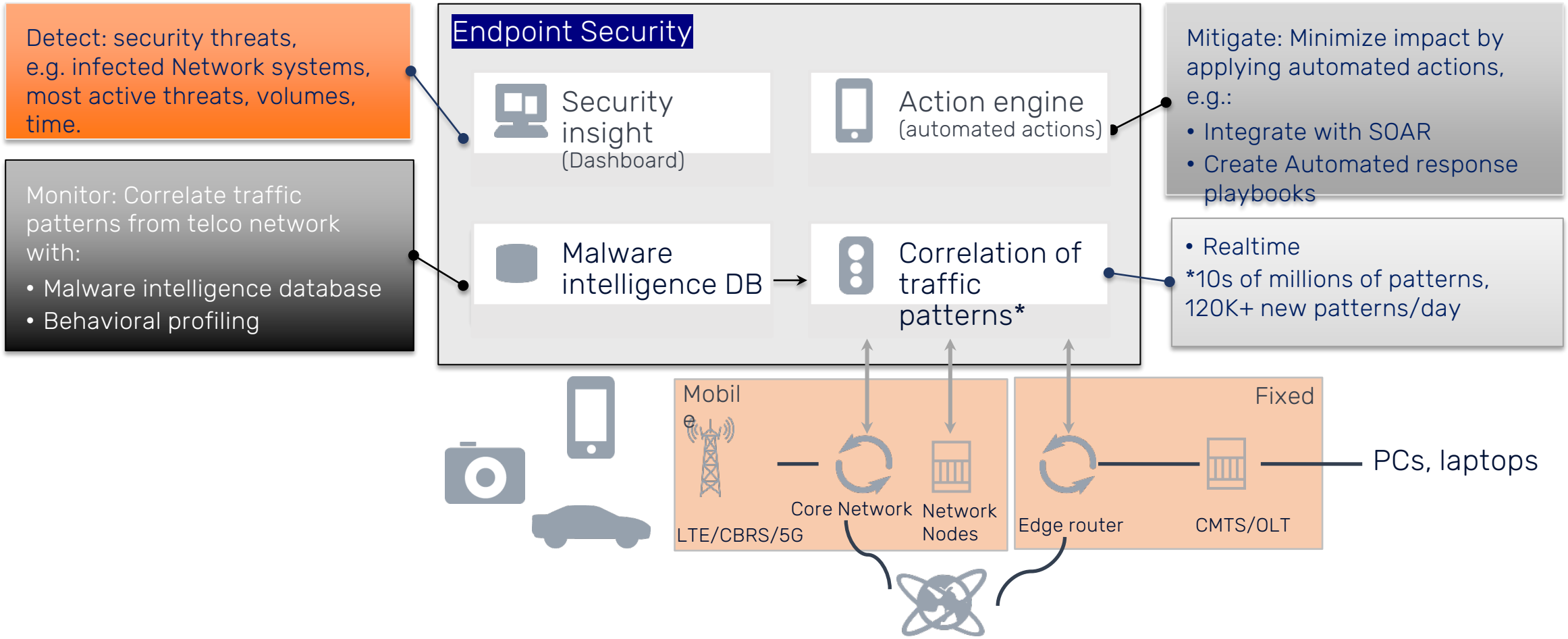
Authentication/authorization,
key agreement

Security negotiation, key hierarchy
Crypto algorithms
Enhanced subscriber privacy

Subscriber/device identifiers/credentials
Secure hardware

- UEs (mobiles) must be authenticated and authorized to use the network or specific services
- “Enhanced subscriber privacy” refers to the fact that in earlier network generations, an attacker can trick mobiles into revealing the true identity of the subscription, a practice known as “IMSI catching”, one that is applied not only by attackers but also by law enforcement. Protection against this kind of attack is considered a requirement for 5G. The attacks on the confidentiality and integrity of the traffic can be mitigated by state-of-the-art cryptography
- This is specified in the 3GPP standard

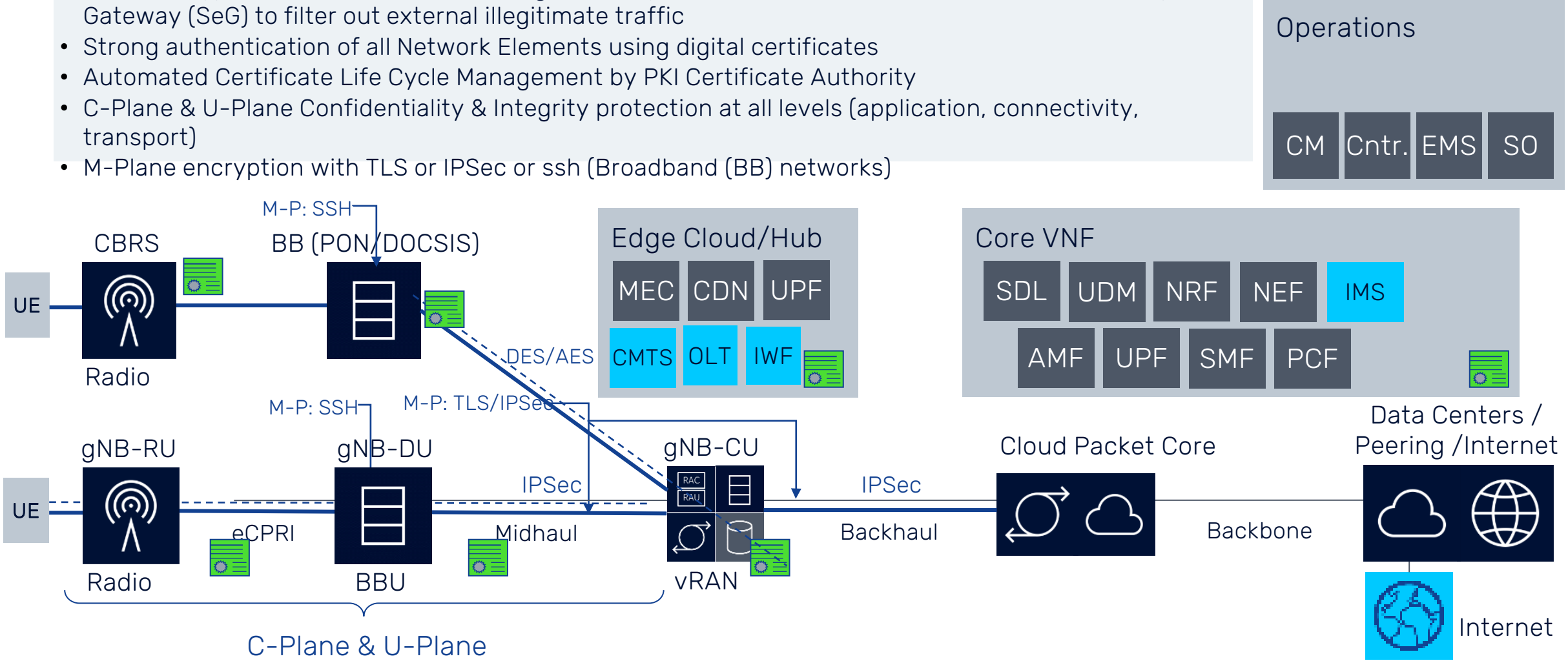
Device & UE security – Virus & Malware



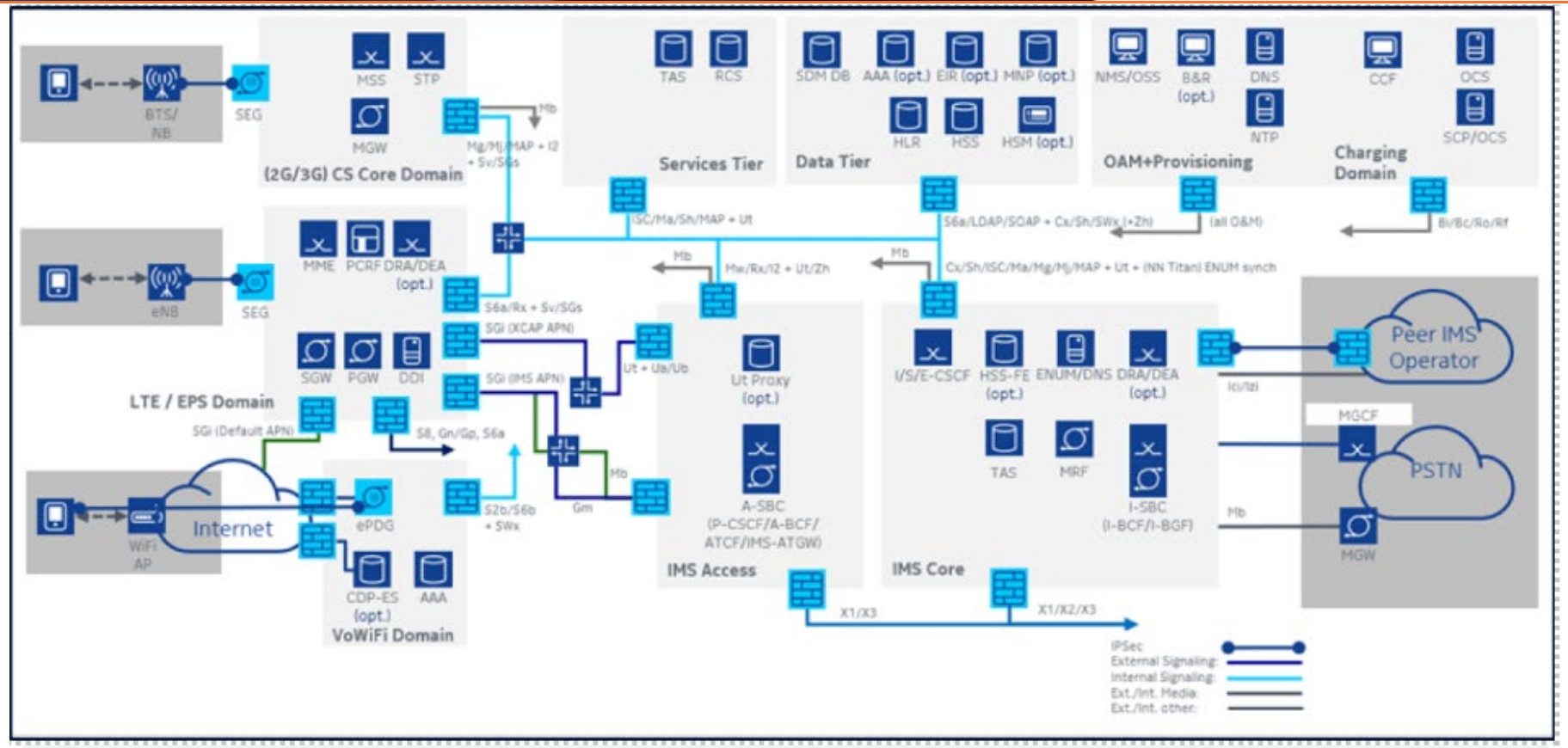
- Security is further enhanced with network-based access agnostic virus and malware detection and remediation

Radio & Transport Security

- IPsec encryption of traffic in Midhaul (High Latency Fronthaul) & Backhaul terminated in Security Gateway (SeG) to filter out external illegitimate traffic
- Strong authentication of all Network Elements using digital certificates
- Automated Certificate Life Cycle Management by PKI Certificate Authority
- C-Plane & U-Plane Confidentiality & Integrity protection at all levels (application, connectivity, transport)
- M-Plane encryption with TLS or IPSec or ssh (Broadband (BB) networks)

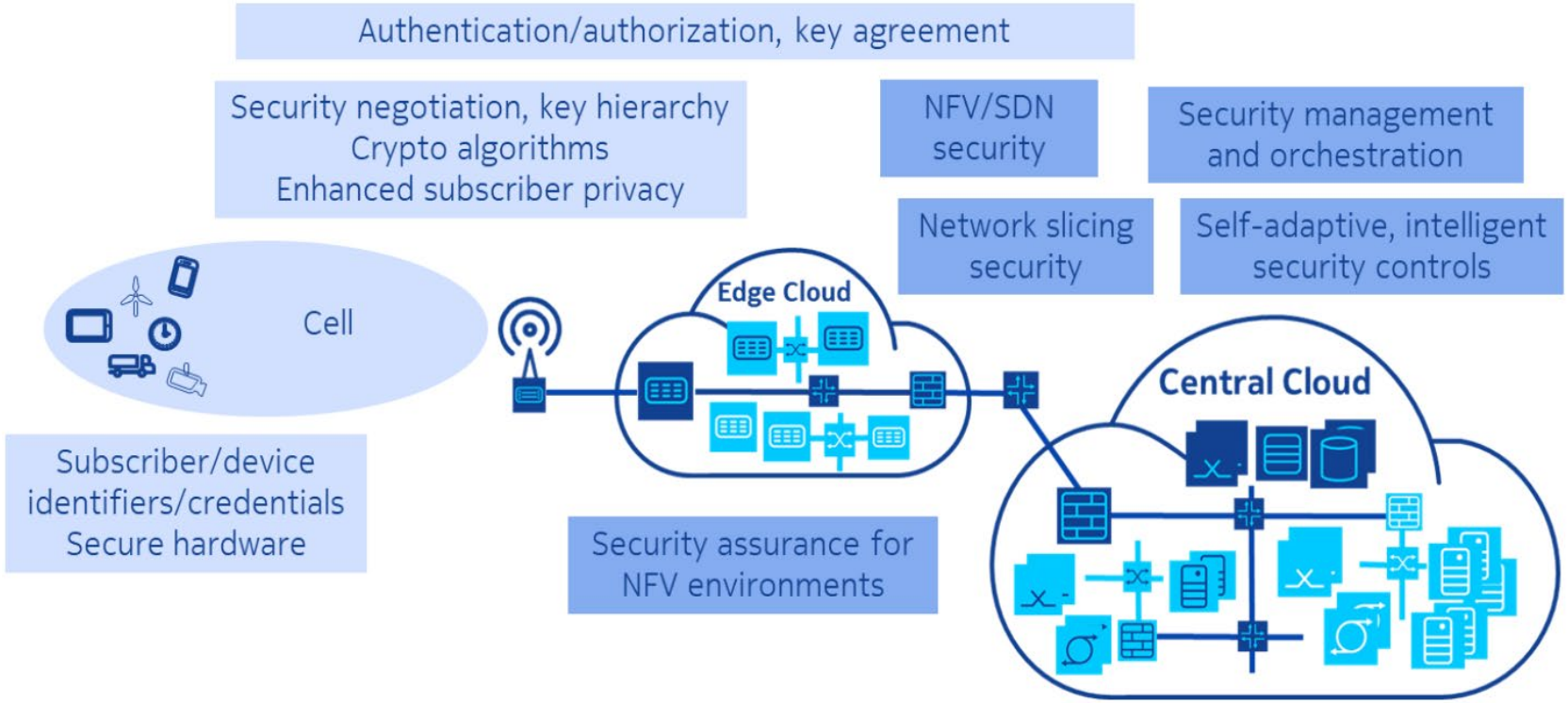


Network & Packet Core Security



- E2E traffic separation and zoning concept is mandatory, Virtualized security appliances provide isolations between security zones or domains
- GTP, SCTP (gNB) & DIAMETER (roaming interface) firewalls
- Physical or virtualized firewall with Intrusion Detection and Intrusion Protection (IDS/IPS) is required at DN or SGi interface to internet &
- Secure DNS

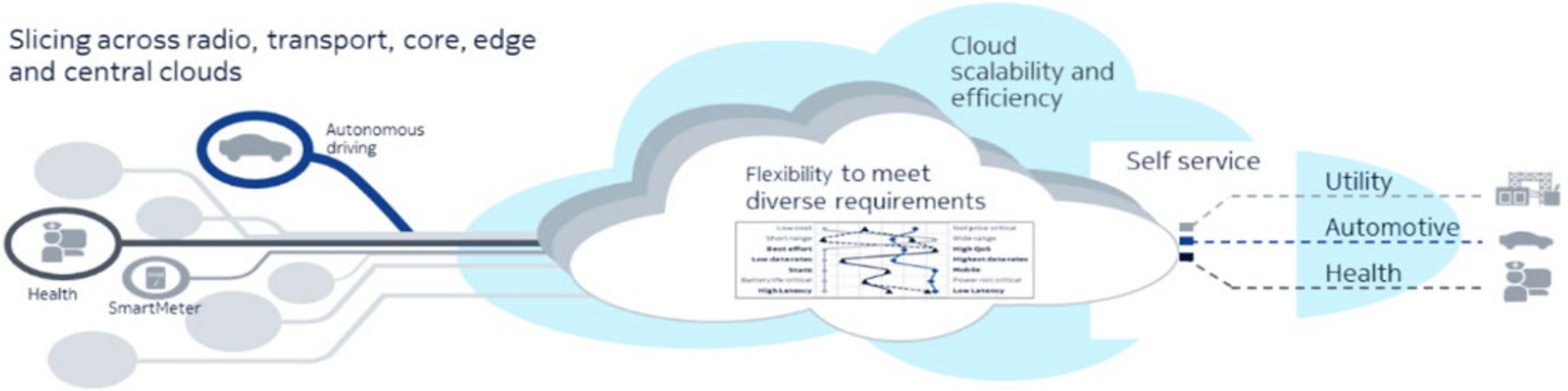
Cloud Infrastructure, NFV & SDN Security



- Secure implementations of the virtualization layer and the overall cloud platform software (e.g. root of trust, hardening, certificate mgmt., & orchestration)
- Robust security implementation of the VNFs & CNFs
- Good logical separation of VNFs provided by the virtualization layer
- Traffic separation by dedicated virtual switches, VLANs and wide-area VPNs

- Perimeter security and network internal traffic filtering by virtual firewalls
- Logically or even physically separated security zones
- Secure operation and maintenance, secure operation of IP services (e.g. DNS)
- Cryptographic protection of traffic and of data on storage
- Robust overload protection controls

Network Slicing Security



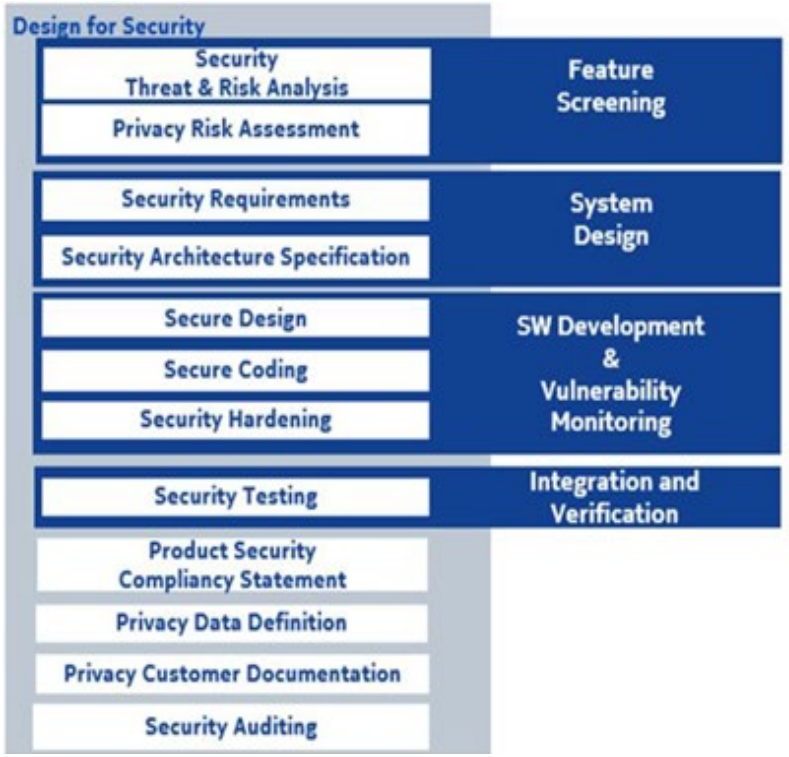
Isolation by equipment-specific mechanisms on (non virtualized) RAN equipment

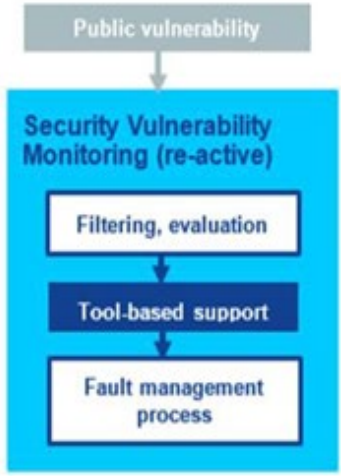
Isolation in the transport by VPNs created via SDN

Isolation in the cloud by NFV mechanisms in the (central/edge) cloud

- Network Slice Isolation = Resource Isolation + Security Isolation
  - Availability: resources dedicated to one slice cannot be consumed by another slice
  - Confidentiality: data/traffic cannot be intercepted/faked by entities of another slice
  - Hardened cloud infrastructure
  - Security management & orchestration must be slice-aware

Design for Security

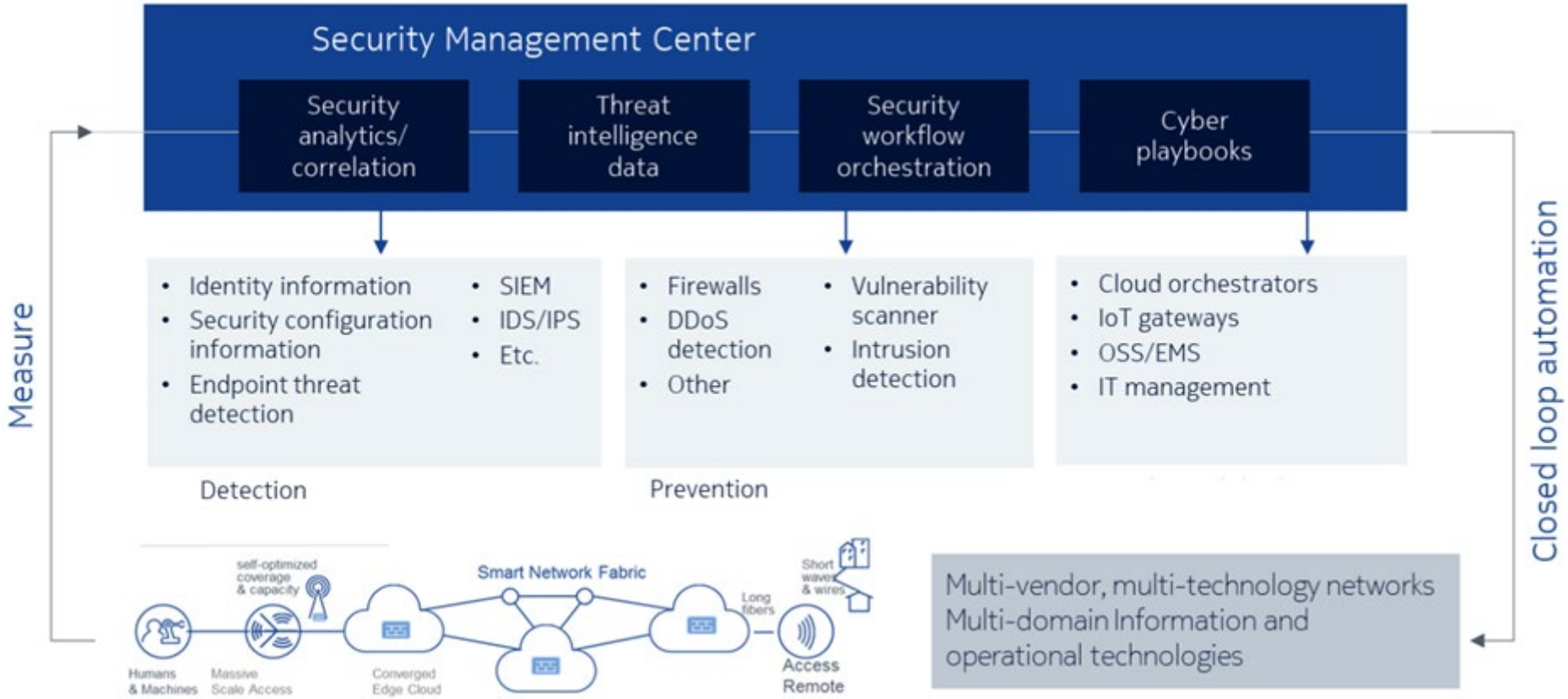




DFSEC Phase	Standard Compliancy
DFSEC	• SSE-CMM (SSE-CMM)
Threat / Risk Analysis	• ISO/IEC 27001
	• 3GPP TS 21.133 Security Threats and Requirements
	• ITU-T X.805 (threat categories)
	• Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003 Part 2
Security Requirements	• ISO/IEC 27001
	• ISO/IEC 17799
Security Architecture	• ITU-T X.805
Secure Coding	• MISRA C
Security Testing	• NIST-1 (2003). NIST Guideline for Network Security Testing.
Security Auditing	• Common Criteria, Common evaluation methodology
	• ISO/IEC 19011 Guidelines for quality and/or environmental management system auditing.

- DFSEC process embedded in the product development lifecycle and applies security requirements and security architecture at the beginning of the product lifecycle
- Ongoing, continuous & process-oriented (across products, releases & major/minor bug fixes)
- Augment with information security, incident response/vulnerability management and independent checks and audits

Security Operations



- DFSEC process embedded in the product development lifecycle and applies security requirements and security architecture at the beginning of the product lifecycle
- Ongoing, continuous & process-oriented (across products, releases & major/minor bug fixes)
- Augment with information security, incident response/vulnerability management and independent checks and audits

Security Operations: 4 key capabilities

Security operations

Comprehensive visibility

"I want to see everything happening in my environment and normalize it."

Integrated intelligence

"Help me understand what to look for and what others have discovered."

High-powered analytics

"Give me the speed and smarts to detect, investigate, and prioritize potential threats."

Adaption
Respond quickly to new cyber-attack approaches

Speed
Reduce the time a hacker stays undetected

Integration
Integrate security systems with centralized reporting

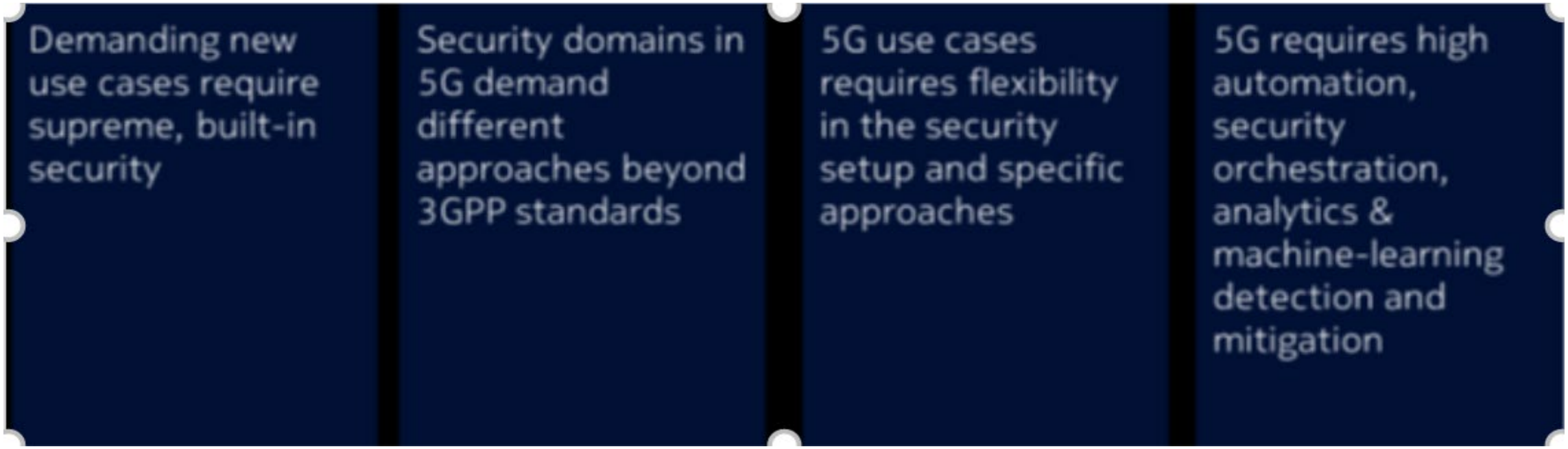
Automation
Comprehensive automation to boost efficiency

XDR: Security capabilities into a single platform

Enables all three areas of integration through a cloud-native architecture

- Detection & Integration: signature & anomaly detection for endpoints, networks and cloud
- Analytics & Intelligence: Threat intel, user, entity behavior analytics based on AI/ML
- Automation & Orchestration: Automated workflows to reduce incident response time

Summary



- 5G has a lot of mission critical use cases requiring supreme, designed-in security
  - Retrofit is always challenging and costly and, in some cases, service impacting
- Number of network functions in a typical 5G network will be an order of magnitude more than 4G or fixed (cable or fiber) BB networks
  - Number of incidents and security logs will increase in the same order of magnitude
- Different use cases means security measures needs to be implemented on top of 3GPP standards
- 5G requires automation, security orchestration and machine learning (ML)
- Partners with deployment experience in numerous 5G networks to be on top of evolving threats and strong engineering capabilities to invest

ATLANTA, GA
OCTOBER 11-14

SCTE
a subsidiary of CableLabs

Thank You!

Vasu Dalal (Director, Product Management) & Patrick Nta (Chief Security Architect)
vasu.dalal@nokia.com / patrick.nta@nokia.com

NOKIA