RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: TECH-T10

# 5G Trust model: Recommendations and best practices for CSPs

**Srinivas Bhattiprolu**

Senior Director- Nokia Software
@srbhatti5

RSAConference2020

- Introduction
- Security paradigm of 5G
- 5G trust model- A few perspectives
- Best practices, recommendations & select case studies
- Conclusions & Apply the learnings

RSAConference2020

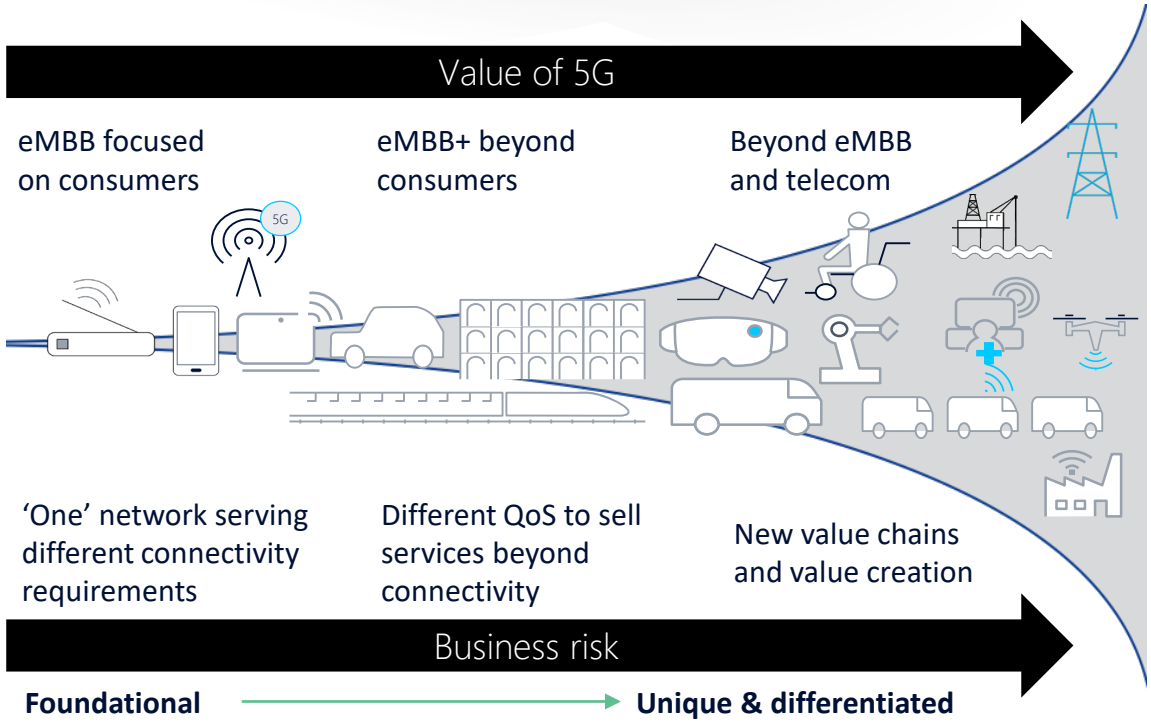
- Introduction 
- Security paradigm of 5G 
- 5G trust model- A few perspectives 
- Best practices, recommendations & select case studies 
- Conclusions & Apply the learnings 

# The Real Value of 5G

5G target markets

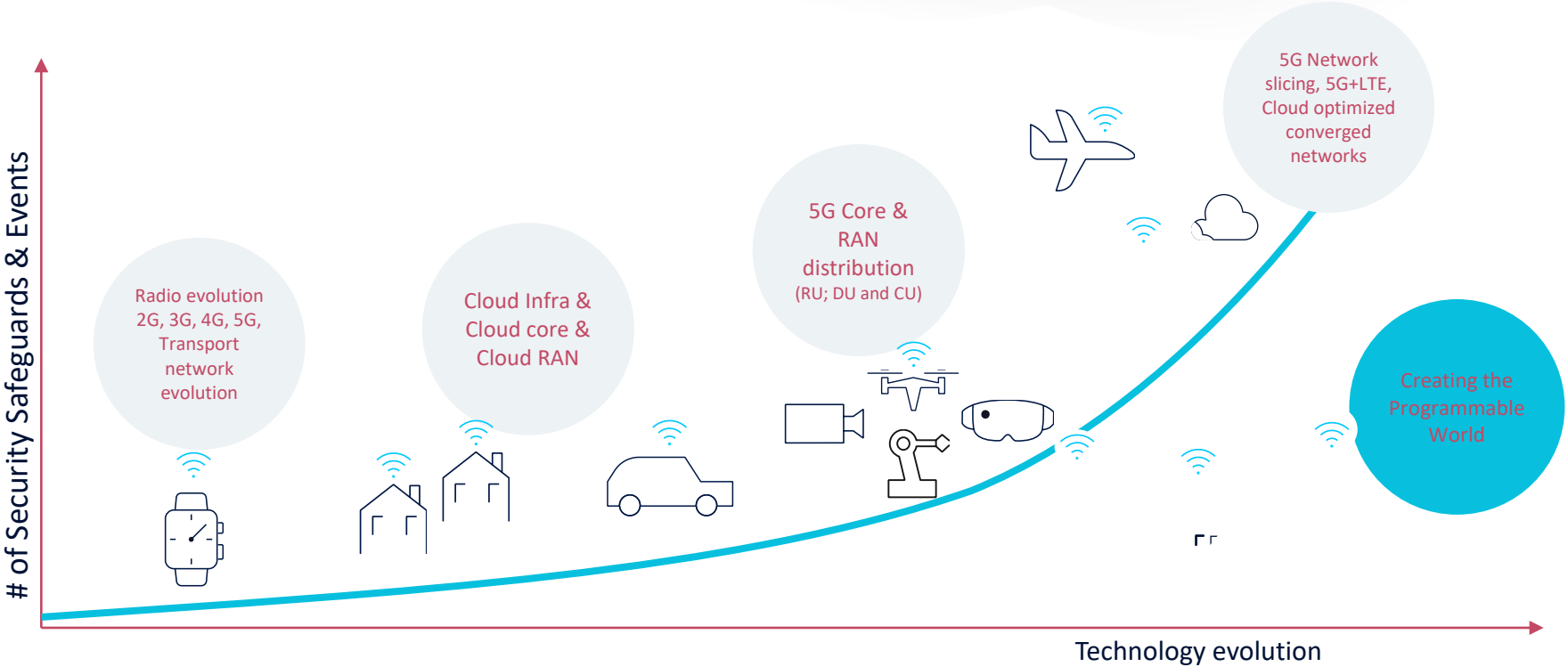
**Business approach**

5G business enablers

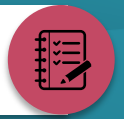


# 5G is a transformation journey – preparations needs to start today

## From 4G Security to 5G Security through combination of technologies



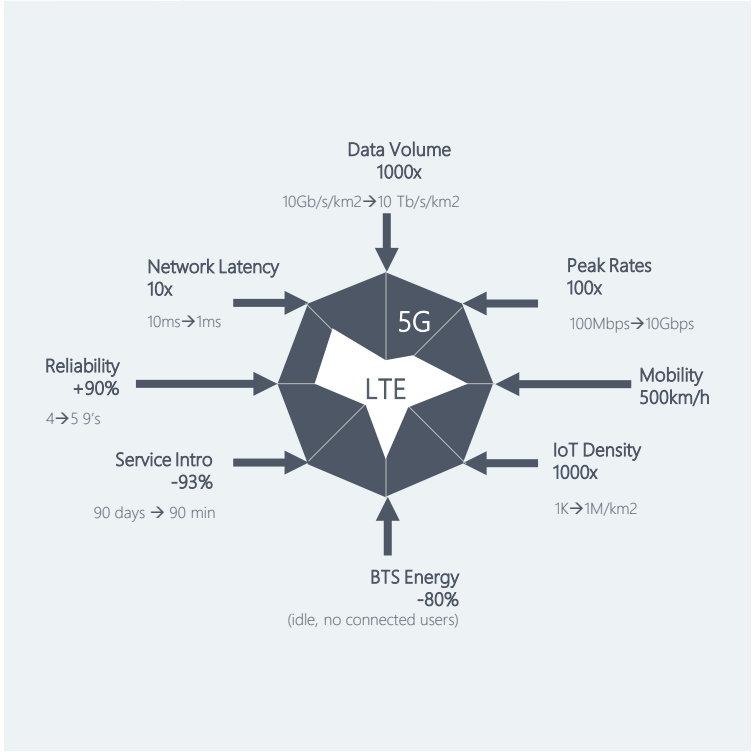
RSAConference2020

- Introduction 
- Security paradigm of 5G 
- 5G trust model- A few perspectives 
- Best practices, recommendations & select case studies 
- Conclusions & Apply the learnings 

# 5G use cases & services have demanding, diverse and dynamic requirements

Network Requirements

| | 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 |



# Security landscape is changing

## Today

Mostly bare metal networks, with security measures primarily based upon

- 3GPP defined mechanisms
- Perimeter security, Network zoning and Traffic separation
- Secure operation and maintenance
- Reactive Security Measures
- Network Element security

## What is Coming in 5G realm?

- **Complex ecosystem** with multiple stakeholders requires trusted and trouble-free interaction between them
- Migration to **NFV/SDN** introduces new security challenges
- Need for **flexible security** measures depending on **use case**
- Growing influence of availability and integrity of network service on **human security** or even **life**

## ...and escalating cybersecurity threats and breaches

**Compliance mandates**

GDPR fines can cost

**billions**

for large global companies

**Skills shortage**

By 2022, there will be

**1.8 million**

unfulfilled cybersecurity positions

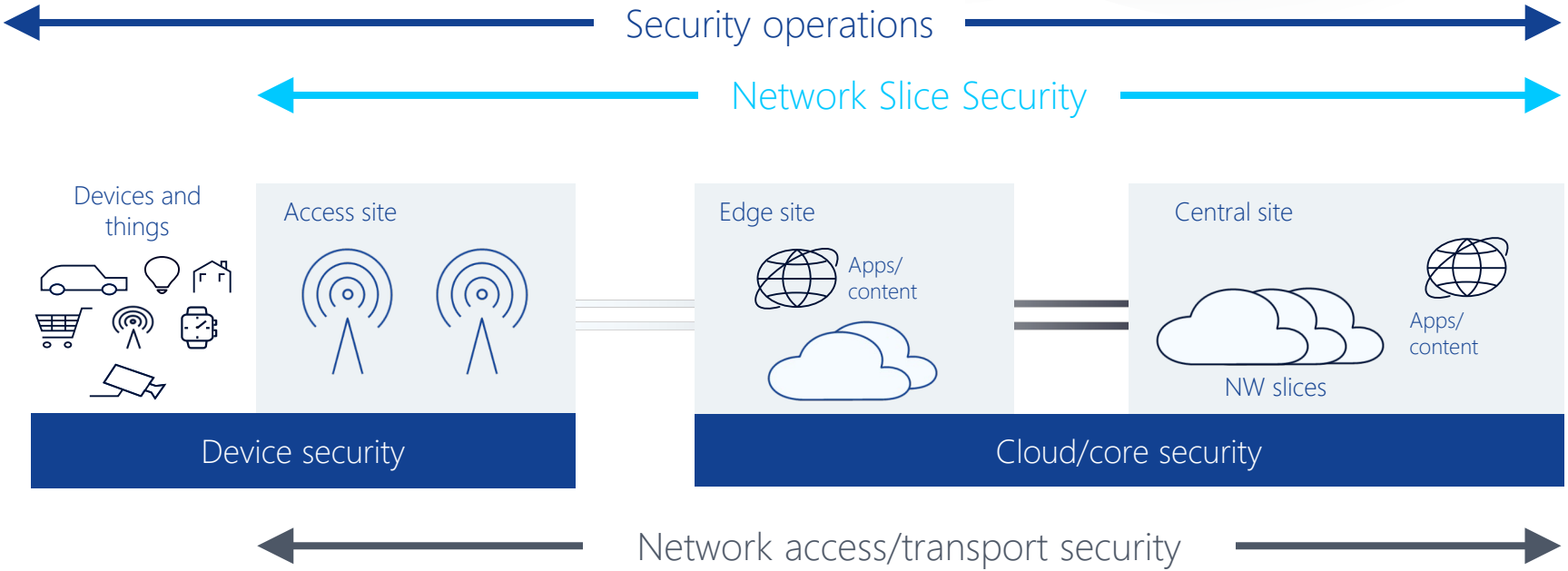
**Too many tools**

Organizations are using

**too many**

tools from too many vendors

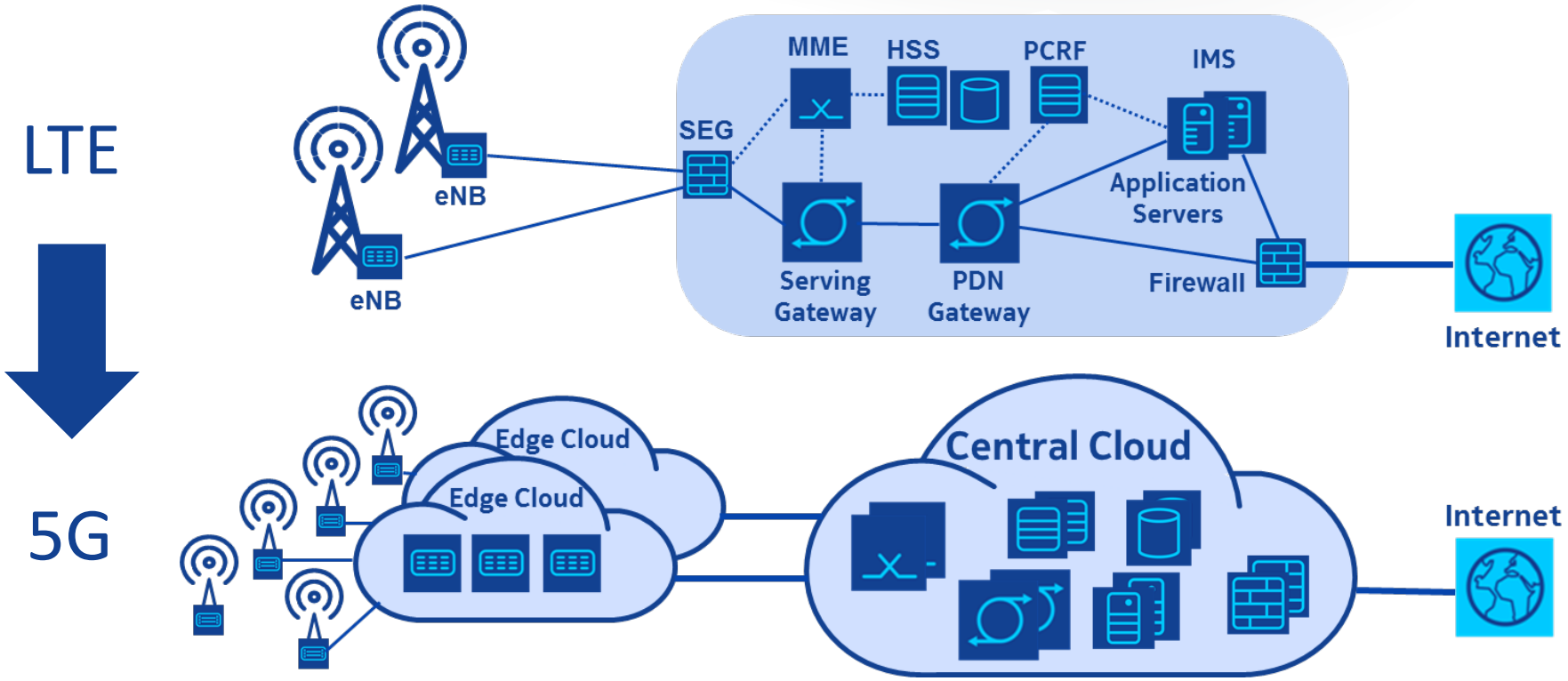
# Architecture view: 5G security operations requirements for CSPs



RSAConference2020

- Introduction
- Security paradigm of 5G
- 5G trust model- A few perspectives
- Best practices, recommendations & select case studies
- Conclusions & Apply the learnings

# From LTE to 5G: Adopting New Networking Paradigms



# 3GPP standard Security Architecture

## 4G vs 5G, a brief comparison

### 4G (LTE) Security

UE is authenticated by 2 methods:
a. LTE AKA on LTE access and;
b. EAP AKA' on Wifi access.

---

Roaming:
No authentication confirmation to Home network

---

MME is considered a trusted node in the authentication process.

---

UE Subscription identifier (IMSI) is not a secret, as it is sent over-the-air (Prone to IMSI-catching)

---

No Integrity Protection of User data, packet injection is possible

---

Core Network is not Service Based

### 5G Security

Access agnostic security- network authenticate UE:
Either 5G AKA or EAP AKA' regardless of access type.

---

An authentication confirmation is sent to the Home AUSF, when UE gets authenticated while roaming.

---

Security Anchor Function is introduced to augment AMF security, deployable in the network edge.

---

Permanent Subscription Identifier (SUPI) is not sent in over the air in any network procedures
(Prevents IMSI catchers, avoids fake eNBs)

---

Supports Integrity Protection of User Plane data, avoids packet injection.

---

Supports Service Based Core Network architecture and better inter-PLMN security.

# Key Cloud Security Risks

## Security Challenges

### Virtualization attack surface

Hypervisor and Virtual Machine (VM) vulnerabilities distribute attacks to virtual infrastructure

### Dynamically distributed resources

Dynamicity, Agility and Site Distribution requires constantly updated Safeguards

### Shared Resources and Privacy

Isolation principle is weakened by shared resources which puts Privacy at risk

### Sensitive VNF Data

Location and trust level of the platform are not guaranteed during VNF deployment (snapshot, image)

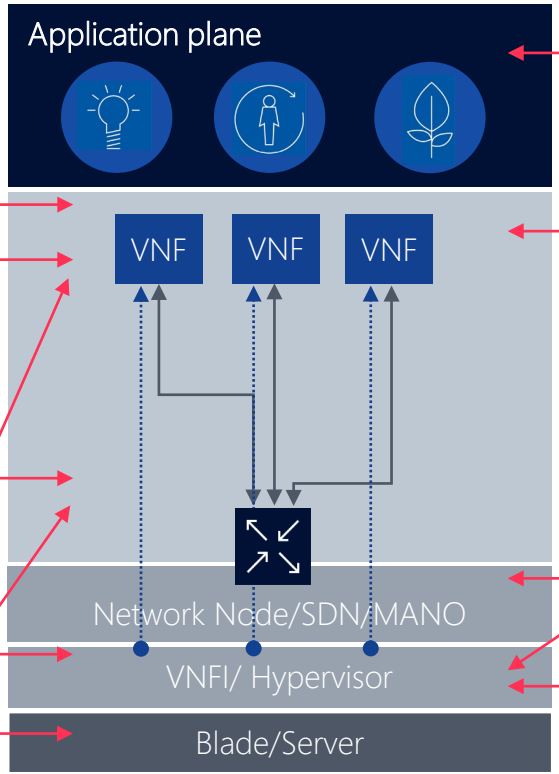
### SDN security exposure

SDN controller and communication channel requires safeguards

### Cloud Orchestration vulnerabilities

Insecure API allows deployment of malicious VM

# Cloud Infrastructure threat landscape




- Malware Injection Attack
- Rogue VM

- API exploitation eg Fuzzing

- SDN surface

- Network Manipulation
- Traffic diversion/redirect
- Injection attacks

- Untrusted evacuation
- VM escape
- Rogue SW update

- Hardware focus attacks (eg.DDoS)

- Exploiting known vulnerabilities
- App manipulation
- Password guessing
- Buffer overflow

- Privillege escalation
- VNF impersonation

- Route BGP/VRF injection
- Traffic sniffing
- Data model injections

- VMI DKSM attacks

- Memory/ Side channel attacks
- Storage attacks

- **External threats** – Attacker can use a vulnerability in the user's VM to take a control of it, then move laterally to other VMs in the cloud until the attacker puts their hand on the crown jewels.
- **Threats from a cloud provider** – Attacker can use a cloud misconfiguration for escalation of privileges or information disclosure. For example, an attacker can launch a new VM, and attach a volume that was used by a previously running user VM to access sensitive user data.
- **Threats from another tenant** – Attacker can, for example, run an escalation of privileges to escape their VM and take a control over the host and/or other tenants. Attacker can also get access to shared resources, such as storage or network resources.

References
CVE-2017-18191, CVE-2018-7262 ,CVE-2018-1128

# IoT eco system and threats at different levels

- Orphaned devices, can be tampered easily
- Physical tampering of the components possible

Physical

- Simplistic implementation of various stacks
- Improper exception handling and input validation
- Excessive and direct exposure to internet

Smart IoT Device

- Use of non IP protocols that are less secure
- Local data link are less secure & lack protection
- Hijack firmware upgrades

Local wireless Communication

- Gateways will form a conduit to devices
- Deficiencies in software libraries

Gateways

- Transport corruption,
- Transport disruption and snooping attacks
- Data poisoning attacks

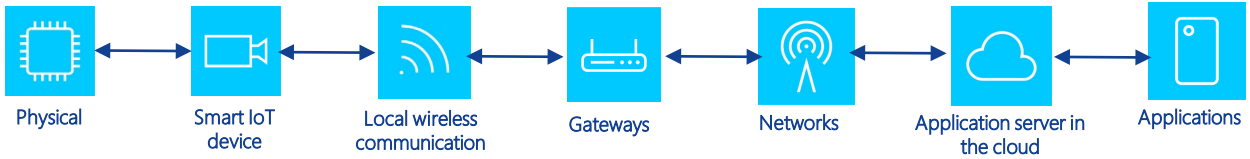
Networks

- Central point of vulnerability
- Potential for Masquerading

Application server in the cloud

- APIs offer hacking opportunities
- Vulnerabilities in middleware
- Steal the credentials of the applications

- Users installing the devices and applications themselves
- Use of default passwords
- Specific device vulnerabilities



# Changing Landscape….

## Today

Operations by technology silos

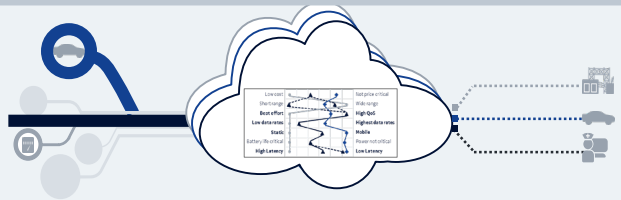
| | | | |
|---|---|---|---|
| Radio vendor A | Core vendor 1 | Transport vendor I | Security vendor * |
| Radio vendor B | Core vendor 2 | Transport vendor II | Security vendor ** |

### Historical de-centralized approach

- Disparate systems, platforms & apps
- Silo solutions for data handling, security monitoring and reporting
- Time, cost- and resource-intensive

## In the 5G era

E2e horizontal Security Services



### Automated Security Operations

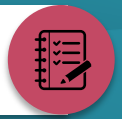
- Aggregated logs and data for real-time monitoring & management
- Consolidated view for efficient reporting
- Simplified incident management and forensics

Automated holistic security orchestration and management will be crucial in 5G networks

End-to-end security needs will have to be managed through a central point of control

Smart security controls are required in order to cope with unpredictable threats that try to exploit weaknesses in the network

RSAConference2020

- Introduction 
- Security paradigm of 5G 
- 5G trust model- A few perspectives 
- Best practices, recommendations & select case studies 
- Conclusions & Apply the learnings 

# Regulatory requirements across the Globe

## Countries must consider 5G specific regulations as an extension of Cybersecurity guidelines

### Key recommendations/best practices

**Prague Proposals**

- Policy
  - Using international, open and consistent based standards
  - Every country is free in accordance with international law
  - Transparency and Equitability are key
- Technology
  - Regular VA and risk assessment
  - Technological changes related to 5G must be taken into account
- Economy
  - Increase diversity of technological solutions is essential
  - Effective oversight is critical

**Key regulatory considerations**

- Promote Digital Single market
- Balance of Interest and Global Context
- Applicable law must be easy to define
- Right to be forgotten
- Foster interoperability and data portability

### Prague Proposals are recommended

1. Ascertains that security of 5G networks is crucial for national security, economic security and other national interests and global stability
2. Recognizes following perspectives
   - Security isn't just a technical issue
   - No Universal solution
   - Broad nature of Cyber threats and measures
   - Proper risk assessment is essential
   - Nationwide approach

# Design for Security

## Proactive: DFSEC

Design, implement & test

Feature screening
- Security threat & risk analysis
- Customer requirements & standards
- Privacy Risk Assessment

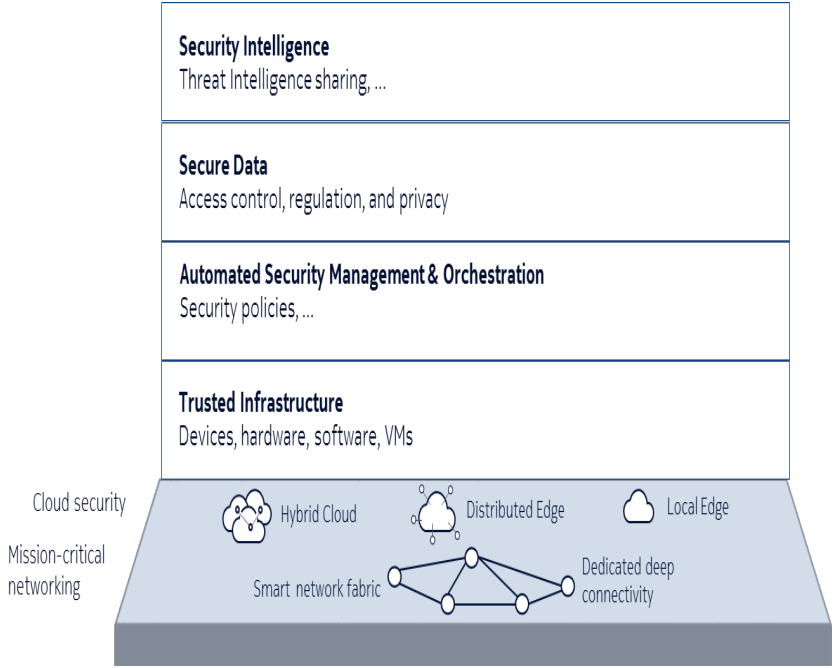
Systems engineering and design
- Security & Privacy requirements
- Security architecture specification

Development
- Secure coding
- Source Code security testing
- Product hardening

Integration & verification
- Security testing

Compliance (Security & Privacy): Gap analysis and Mitigation plan

## Security Layer Model to address APTs



# How should CSPs 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 Telco Cloud

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

### 3 IOT & Devices

- 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

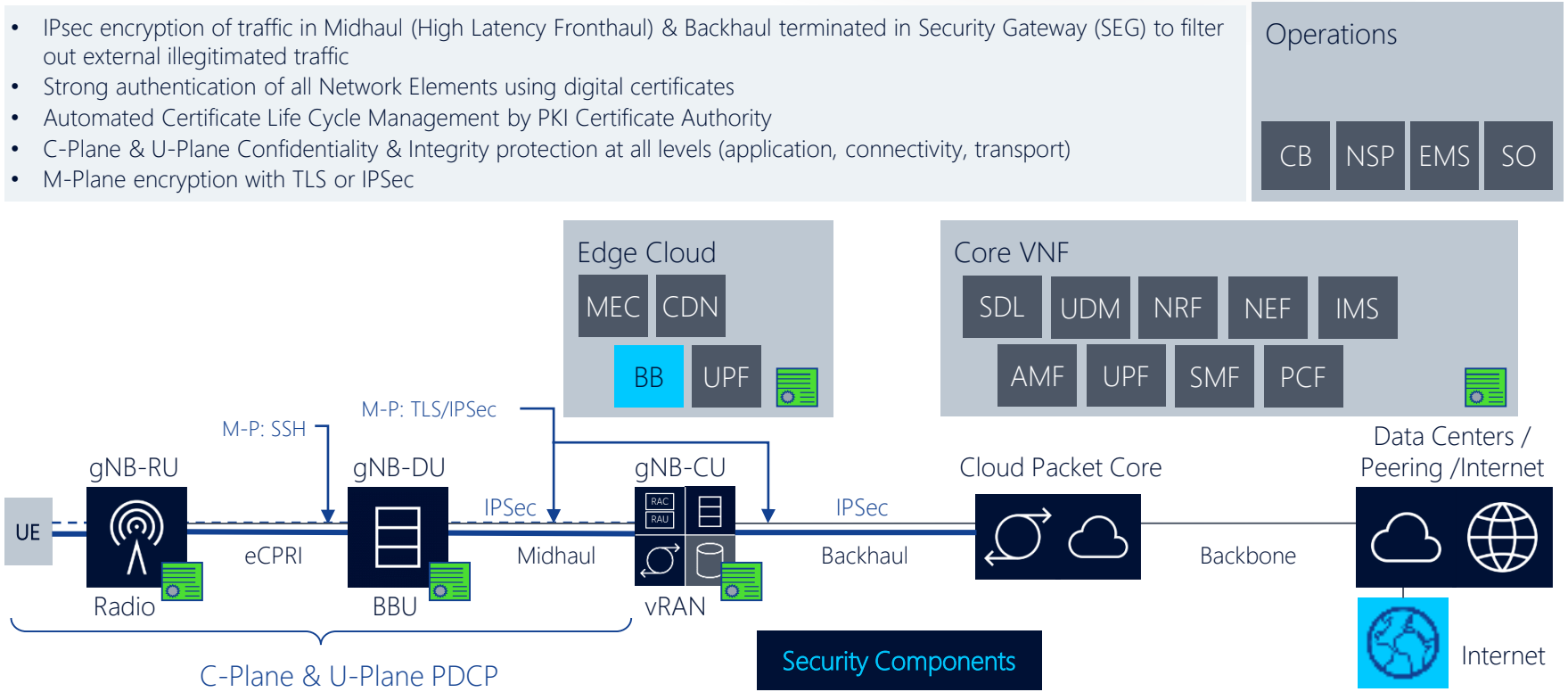
- Automated holistic security orchestration and management will be crucial in 5G networks
- E2E security needs will have to be managed through a central point of control
- Smart security controls required to cope with escalating threats to NEs

### 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

# 5G Radio Transport Security

- IPsec encryption of traffic in Midhaul (High Latency Fronthaul) & Backhaul terminated in Security Gateway (SEG) to filter out external illegitimated 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



# Four key 5G security operations capabilities to help CSPs build digital trust

## 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

# Best practices- Use of next generation technologies in 5G Security

## Multi dimensional analytics

- Analytics are important because many threats are designed to stay undetected for as long as possible, Analytics will help in the aspect of "visibility" from the device up through the network and into the cloud.
- Without the ability to collect, correlate and analyze data from end to end, security threats could easily be missed.
- Analytics will provide a comprehensive real-time view of all the key components

## Machine Learning

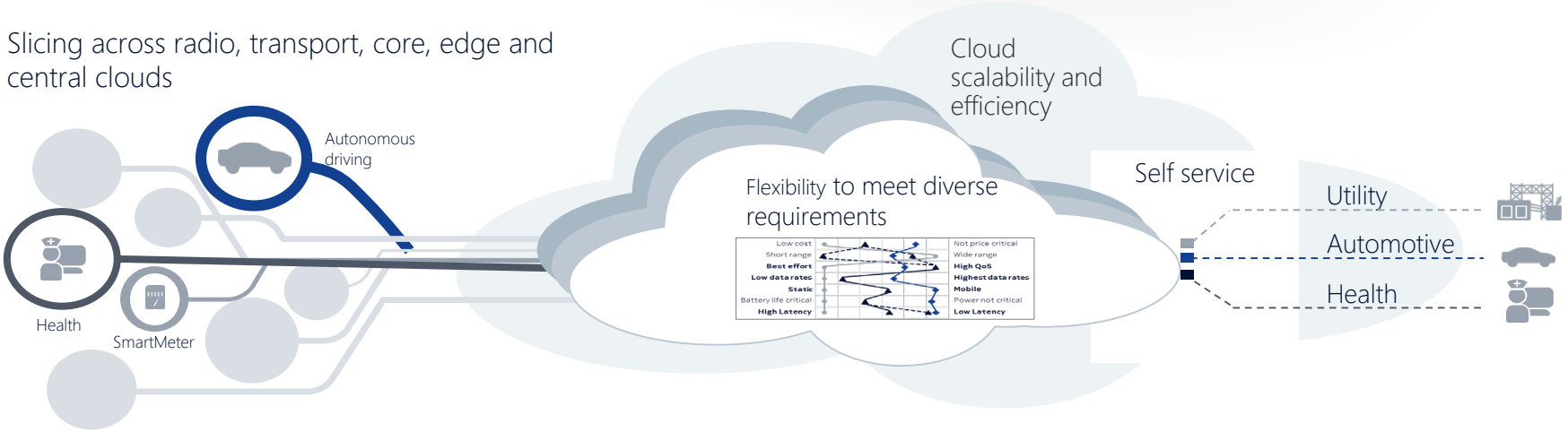
- Prediction and automation is achieved through Machine Learning
- A few uses of ML are
  - To correlate data from multiple domains, sources
  - Catch anomalies
  - Provide contextual intelligence about threats
  - Weigh business risks in a structured manner
  - Recommend (or enact) mitigation steps.
- ML and Analytics are integral part of SOAR strategy.

## Blockchain

- Blockchain can be utilized for credibility verification in the IoT scenario
- The idea is to establish a credibility verification structure, data flow and a credibility verification process
- The primary objective of the process is to prevent any device spoofing So, the device will have to perform three specific activities,
  - share its certificate
  - confirm that the device is the original one
  - Prove the data is original
- This is a novel & effective approach.

Key is to achieve *Visibility, Prediction and Automation*

# Network Slicing Security & Network Slice Isolation




Network Slice Isolation = Resource Isolation + Security Isolation

- Resources dedicated to one slice cannot be consumed by another slice.
- Data/traffic cannot be intercepted/faked by entities of another slice.

**Isolation is a crucial security aspect in network slicing security**

# A few case studies

## Creating foundation for comprehensive 5G Security measures

### 1 A large CSP in USA

- Implemented Digital Identity management for IoT and network elements
- Adaptability to customer requirements in IT and Mobile network domain
- The scope includes automated full lifecycle management
- Eliminate manual intervention for 100K certs
- This will reduce the manual intervention and will eliminate human errors

### 2 A large global CSP

- Built a comprehensive framework for securing the converged cloud established across IT and network
- These include aspects like Zoning, secure communication and VNF security
- Holistic principles to focus on three important aspects- people, process and technology and multi vendor environment

### 3 A large CSP in Asia

- Simplify security operations and enforce security policies more effectively, as well as accelerate the responsiveness to incident analysis
- Security operations automated through SOAR concept
- 3000+ security incidents have been proactively identified and effectively managed to avoid any service disruption.

### 4 A large CSP in Japan

- Established an SoC with
  - Enhanced threat detection & response
  - Comprehensive visibility
  - Realtime reporting
  - Automated remediation using SOAR for various activities
  - A single SoC across IT and network with advanced detection and automated remediation

RSAConference2020

- Introduction
- Security paradigm of 5G
- 5G trust model- A few perspectives
- Best practices, recommendations & select case studies
- Conclusions & Apply the learnings

# In summary- Key recommendations

## Holistic approach

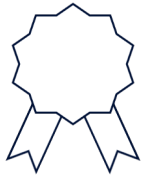
5G Security isn't just a technical issue. People, process and Technology will play an equally important role

## Sound Risk Assessment

Systematic and diligent risk assessment, covering both technical and non-technical aspects of cyber security, is essential to create and maintain a truly resilient infrastructure

## 5G Security must be budgeted

5G security will require transformational changes to the current security mechanisms in CSPs. This requires additional budgets



## Embed Security in the network

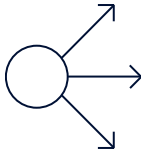
5G network will not have conventional boundaries: it will be an open ecosystem with all kinds of unmanaged third-party devices

## Design for Security

CSPs to engage the market and monetize the investments they're making in their networks to deliver on the new 5G use cases at scale

## Co existence of solutions

Multi vendor environments are here to stay in 5G. Select your 5G solutions that support open, multi vendor approach.



## Advanced Technologies

Multiple layers to be secured at scale, this is impossible with conventional methods, us of advanced concepts like Analytics, ML in security is a must

## Eco system for sharing

To proactively detect and respond to security threats, security-related intelligence has to be shared across all the stakeholders -suppliers, partners and customers

## 5G Security Operations

Automated, adaptive security operations with centralized command control and smart security measures will be the key to success

# Apply the learnings from this session

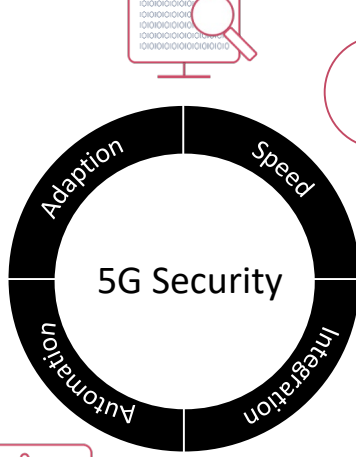
## Points to ponder……

**Remember holistic approach involves people, process and technology**

Central point of control will be key

Cooperation among players is key

Create Security budget early in the process




Automation is a must

Remember- Security across layers

Mandatory to use advanced concepts

Multi vendor environment is here to stay

RSAConference2020

# Q&A