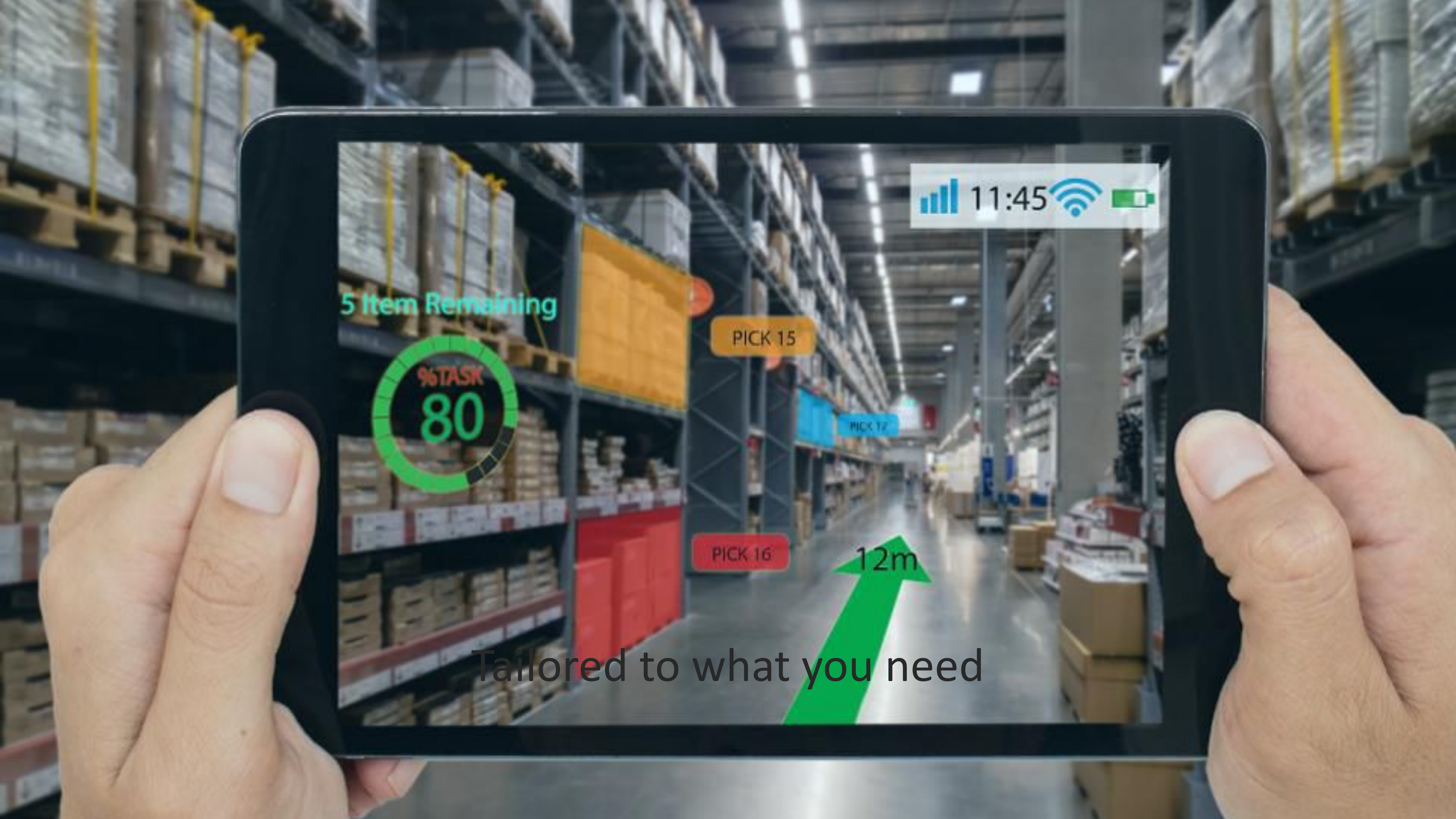
# Applying Security in A 5G World

Peter Romness
Cybersecurity Solutions Lead
US Public Sector CTO Office

From Material by:

Mike Geller & Pramod Nair



Tailored to what you need

# Security Challenges in 5G & evolving architectures

| | |
|---|---|
| **IoT & M2M** | • Weak inbuilt security in IoT devices, peer to peer attacks |
| **Virtualization** | • Increased complexity in mitigating side channel attacks and securing cloud native architectures |
| **Distributed Architectures** | • Increased threat vectors due to distributed DC, edge computing and Network slicing |
| **New and Legacy Technologies** | • Multiple Technology convergence, threat migration between technologies |

# Threats in 5G and evolving architectures

RAN

MEC & Backhaul

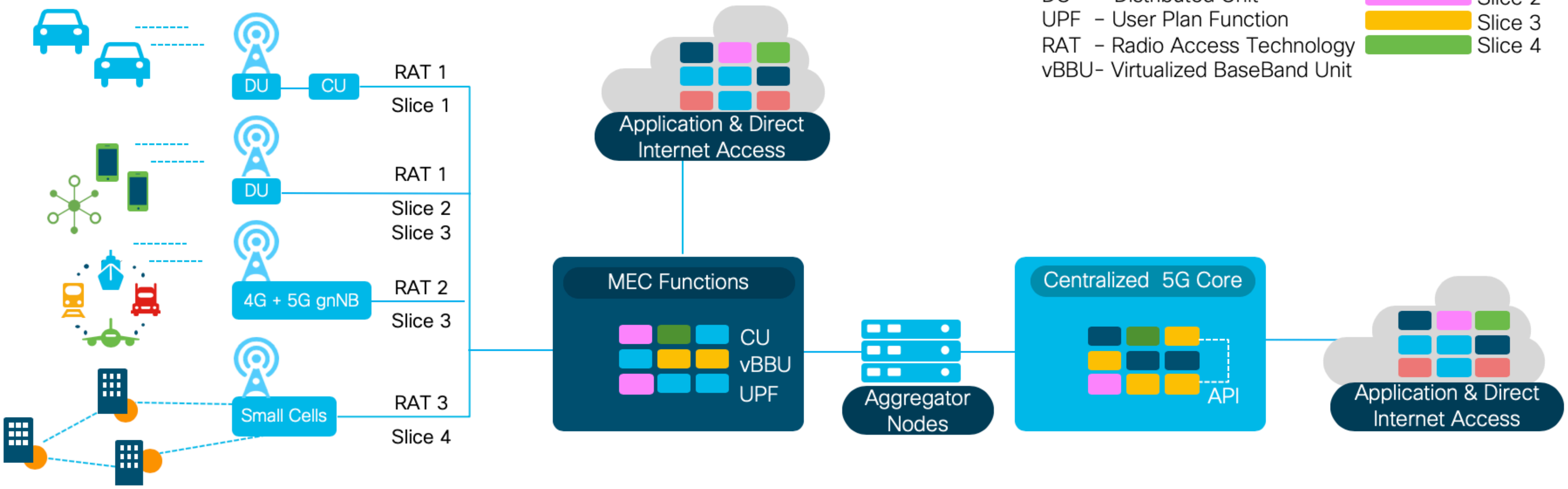
5G Packet Core & OEM

Air interface

IoT and M2M

Convergence (4G-5G-wired)

# Threats in 5G & Evolving Architectures



CU - Centralized Unit
DU - Distributed Unit
UPF - User Plan Function
RAT - Radio Access Technology
vBBU- Virtualized BaseBand Unit

🟦 Slice 1
🟪 Slice 2
🟨 Slice 3
🟩 Slice 4

### Device Threats

- Malware
- Bots DDoS
- Firmware Hacks
- Device Tampering
- Sensor Susceptibility
- TFTP MitM attacks

### Air Interface Threats

- MitM attack
- Jamming

### RAN Threats

- Rogue Nodes
- Insecure S1, X2
- Insecure Xx, Xn

### MEC & Backhaul Threats

- DDoS attacks
- LI Vulnerabilities
- Insecure Sx
- Insecure N6
- CP / UP Sniffing
- MEC Backhaul sniff
- Side Channel attacks
- NFVi Vulnerabilities

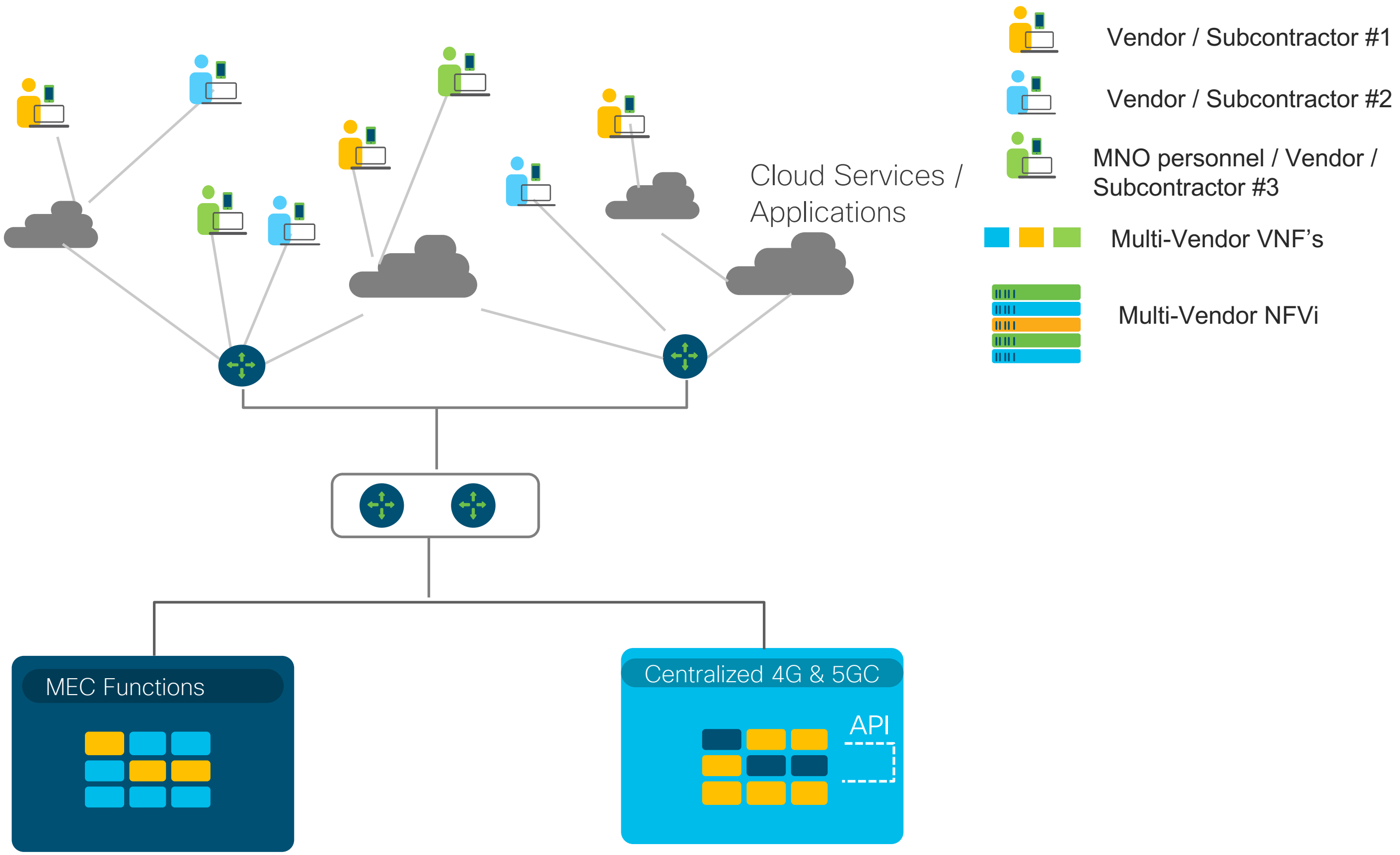
### 5G Packet Core & OAM Threats

- Virtualisation
- LI Vulnerabilities
- Improper Access Control
- Network Slice security
- API vulnerabilities
- IoT Core integration
- Roaming Partner
- DDoS & DoS attacks

### SGi / N6 & External Roaming Threats

- IoT Core integration
- VAS integration
- App server vulnerabilities
- Application vulnerabilities
- API vulnerabilities

Problem | Multiple NFVi / NF Vendors, Contractors, Sub-contractors, employees accessing the network during configuration



Cloud Services / Applications

MEC Functions

Centralized 4G & 5GC

API

Vendor / Subcontractor #1

Vendor / Subcontractor #2

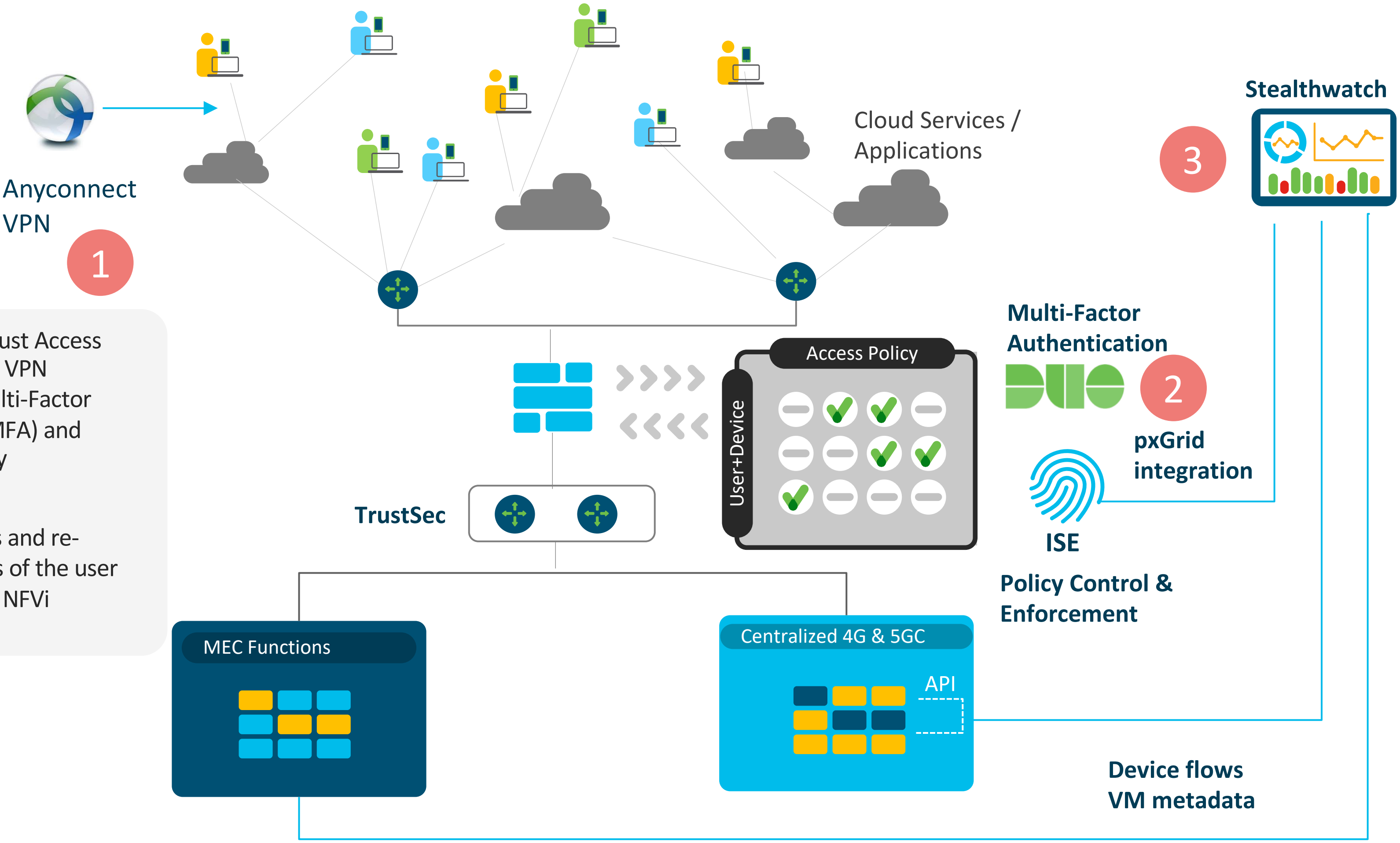
MNO personnel / Vendor / Subcontractor #3

Multi-Vendor VNF’s

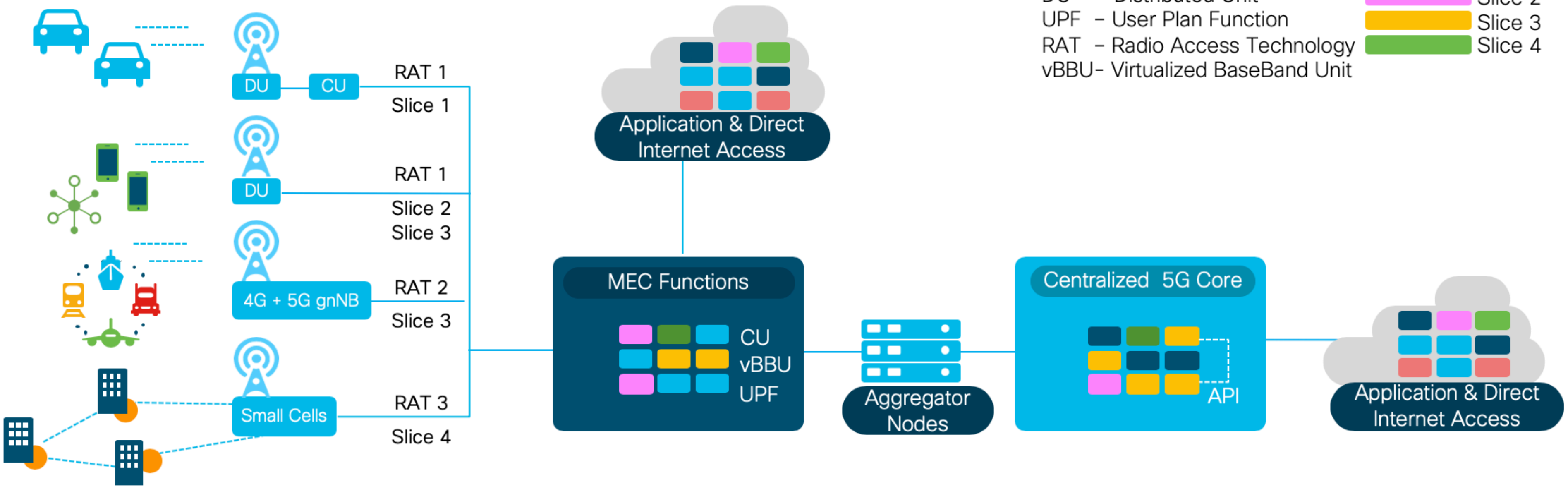
Multi-Vendor NFVi

Solution | Zero Trust Access Security based on VPN (Anyconnect), Multi-Factor Authentication (MFA) and enhanced visibility (Stealthwatch)

Benefits | Verifies and re-verifies the access of the user to specific VNF or NFVi



# End to End Threats Mitigation



CU - Centralized Unit
DU - Distributed Unit
UPF - User Plan Function
RAT - Radio Access Technology
vBBU- Virtualized BaseBand Unit

Device Threats

Air Interface Threats

RAN Threats

Backhaul / Remote DC Threats

5G Packet Core & OAM Threats

SGi / N6 & External Roaming Threats

Enhanced Visibility & Threat detection Layer — Stealthwatch

DNS Protection Layer — Umbrella

Application Protection & Policy enforcement — Tetration, Radware

NGFW & DDoS protection Layer — Firepower, Radware

Segmentation & Isolation Layer — ISE, Duo

Advanced Malware Protection Layer — AMP

# Key Takeaways

- 5G deployment will see greater number of users (vendors, sub contractors etc) trying to access the network, Cisco recommends to use the Zero trust based access security to better control the access of users to prevent any malicious attacks
- Low inbuilt security in the IoT network components require security layers to be included in the choke  points such as Segmentation in the IoT Slice, IoT Application security and securing the IoT device  controller
- MEC & CUPS exposes the Packet Core to multi vector threat surfaces and the mitigation should include  multiple layers of security
- Evolving architectures should follow the best practices of yesterday, today and tomorrow

# 5G Security – Reference5G Americas, ATIS, CSRIC/FCC, 3GPP

- 5G Americas White Papers – Mike Geller, Lead Editor
  - 5G Security v1:
    - https://www.5gamericas.org/the-evolution-of-security-in-5g/
  - 5G Security v2 – Network Slice focused:
    - https://www.5gamericas.org/the-evolution-of-security-in-5g-2/
- 5G Security Innovation with Cisco – Authors: Mike Geller & Pramod Nair
  - https://www.cisco.com/c/dam/en/us/products/collateral/security/5g-security-innov-wp.pdf
- Reimagining the Mobile Network in the 5G Era
  - https://www.cisco.com/c/dam/en/us/solutions/service-provider/mobile-internet/pdfs/reimagining-mobile-network-white-paper.pdf

# Thank you

You make **possible**