RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **CMI-W03V**

Small Cells and Smaller Devices: Using 5G to Solve IoT Device Security

Senthil Ramakrishnan

Director – Internet of Things
AT&T Business
@senthil_rn

Agenda

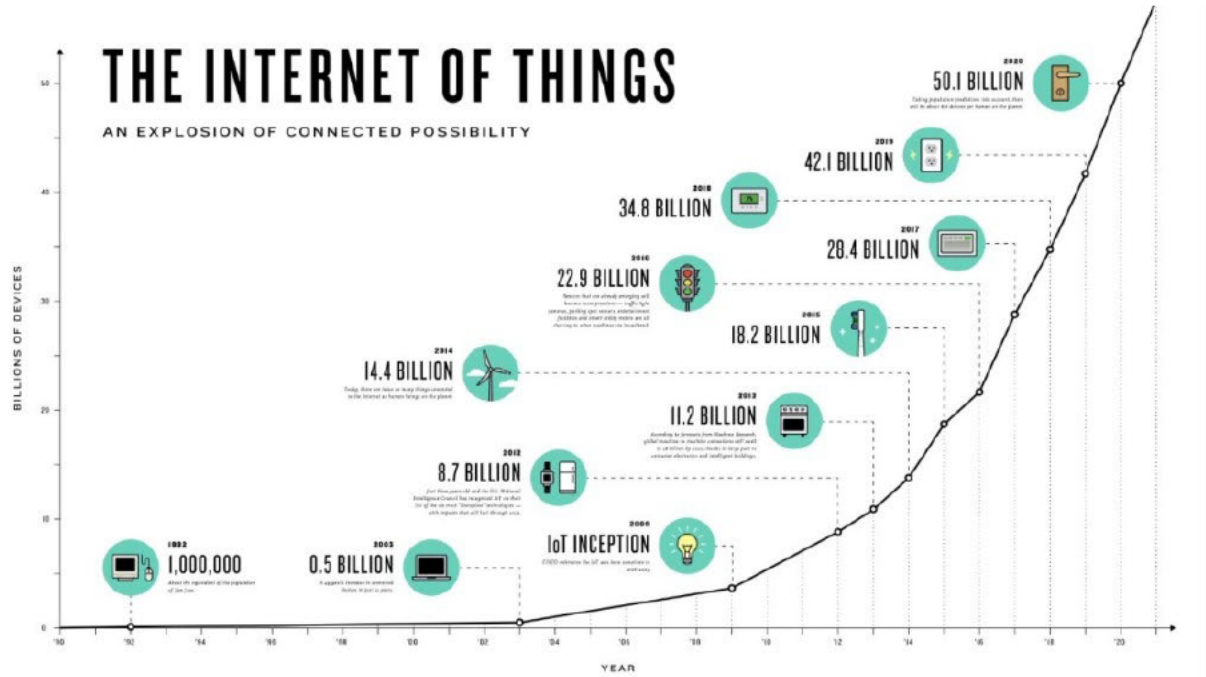
- Introduction to IoT
- IoT Security Challenges
- IoT Security Framework
- Introduction to 5G
- 5G Security Capabilities
- Network-based IoT Security
- Conclusion

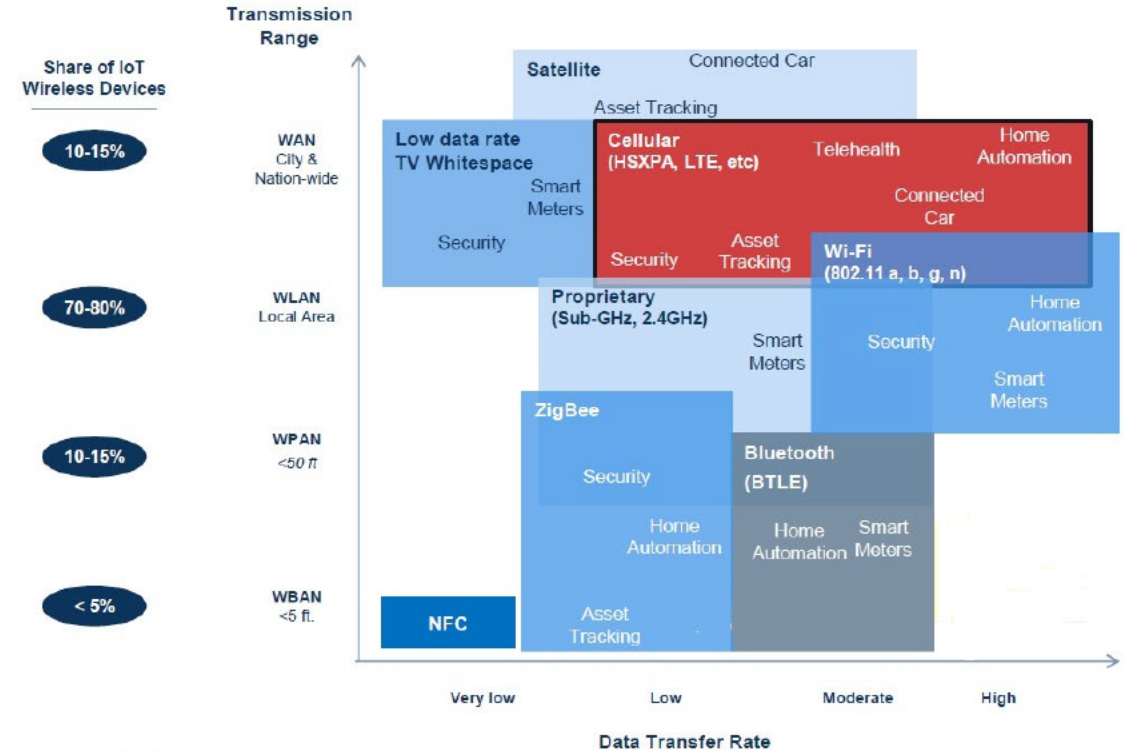
RSAConference2020 APJ

A Virtual Learning Experience

Introduction to IoT

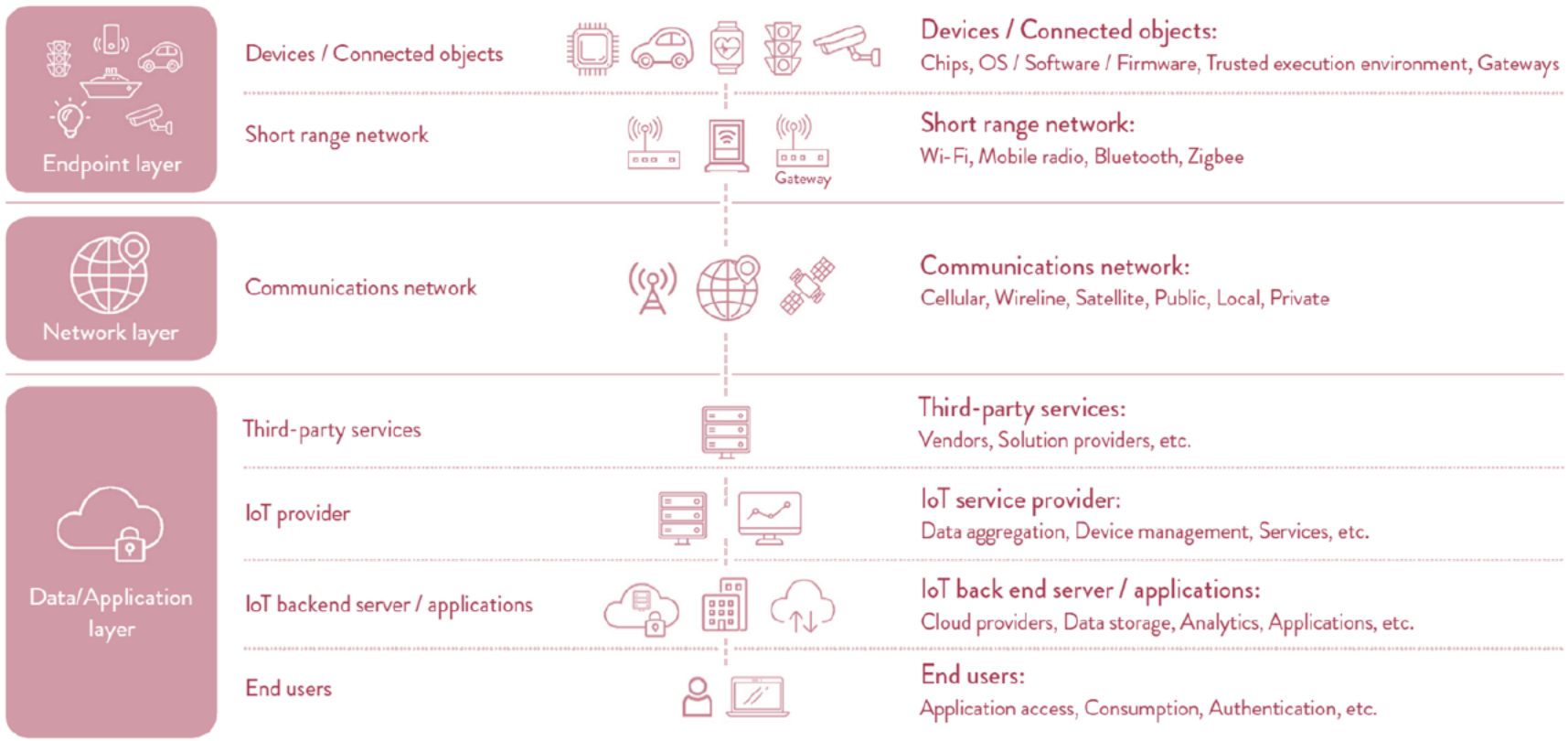
IoT - Growth and Deployment





Source: IEEE, AV&Co. Research

IoT Architecture



IoT in the Real World

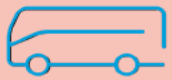
Manufacturing

Logistics

UBI

Fleet OEM

Value Added Reseller



Retail

Security

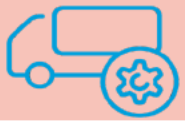
Drones

Agri-Tech

Oil / Gas

Connected Car

Fleet Mgmt



Wearables

Automation

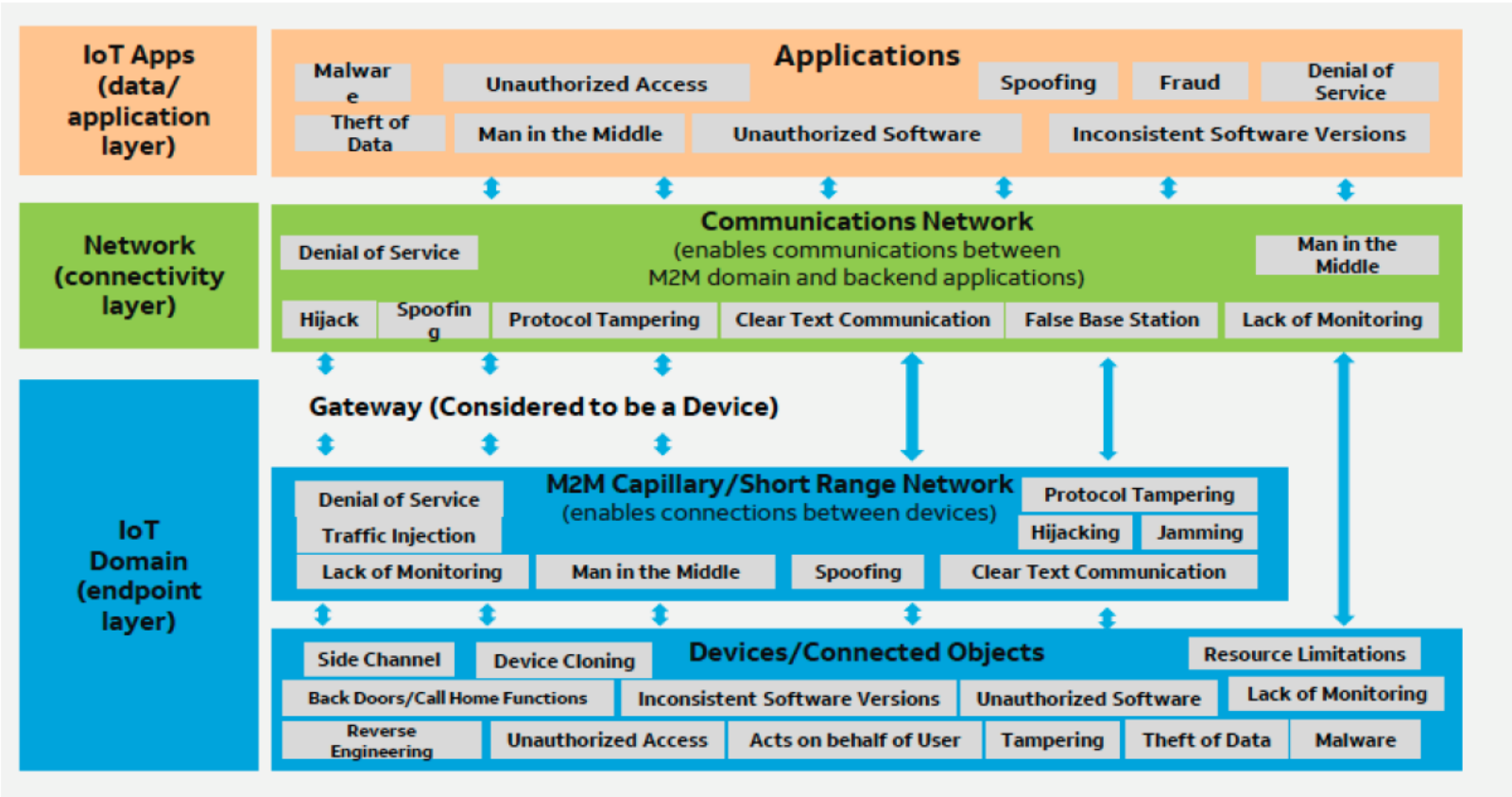
mHealth

Smart Cities

RSAConference2020 APJ
A Virtual Learning Experience

IoT Security Challenges

IoT Security Considerations

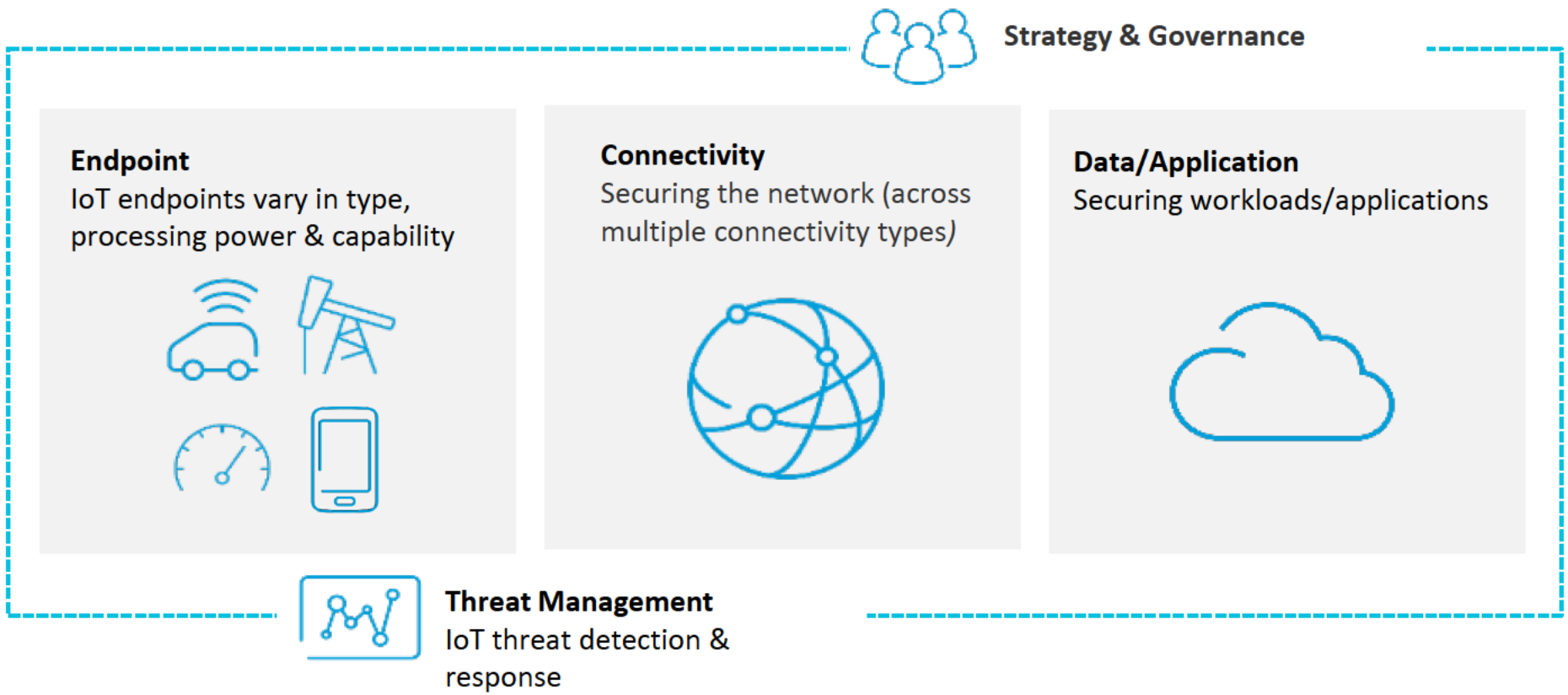


IoT Security Impacts

	IoT	Security Challenge
Device Volume	Very large volumes	• Need to monitor and manage a very large number of devices • Deployed in various environments and geo locations
Device Types	Wide variety of custom devices	• Wide variety of devices with varying security capabilities • Singular/standardized security solutions cannot be deployed across all device types
Hardware/Software	Custom and varied	• Custom hardware and software prevents • Complex lifecycle management
Management and Control	Primarily unmanaged devices	• Need for multiple device management solutions • Security patching and FOTA requirements are very complex
Applications/Backends	Fully custom	• Cannot integrate to existing security solutions
Device Access	Both remote and public depending on IoT vertical	• Vulnerable to tampering • Exposed to hostile environments • Not easily accessible
Risks	High risk for certain verticals	• Data Loss/compromise • Lost revenue • Impact to life

IoT Security Framework

A multi-layered approach to security is highly recommended to help protect the IoT ecosystem end-to-end



RSAConference2020 APJ

A Virtual Learning Experience

5G and IoT Security

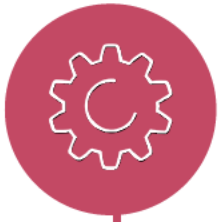
5G Capabilities

Ultra low latency

<20ms Round-trip time latency expected

Ultra reliability

Support mission critical latency sensitive apps



Massive IoT connectivity

Support billions of connected devices

Ultra high-speeds

Faster speeds possible with mmWave

Numbers represent the long-term requirements for 5G and may take years to realize

mmWave = millimeter wave

Edge to Edge Transformation

Expanded radio access

- Ultra-fast speeds
- Ultra-low latency
- Higher reliability
- Massive densification
- Wi-Fi convergence

Smarter devices

- Autonomous car
- Sensors / tracking
- MR (Mixed Reality)
- High definition cameras

Edge computing

- Lower latency
- Reduced cloud opex
- Service chaining
- Innovation driver

Transport

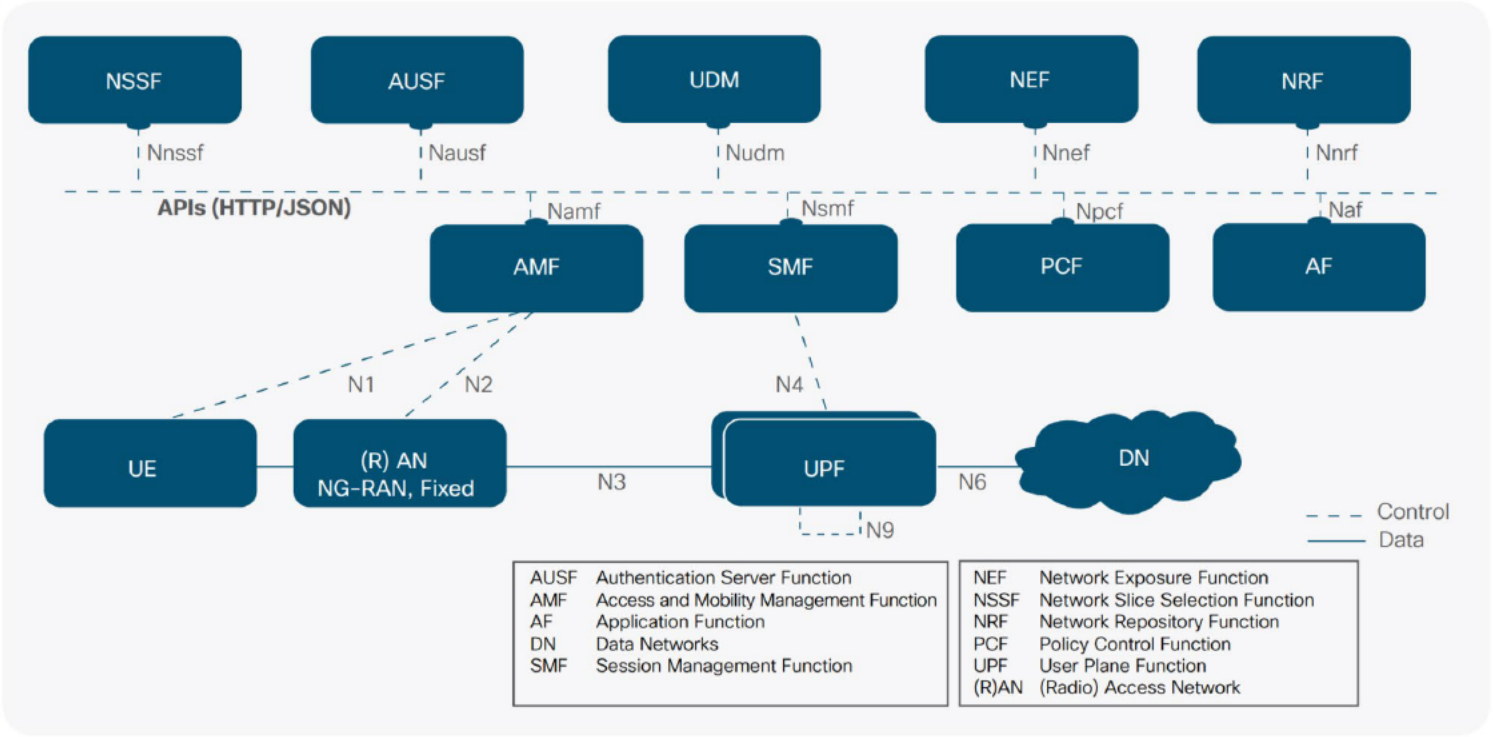
- Flexible schemes
- Self-backhauling

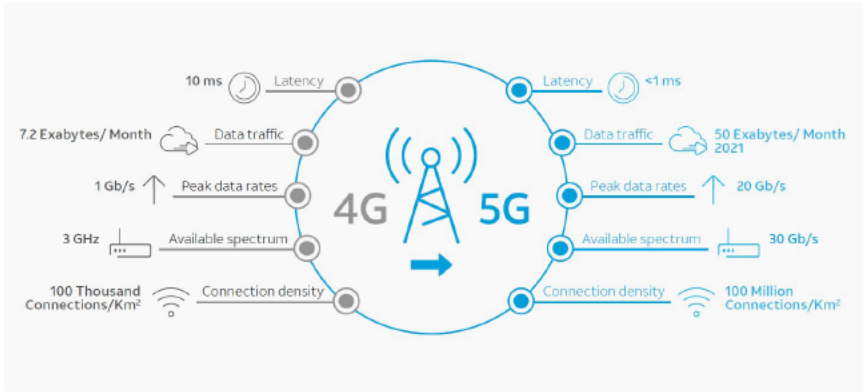
Reimagined core

- Control/user plane separation
- Native NFV
- Network slicing
- Higher reliability
- Scalability

5G Reference Architecture

- The 5G core has evolved from the 4G EPC in two steps:
  - Control and User Plane Separation (CUPS) of the 4G Evolved Packet Core (EPC)
  - Reorganizing the 4G EPC Control CUPS functions into service based architecture
  - Massive virtualization





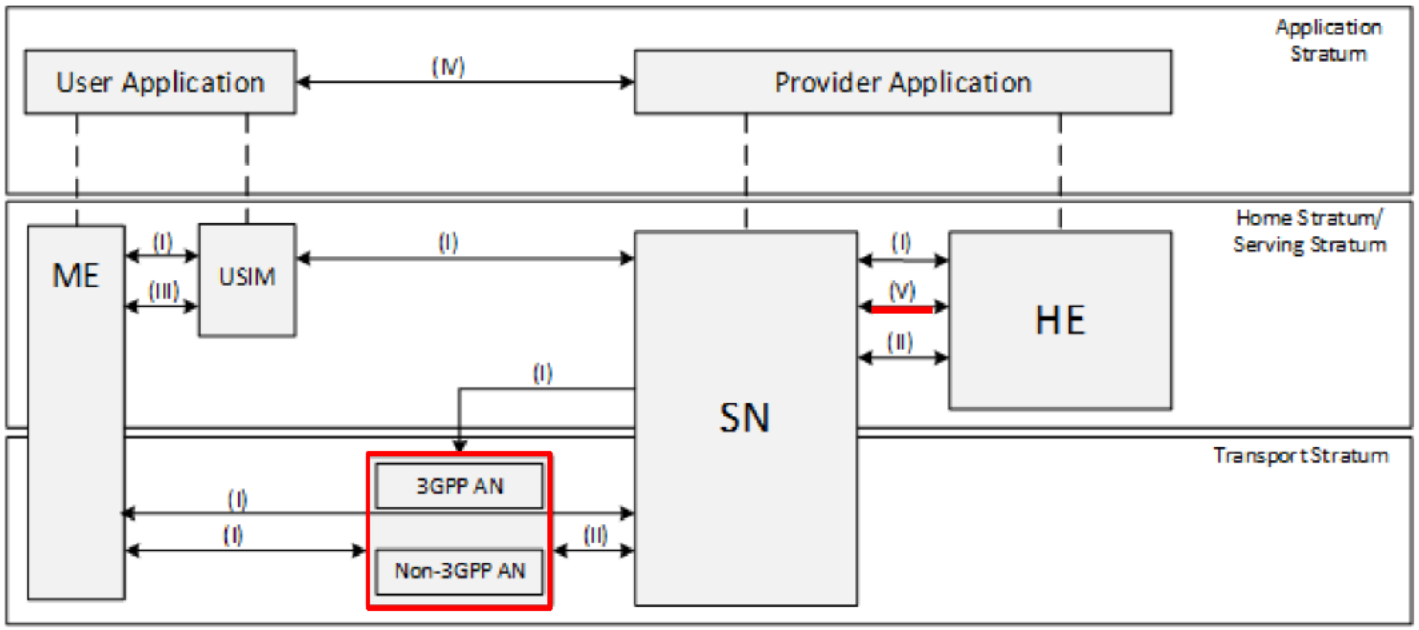
Security improvements in 5G

- Transition from centralized core and RAN to highly distributed, virtual network
- Addition of the Edge to the network
  - New and embedded security functionalities to ensure a highly secure mobile network, including:
    - Distributed Denial of Service (DDoS) detection and mitigation at the edge of the network to enhance the ability to respond to attacks and reduce potential broader network impact.
    - Stronger encryption for over-the-air interface and encryption of each device's IMSI to further secure device consumer specific information.
- A Security Edge Protection Proxy that will mitigate vulnerabilities in prior technology (e.g., SS7 and Diameter) and attacks when subscribers are roaming between different carriers' networks.
- In addition, wireless providers are increasingly deploying network components that are virtual instead of relying on the hardware of the past.
- As network operations are virtualized, through Network Functions Virtualization and Software Defined Networking, 5G's virtual and cloud-based network systems will allow for more adaptable security because they can be quickly adjusted, removed, or replaced using software, reducing the likelihood that an entire network would be impacted by a cyberattack.

5G Security Overview

- Increased home control
  - Authentication of device when roaming
  - Address vulnerabilities in 3G/4G around network spoofing and false signaling
- Unified Access Framework
  - Access agnostic authentication
- Security Anchor Function (SEAF)
  - SEAF allows for re-authentication of device as it moves between networks without full auth
- Subscriber Identifier Privacy
  - Subscriber Permanent Identifier (SUPI) and Subscriber Concealed Identifier (SUCI)
  - Prevents vulnerabilities during attach process

5G Security Architecture



Security Domains:

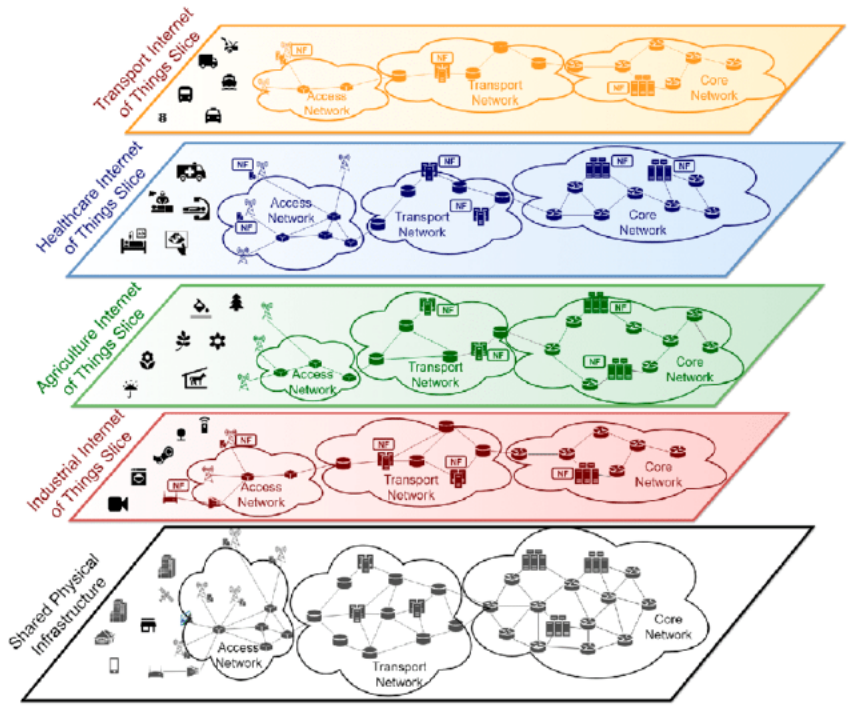
(I) Network Access Security
(II) Network Domain Security
(III) User Domain Security
(IV) Application domain security
(V) SBA domain security
(VI) Visibility and configurability of security

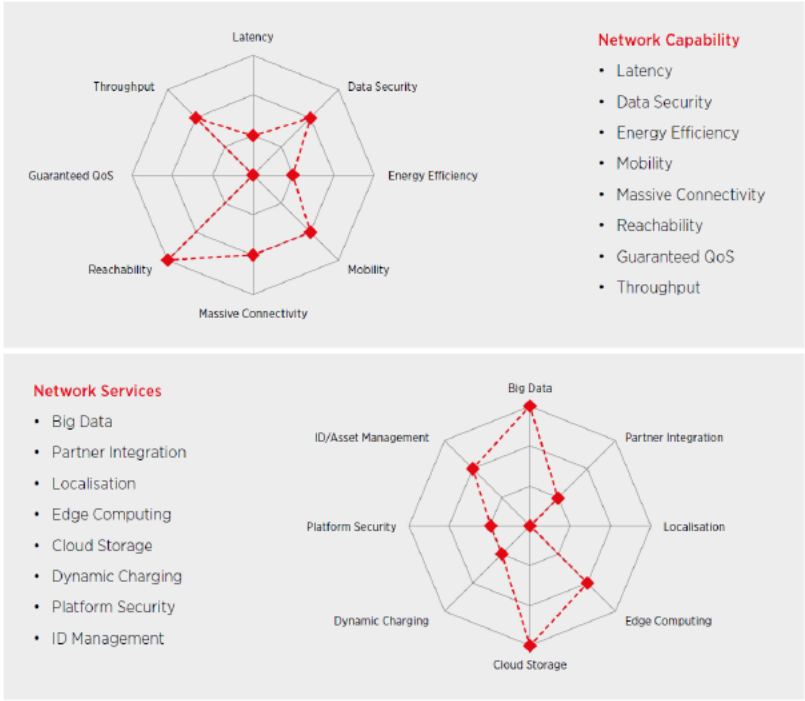
5G Network Security Solutions

- Network Virtualization
  - Network Slicing
  - Need based resourcing
  - Application-layer security
- Edge based Security
  - Authentication/Authorization
  - Threat Detection and Management

Network Virtualization

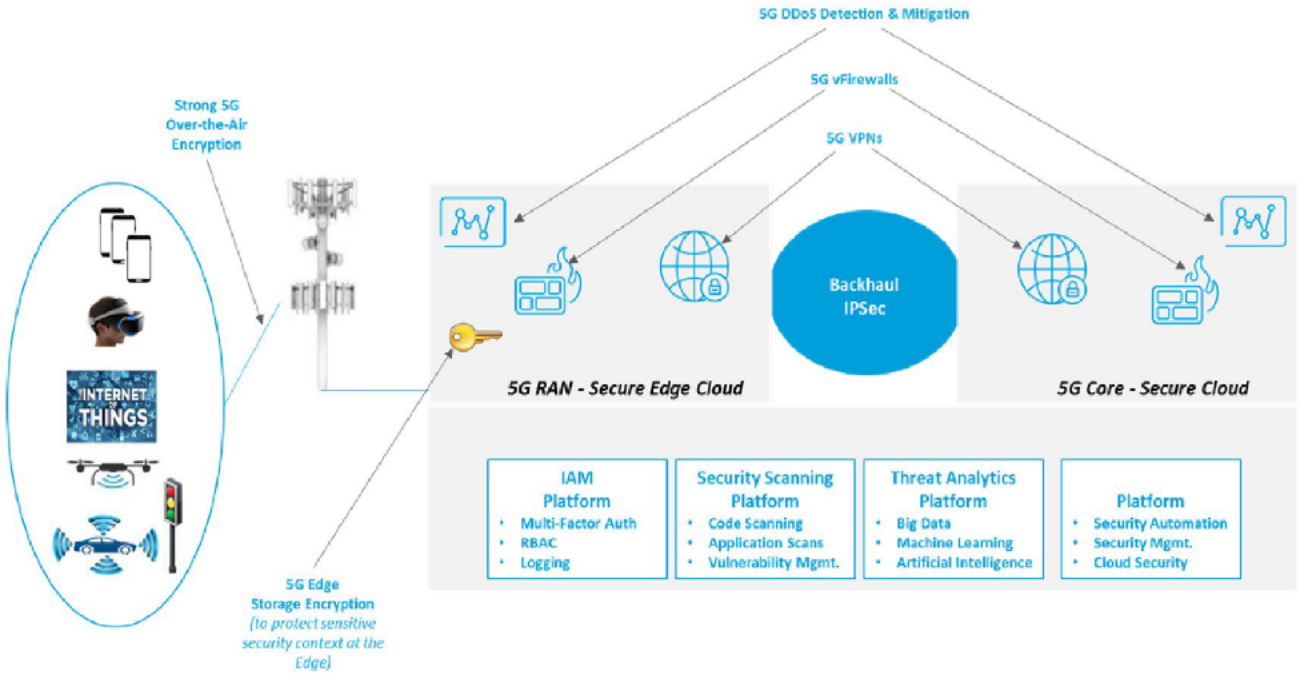
- A network slice is a complete logical network (providing Telecommunication Services and Network Capabilities) including Access Network (AN) and Core Network (CN)
- Security policy may drive slide definition and management
- Need based enablement of resources and capabilities



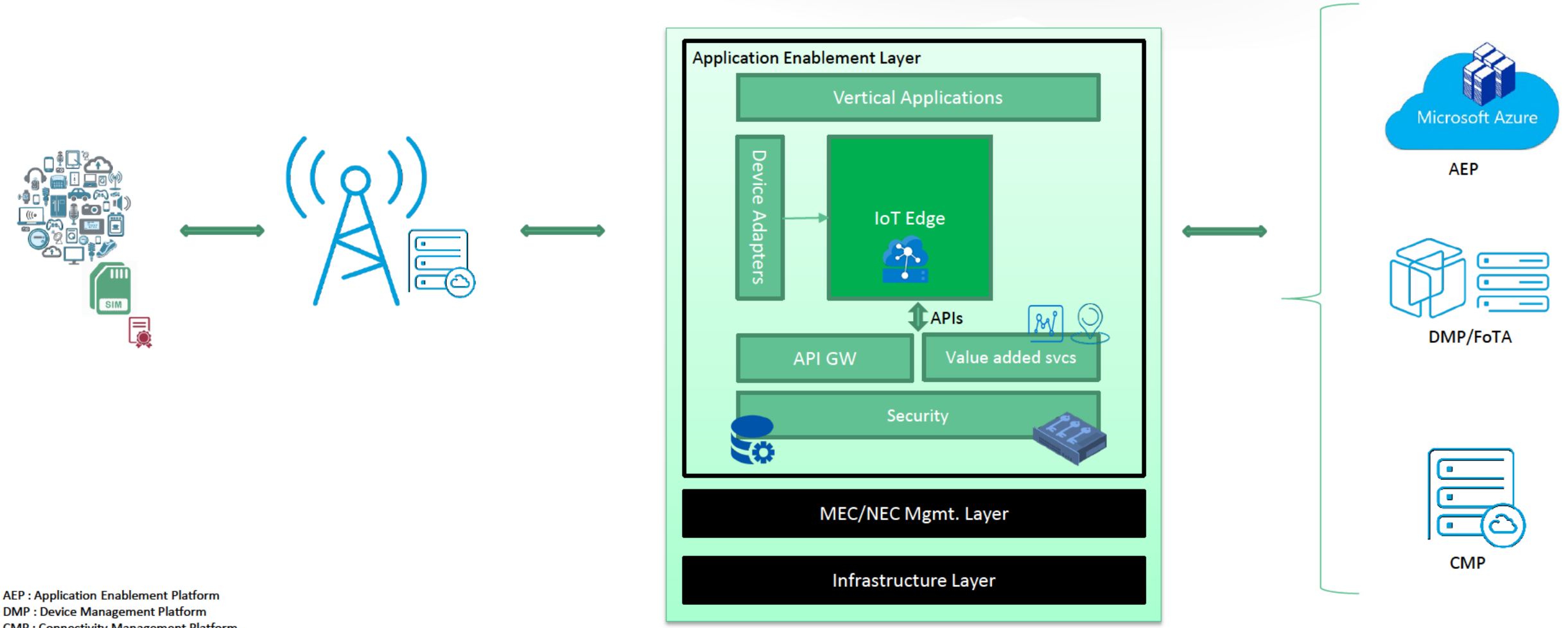


Security at the Edge

- De-centralization of the cloud is happening
  - Lower decision latency and action latency at Edge
- Multiple edge options based on IoT need
  - Mobile Edge Cloud (MEC)
  - Network Edge Cloud (NEC)
- Move device and cloud based security capabilities to the edge
  - Device Identity : Auth/AuthZ
  - Threat Detection : ML/AI based solutions



Security at the Edge



AEP : Application Enablement Platform
DMP : Device Management Platform
CMP : Connectivity Management Platform

Applying a Zero-trust security model with 5G

- 5G security capabilities allow enterprises to apply a zero-trust security model (ZTM) more easily
  - SDN allows for implementation of ZTM
  - Easier deployment and management
- Network slicing can enable limited resources for non-critical IoT deployments
  - Limit access to internal systems and applications
- Use the Edge to limit access to the backend
  - Move identity and auth services to edge and limit the perimeter

Using 5G Networks to secure IoT

	IoT	5G Solution
Device Volume	Very large volumes	• Independent IoT slices to handle large volumes and different device types • Use network slicing to manage needs and requirements • Small-cell based densification to allow larger volume
Device Types	Wide variety of custom devices	
Hardware/Software	Custom and varied	• Move on-device capabilities to MEC and NEC
Management and Control	Primarily unmanaged devices	• Move device management to the Edge • Edge based device auth/authz to minimize backend communication • Use network based solutions to manage application services
Applications/Backends	Fully custom	• Use Edge to deploy apps closer to the device to drive decision and action latency lower
Device Access	Both remote and public depending on IoT vertical	• Improved user plane security compared to LTE, Wi-Fi and other access technologies • Built-in e2e encryption to reduce overhead (computation and communication)
Risks	High risk for certain verticals	• Reduce risk by enabling network slicing • Reduce risk by enabling security capabilities on a need basis

5G & IoT Security Summary

- Virtualized, automated security controls. By now it is clear that the expanded surface area of a 5G network — including MEC and potentially compounded by the faster speeds of 5G — creates territory where automation can more efficiently be used to manage an environment. Automated remediation and virtualized security controls will help to equip enterprises to mitigate risks of the future.
- Machine learning and threat detection. 5G devices and MEC will generate a lot more activity on the network, which may dramatically increase the amount of data that security tools must analyze. Threat detection and threat intelligence will need to be informed by machine learning and other forms of artificial intelligence in order to keep pace.
- A zero-trust environment. If they are not implementing a zero trust approach to their environment, at the very least security practitioners should be considering a more sophisticated approach to identity and authorization. This is required for the number of devices involved and for the possibility that authorized users can inadvertently introduce malware to the network.
- A shared security model. Even though 5G offers some inherent security features, the enterprise must take responsibility for covering many aspects of security.

Next Steps and Take-aways

- Pre-planning Stage
  - Understand the significant differences of an IoT deployment
  - Identify the security gaps and risks
  - Understand the new security capabilities that 5G has to offer
- Architecture Stage
  - Identify the security needs for your IoT deployment
    - Network Capabilities
    - Security needs
  - Perform a risk assessment and choose acceptable risk level
  - Incorporate the new 5G security capabilities into your design
- Deployment and later stages
  - Continue to manage the security needs of your IoT deployment
    - 5G network based policy
  - Continued testing and capability enhancement