

An aerial view of a city skyline, likely New York City, with a prominent green overlay. The green overlay is a semi-transparent rectangle that covers the central and right portions of the image. The text is white and centered within the green area.

# SECURITY STRATEGY IN 5G

## Key Considerations

**Sriram T V**

**JUNIPER**  
NETWORKS

Engineering  
Simplicity



# AGENDA

---

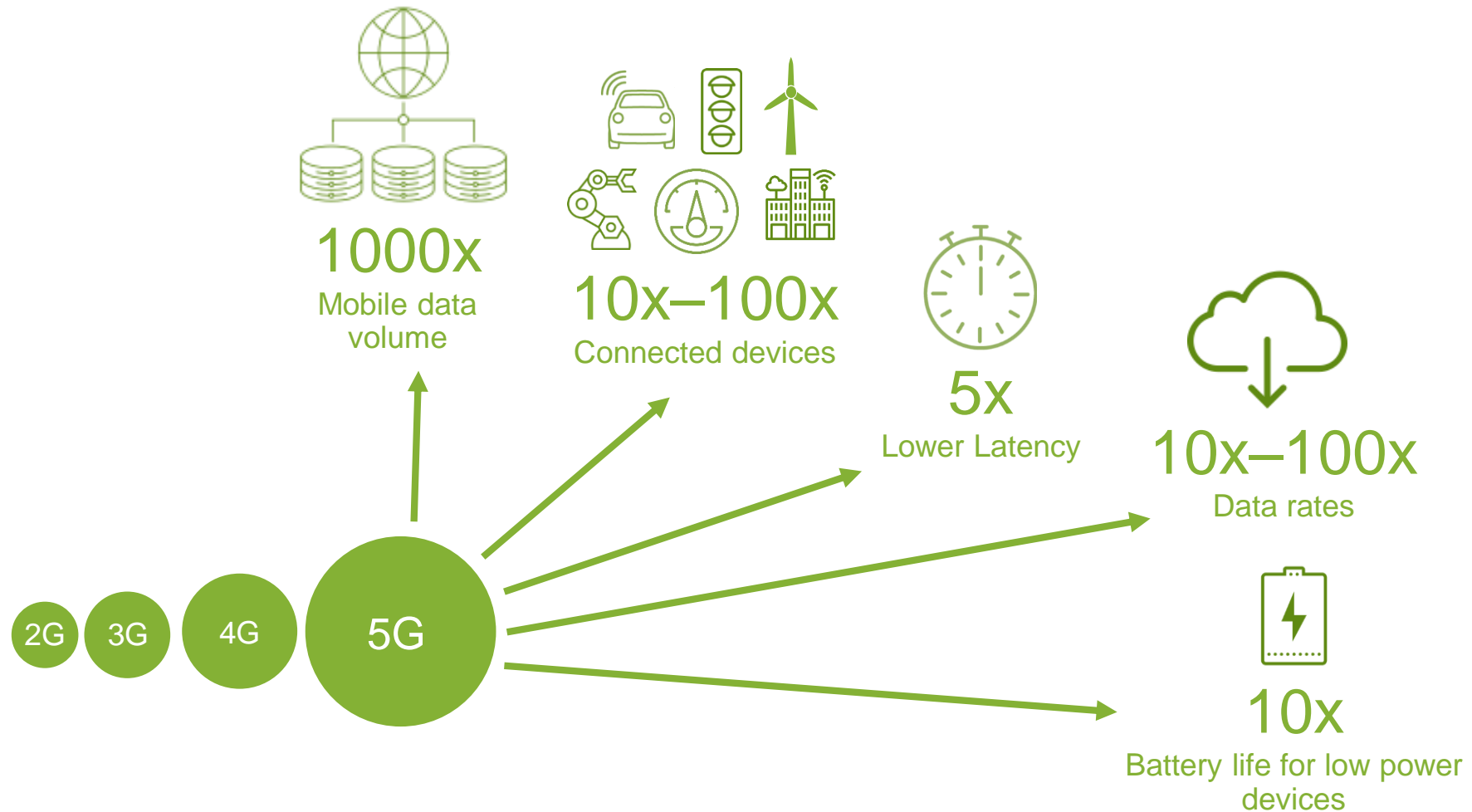
- **What's new in 5G ?**
- **Implications on Security**
- **Juniper Approach**
- **Summary**



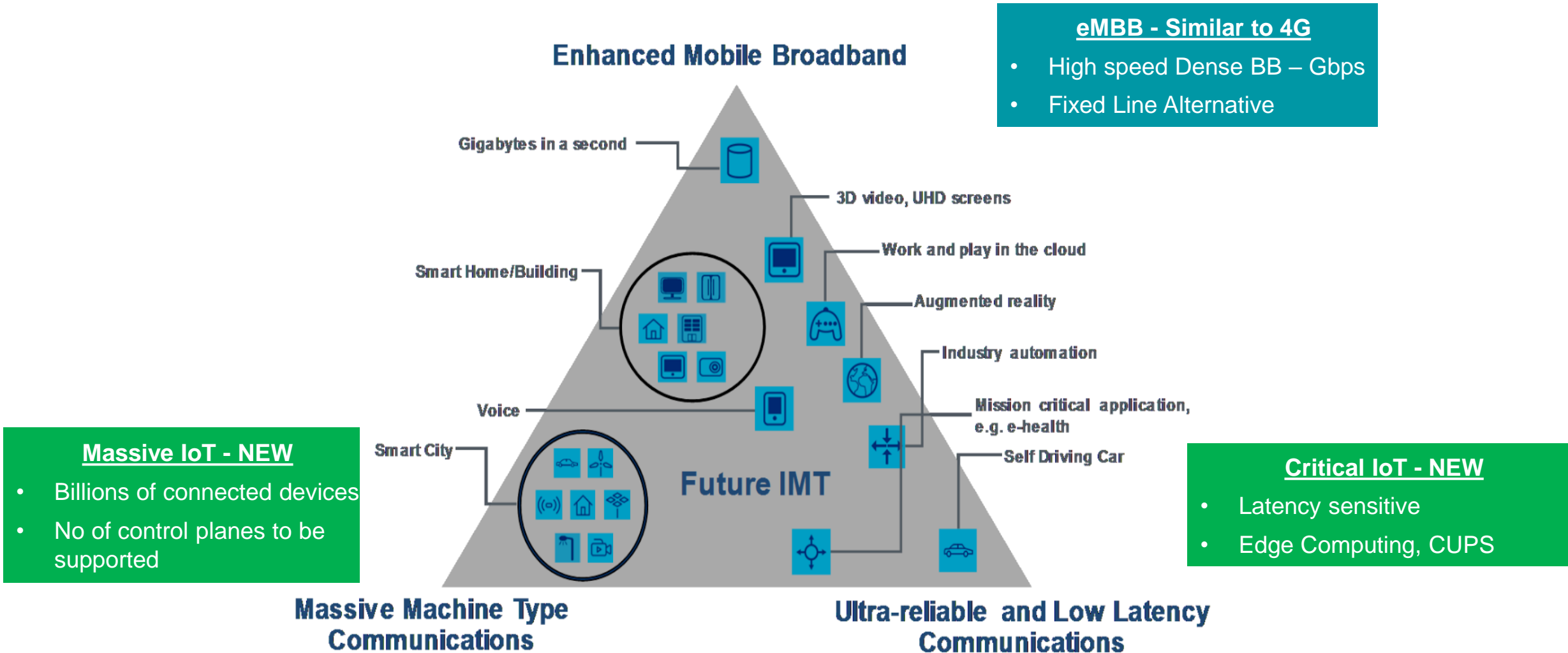


## 5G – What's new

# 1. AMBITIOUS GOALS

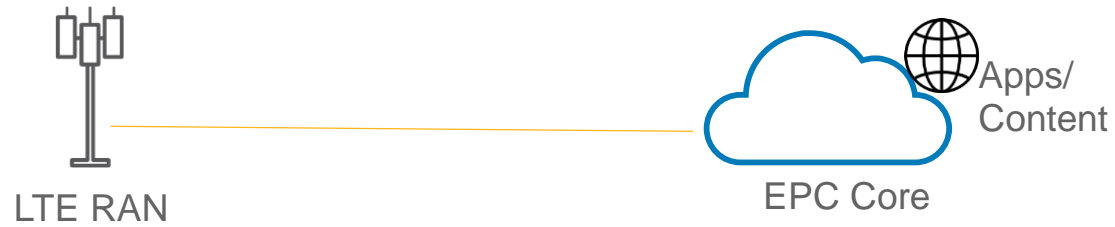


## 2. USE CASES

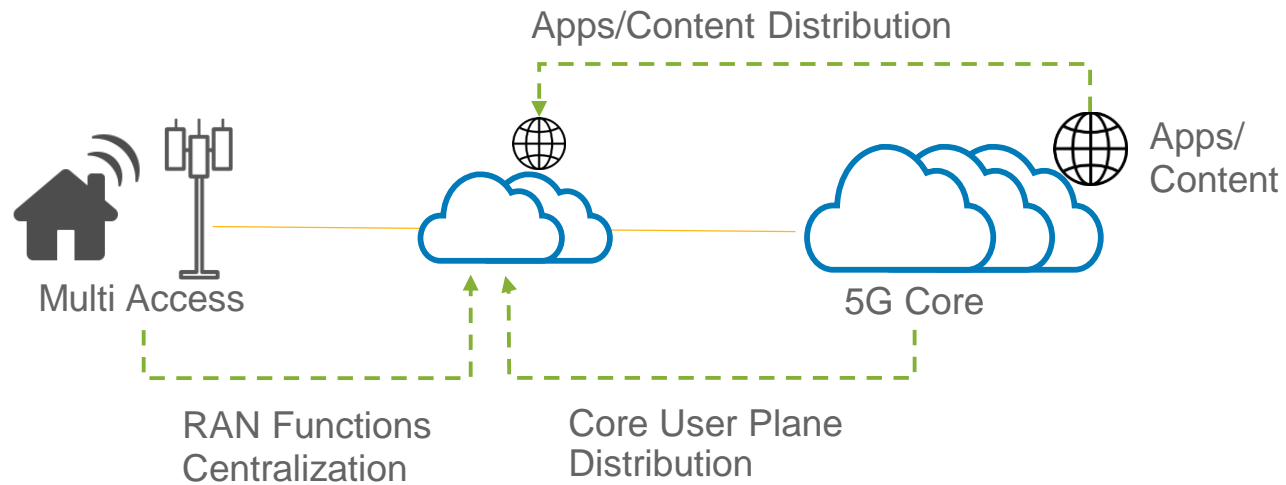


# 3. ARCHITECTURE EVOLUTION

## 4G Networks



## 5G Networks



### Centralized RAN

- BBU – centralized in DC
- RRU – scaled independently

### EPC

- Bandwidth & Latency
- Distributed user plane



## Implications on Security

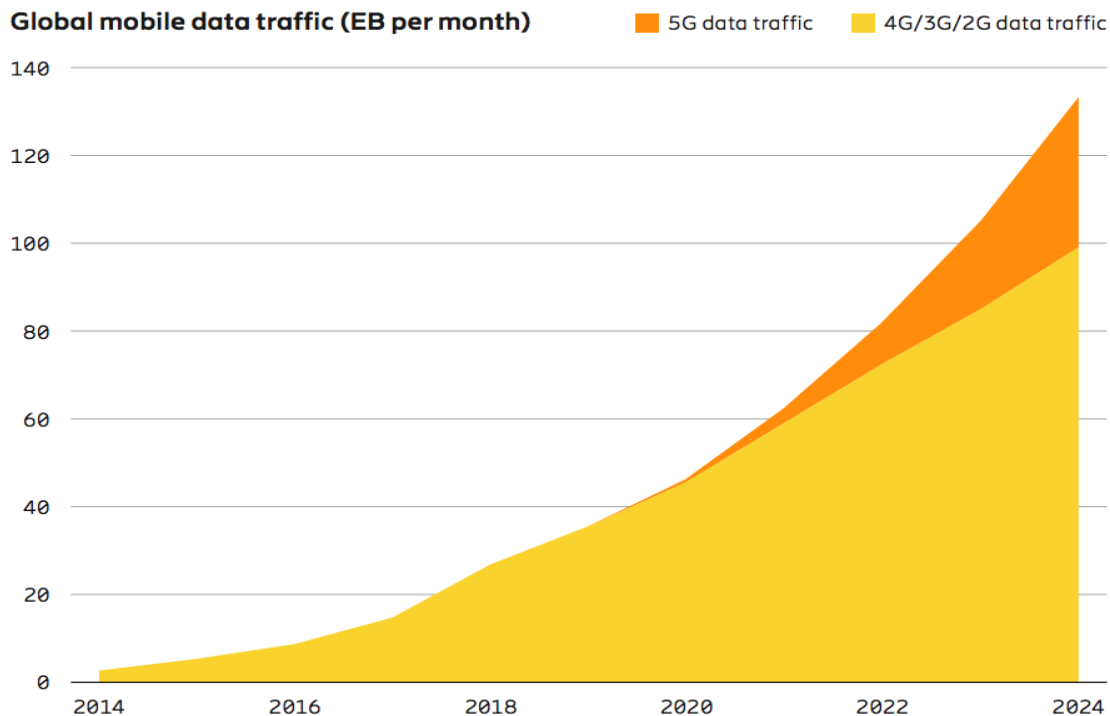
---

## *Implication #1:*

**Scale up & Scale out of Security Performance & Security Operations (SecOps)**



# TRAFFIC GROWTH DRIVES THE NEED FOR SCALING SECURITY



Source: Ericsson Mobility Report

- Data traffic – 25% in 5G & rest across 4G/3G/3G networks
- Security requirements doubling every 2 years
- Performance Vs Security trade off

## Gi Firewall

Requirement	2018	2020	2022
IMIX throughput (Gbps)	300-600	600-1,200	1,200-2,400
CPS (M)	1	2	4
Session count (M)	100	200	400

## Security Gateway

Requirement	2018	2020	2022
IMIX throughput (Gbps)	100	200	400
Tunnels per second (TPS)	250	500	1000
Tunnel count (K)	50	100	200

# TERABIT-SCALE DDOS ATTACKS FUELED BY IOT BOTNETS

## - THE NEW NORMAL

### World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices

September 28, 2016



Name	Date	Type of affected devices	Type of compromise	Number of affected hosts*
Mirai	October 2016	Routers, DVRs, CCTV cameras, printers, & more	Default/hard-coded passwords	500,000
Persirai	April 2017	IP cameras	SSDP, web	10,000-30,000
Reaper/IoTroop	October 2017	IP cameras, routers	Exploit	1 million



Cloud Data Center

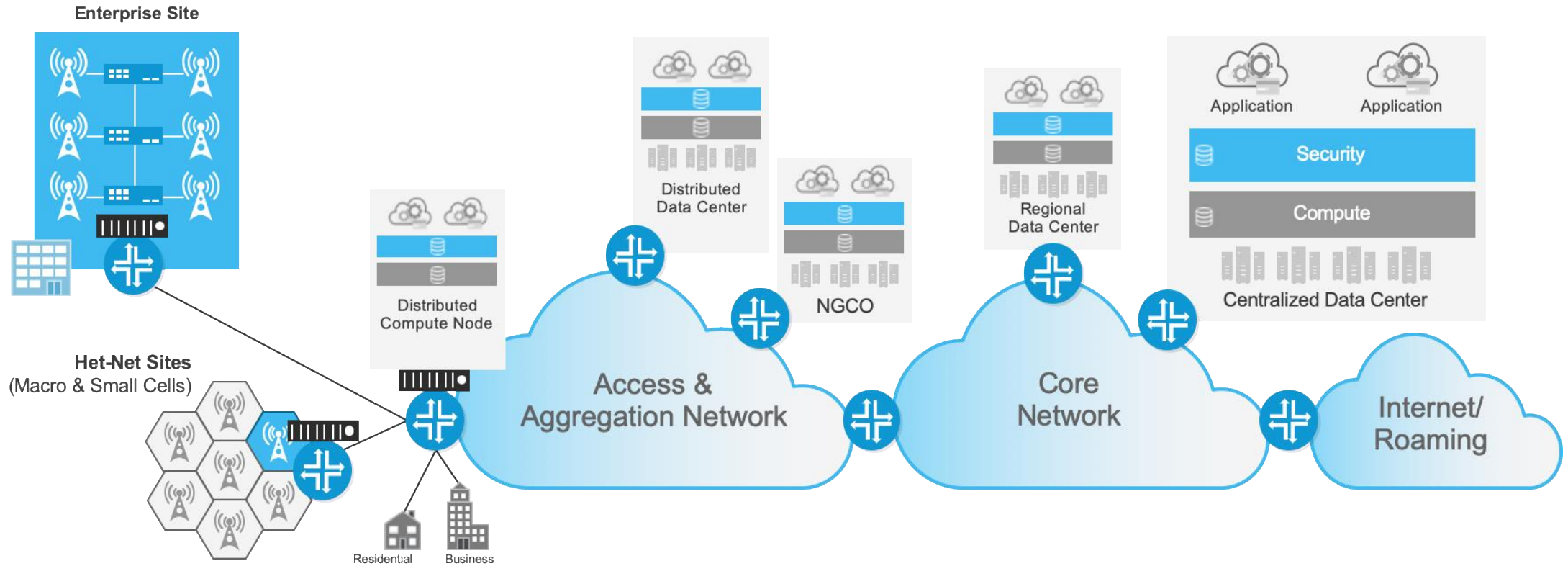


**Out of Resources  
Service Offline**

### New vicious Torii IoT botnet discovered

Move over, Mirai. There's a new, much more sophisticated Internet of Things botnet boss. The Torii IoT botnet has advanced techniques and persistence methods.

# VIRTUAL SECURITY – NOW MUST-HAVE SECURING DISTRIBUTED CLOUD



- Virtual security for Distributed Telco Cloud to protect VNFs
- Unified Security Management for SecOps – manage VNFs & PNFs, automate policy enforcement, provide holistic system-wide visibility

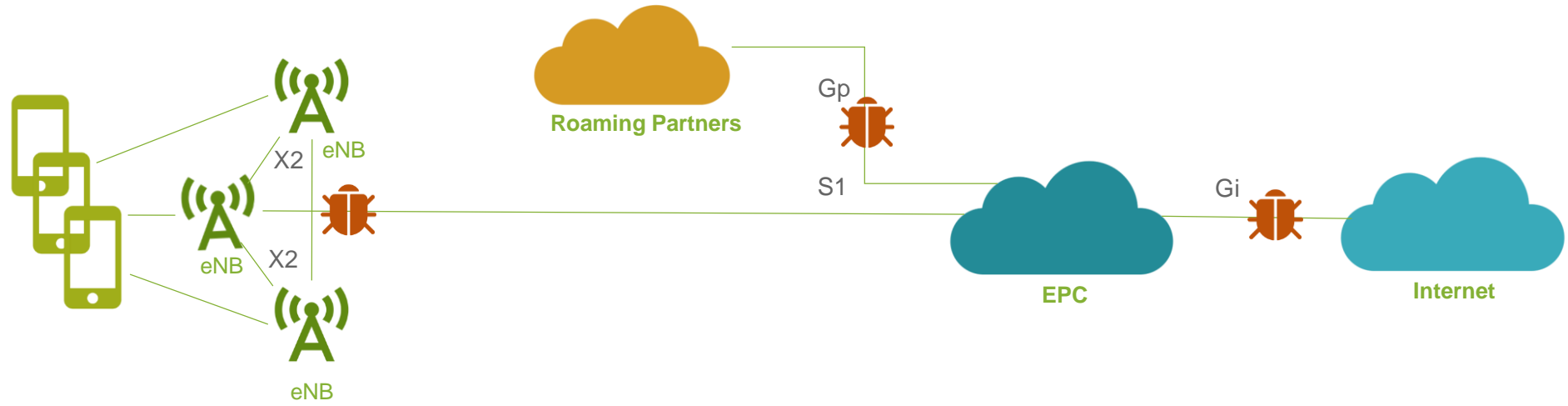
---

**Implication #2:**

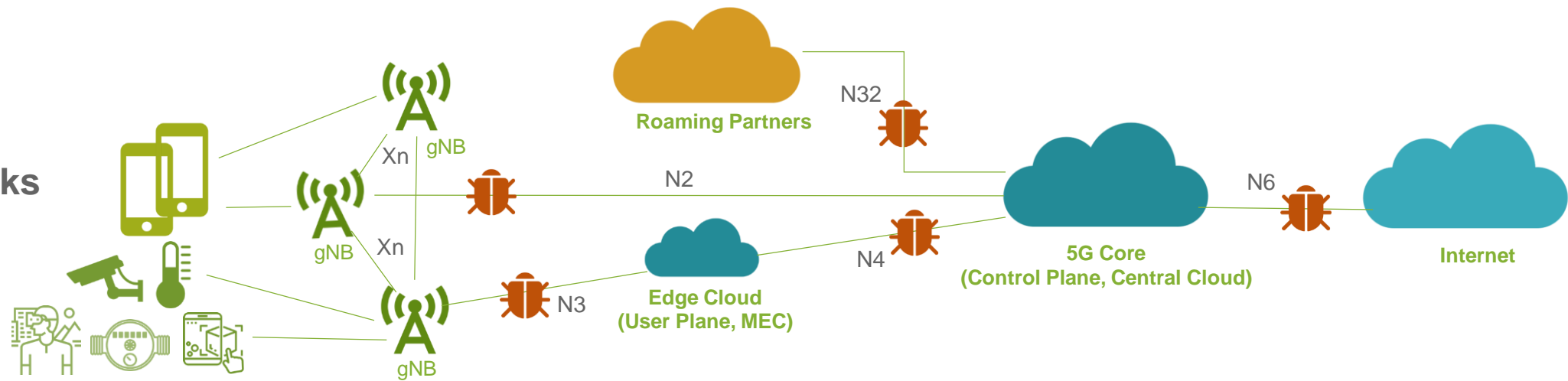
**Network Architecture Evolution and New Enabling Technologies Open Up New Vulnerabilities**

# NEW ARCHITECTURE BRINGS IN NEW VULNERABILITIES

4G Networks



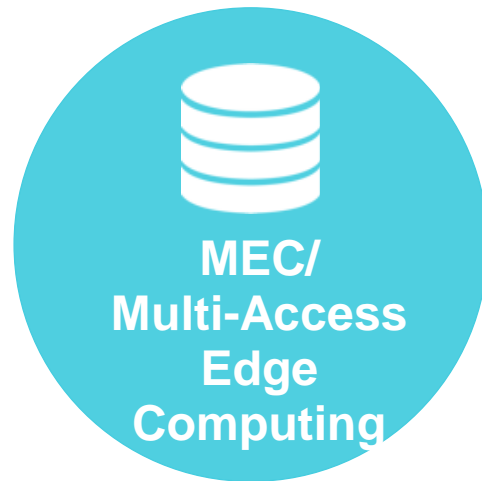
5G Networks



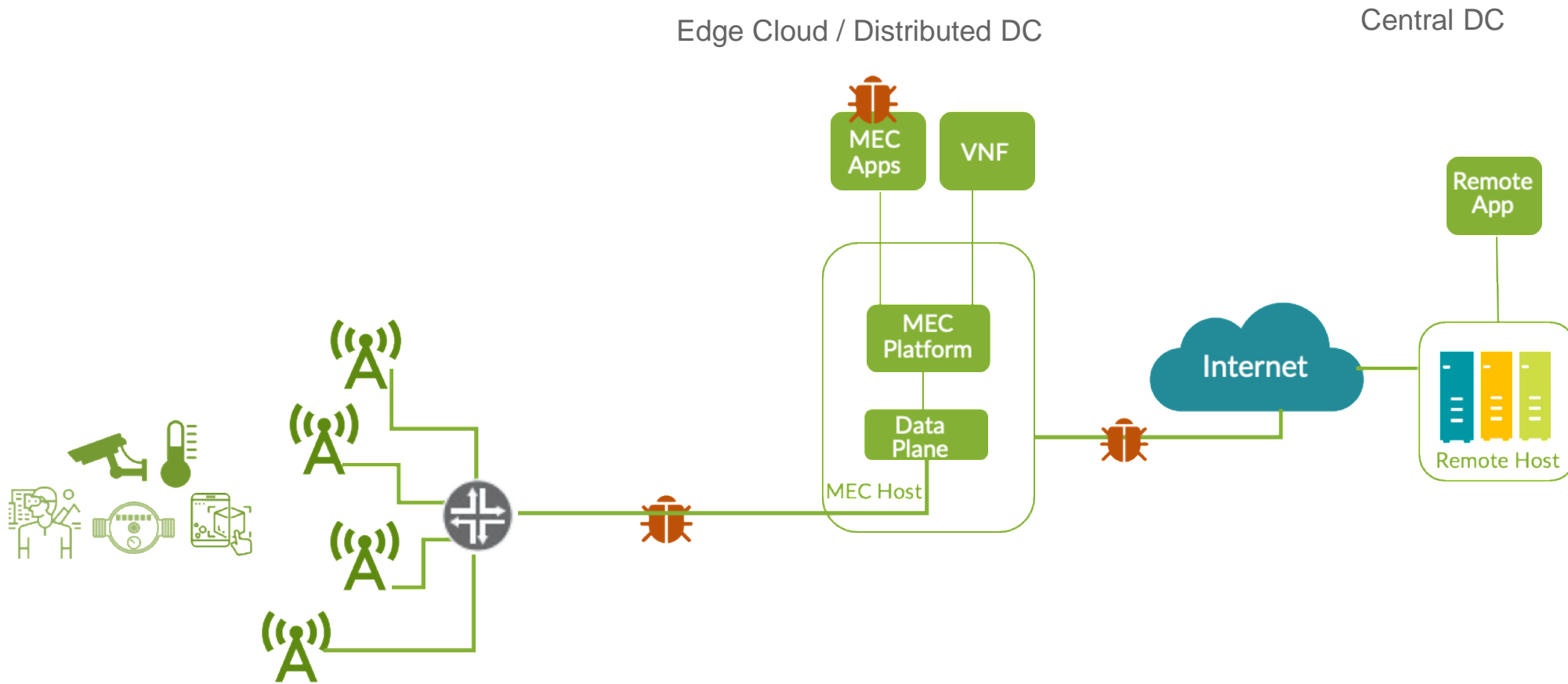


# NEW ENABLING TECHNOLOGIES ALSO BRING NEW ATTACK SURFACES

---

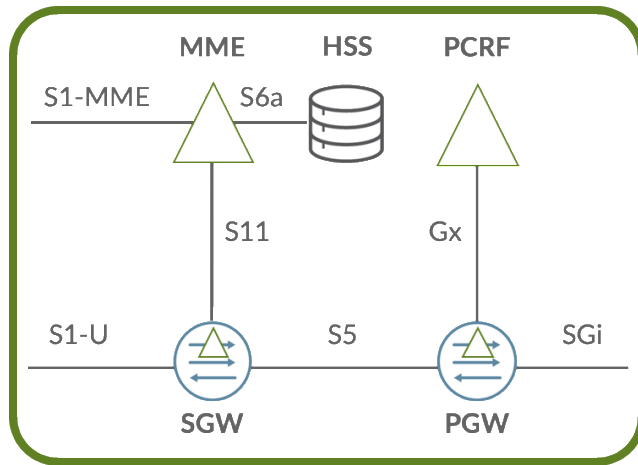


# EDGE COMPUTING ATTACK SURFACES

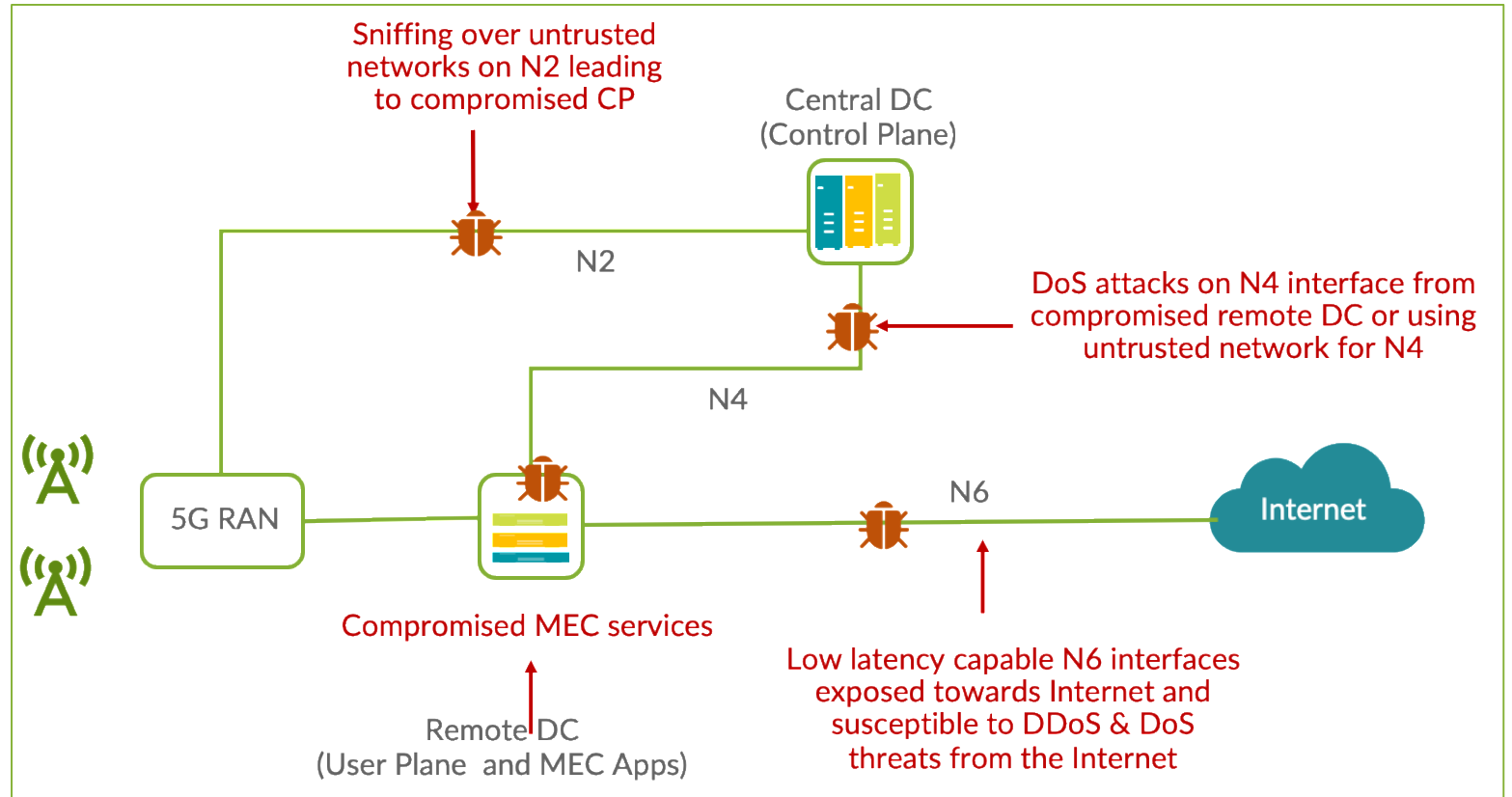
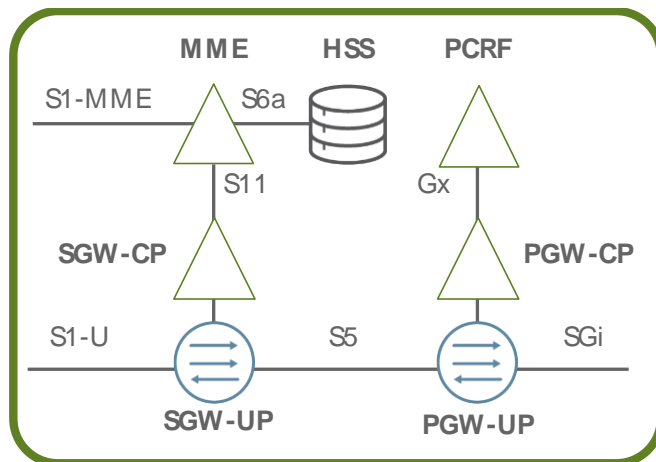


# DISTRIBUTED CORE ATTACK SURFACES

**EPC today**

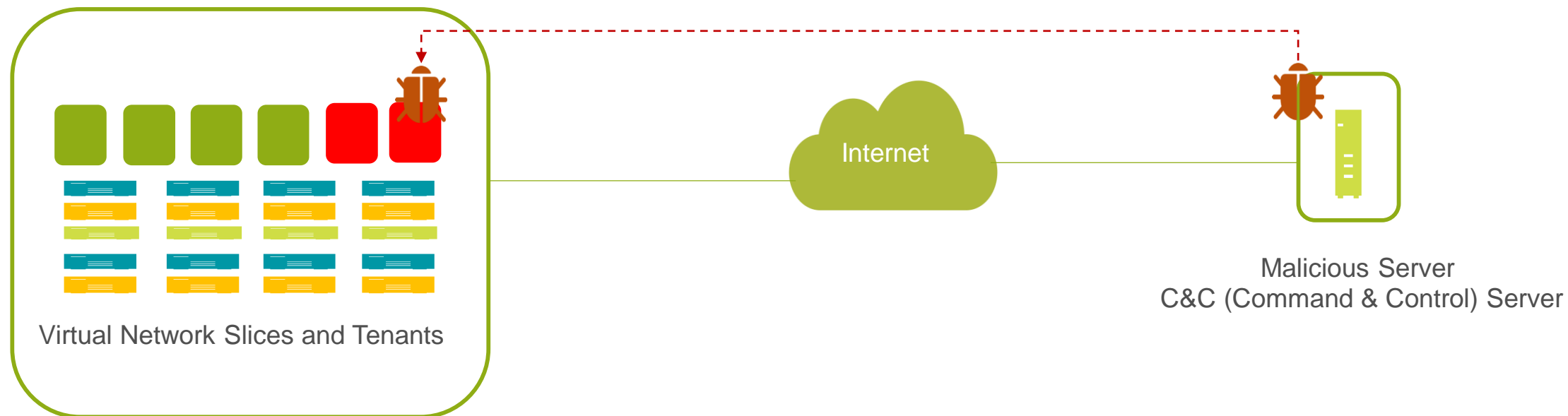


**After CUPS**



All new interfaces between the Control Plane (CP) & User Plane (UP) are new attack surfaces

# NETWORK SLICE EXHAUST ATTACK SCENARIO



- Vulnerable slices with lower security can be exhausted
- Denial of Service (DoS) vulnerability for other slices

- Baseline security to cater for all slices is critical
- Adequate isolation between slices for limiting the threat

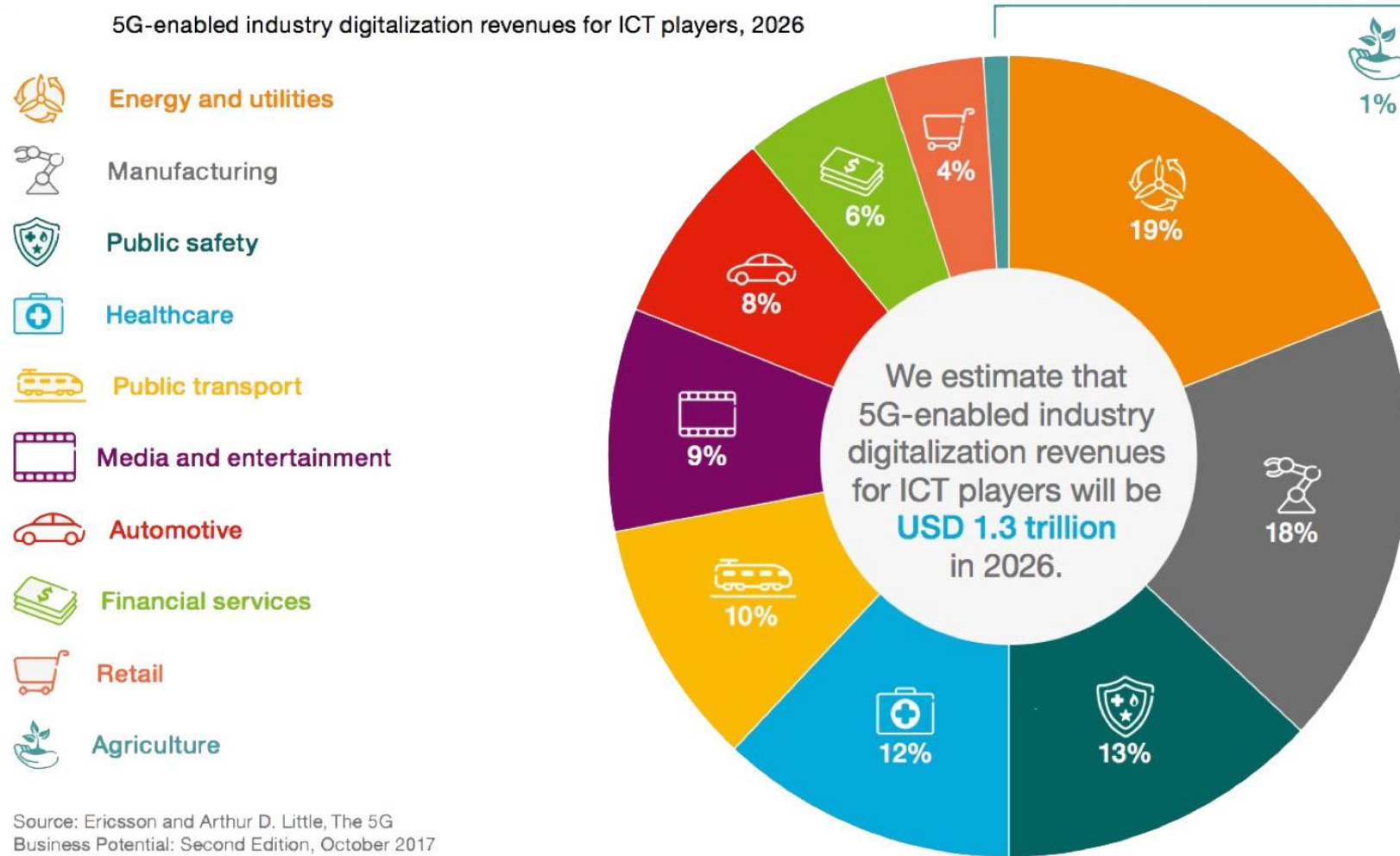
---

**Implication #3:**

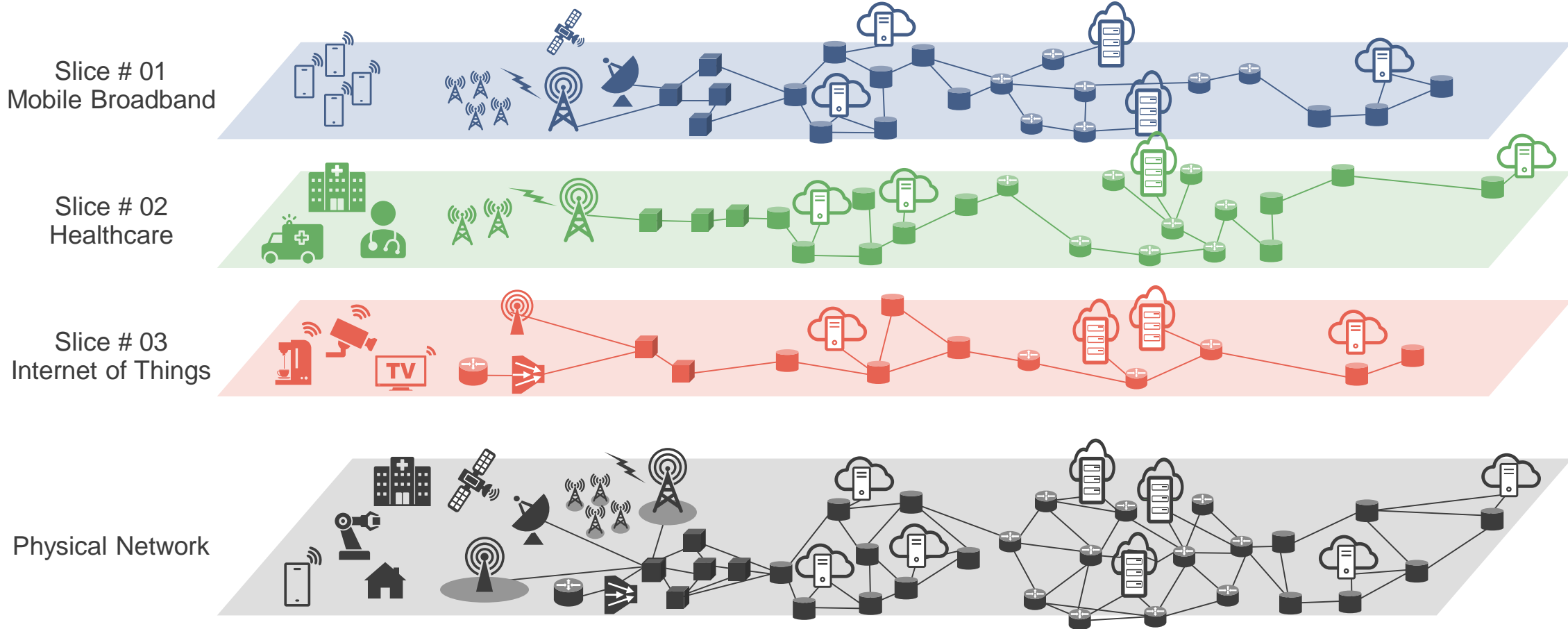
**Security is An Essential Enabler for New Revenue Opportunities in 5G and IoT**



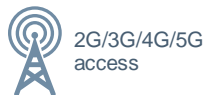
# 5G-ENABLED INDUSTRY REVENUE OPPORTUNITY IS HUGE



# NETWORK SLICING HOLDS THE PROMISE FOR SERVING DIVERSE VERTICALS AND SECURITY NEEDS TO SUPPORT



WiMAX  
access



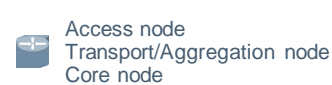
2G/3G/4G/5G  
access



Satellite  
access



xDSL/Cable  
access



Access node  
Transport/Aggregation node  
Core node

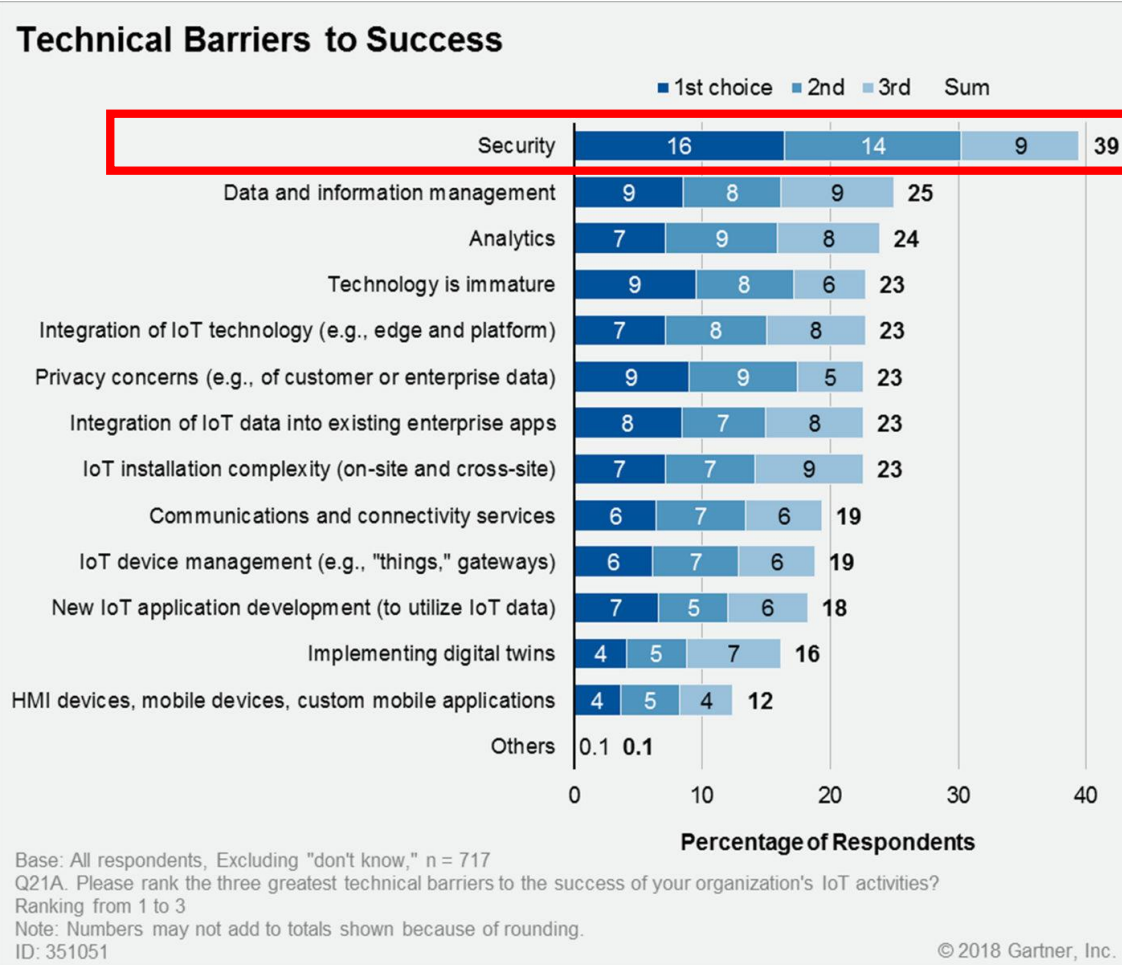


Edge  
Cloud



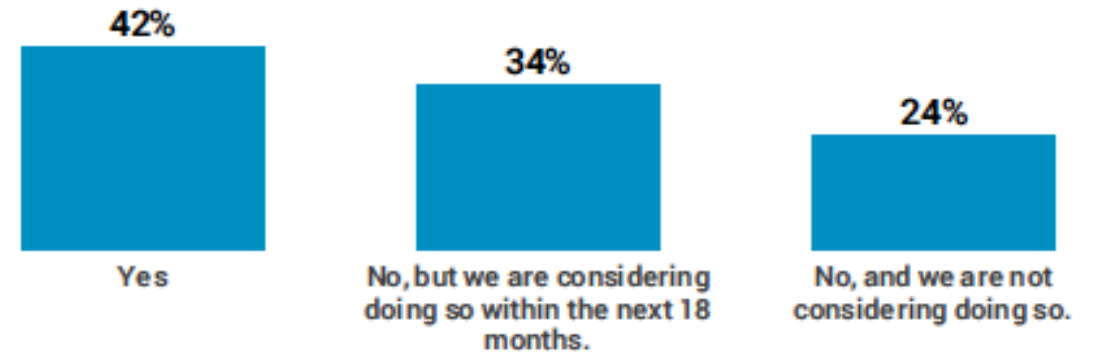
Core  
Cloud

# SECURITY IS ESSENTIAL FOR SP IOT VALUE PROPOSITION



## Market Insight: Security Is Essential to a Successful CSP IoT Value Proposition

Are you currently using managed security services?



Source: IoT Institute Survey Research

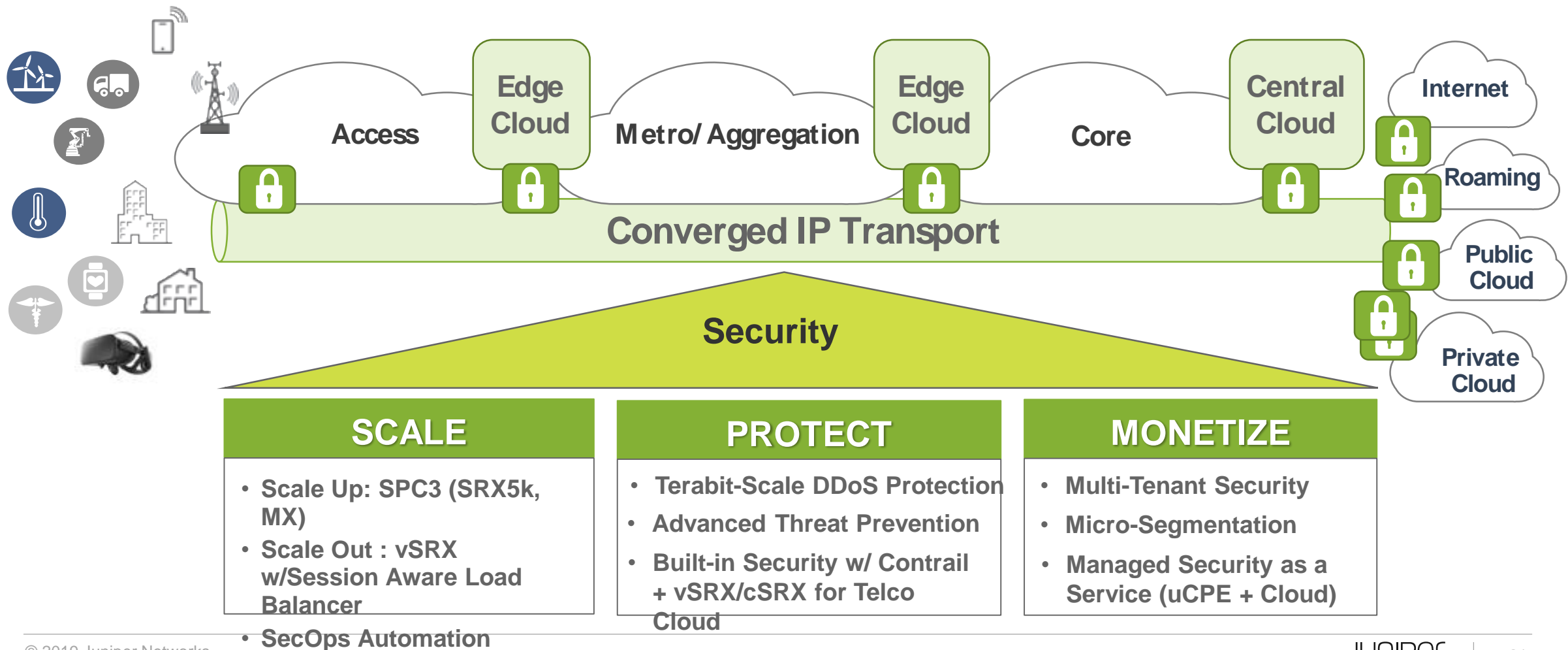
Base = Respondents with direct involvement in IoT Security (n=176).



# Juniper Approach

# SECURE. AUTOMATED. CLOUD.

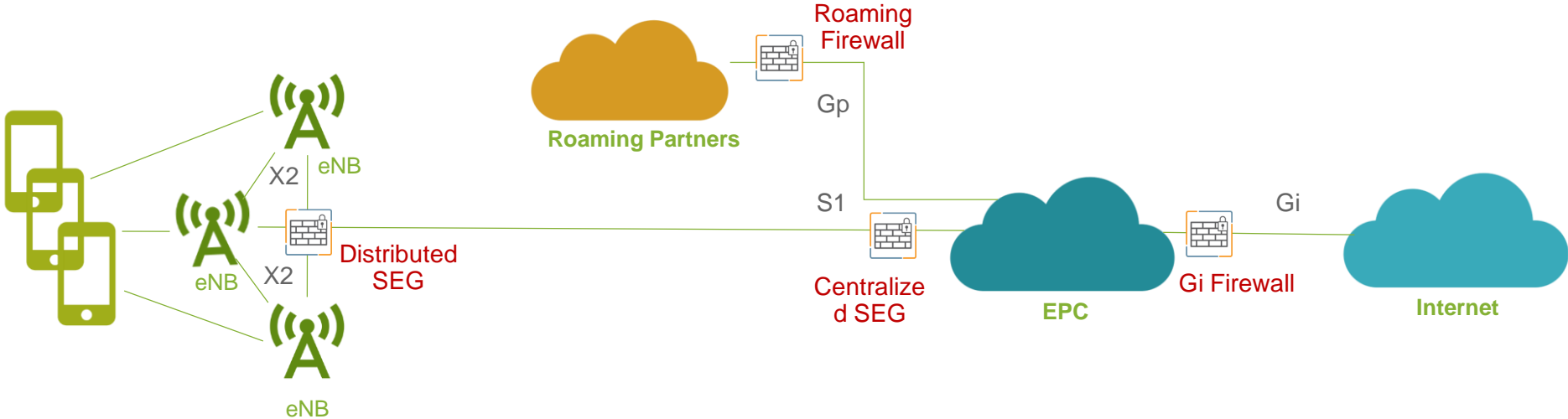
Juniper strategy for SP



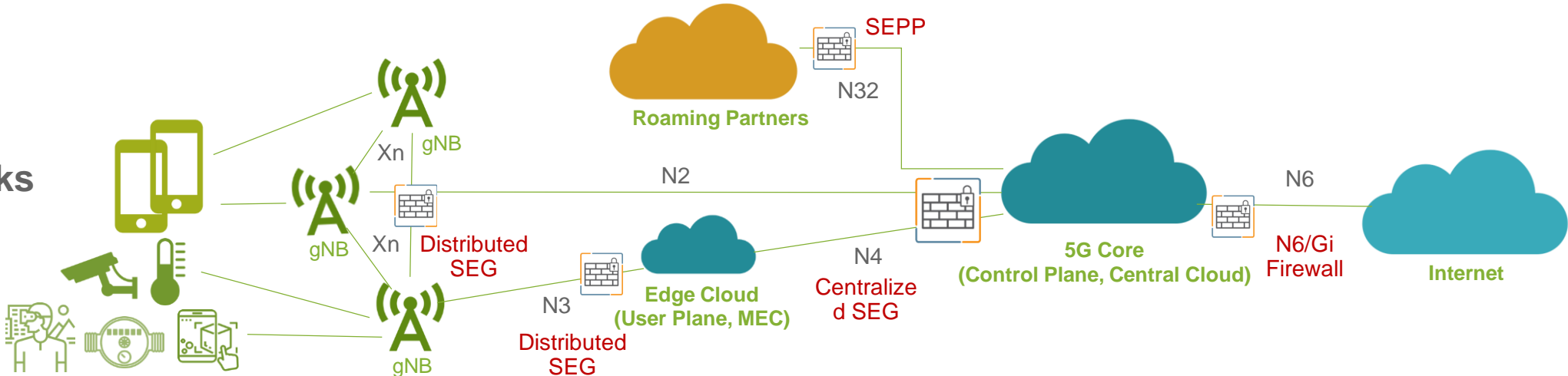


# SECURING MOBILE NETWORK (4G & 5G) INTERFACES

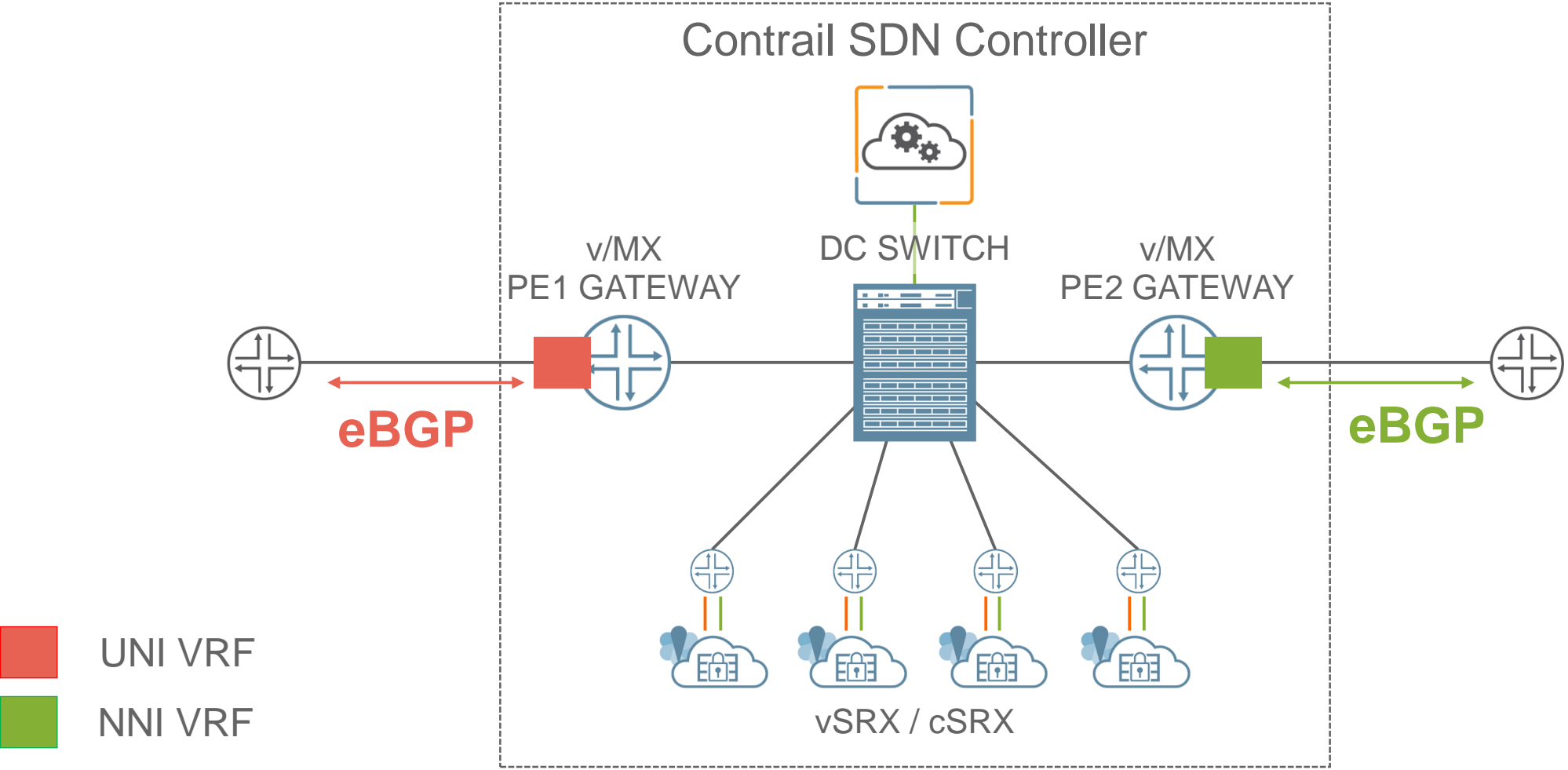
4G Networks



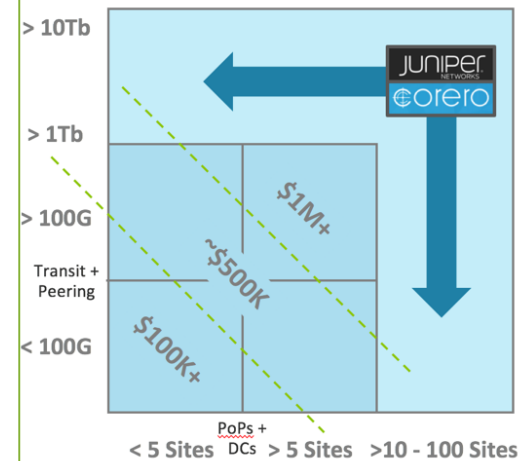
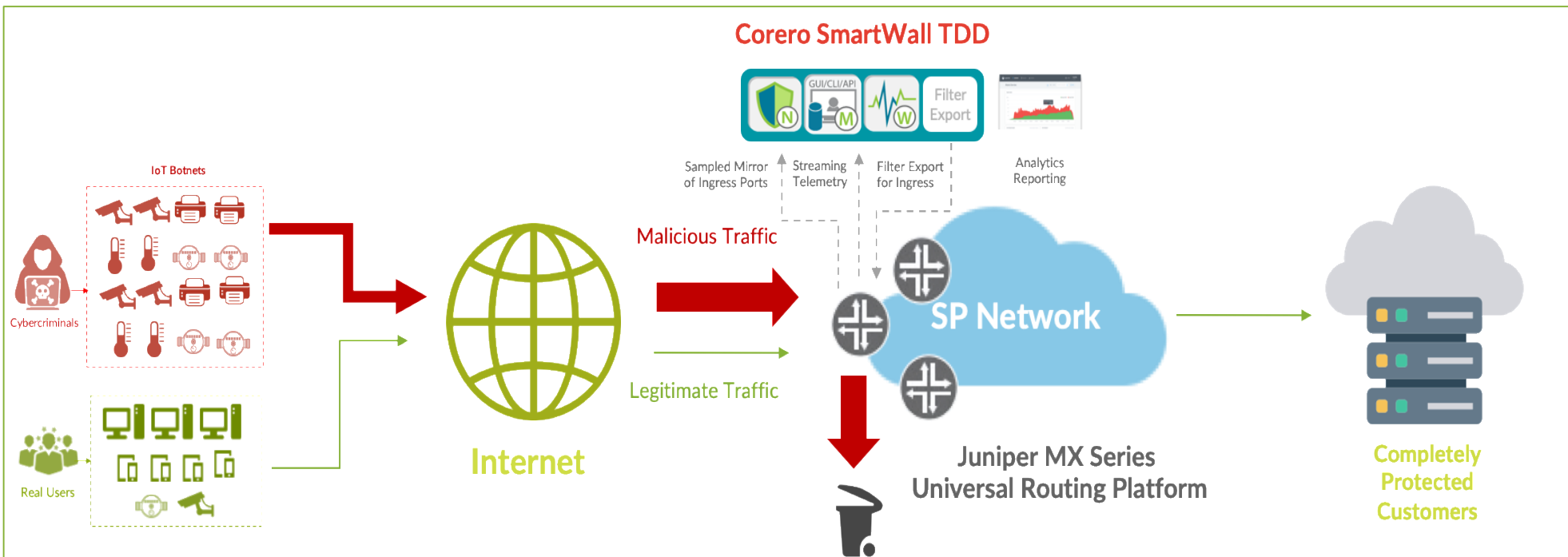
5G Networks



# SCALING OUT VIRTUAL FIREWALL FOR SECURING TELCO CLOUD



# JUNIPER + CORERO JOINTLY DELIVER TERABIT-SCALE DDOS PROTECTION



### Continuous Monitoring

- Juniper MX deployed at Network Edge
- Monitor Ingress Traffic via Sample Mirror
- Mirror Samples and Streaming Telemetry Forward to Corero SmartWall TDD

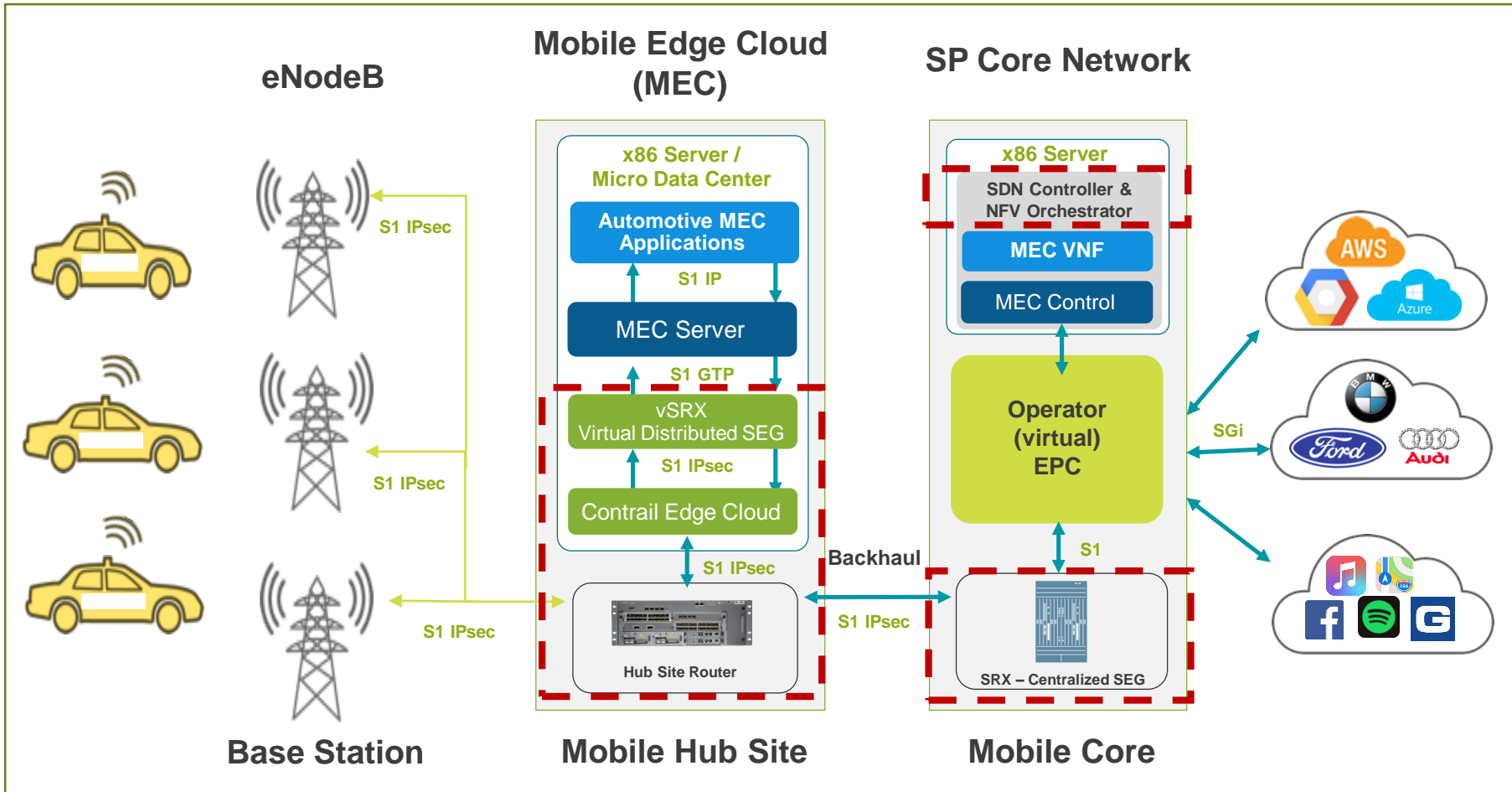
### Real-Time Detection

- Corero TDD Inspects every packet in the feeds from Juniper MX routers
- TDD automatically detects any high-volume DDoS attacks, within seconds

### Line-Rate Mitigation & Visibility

- TDD automatically generates firewall filters and configures MX via NETCONF to block DDoS packets
- TDD delivers comprehensive visibility before, during and after any attack with Splunk-powered analytics

# MOBILE EDGE SECURITY

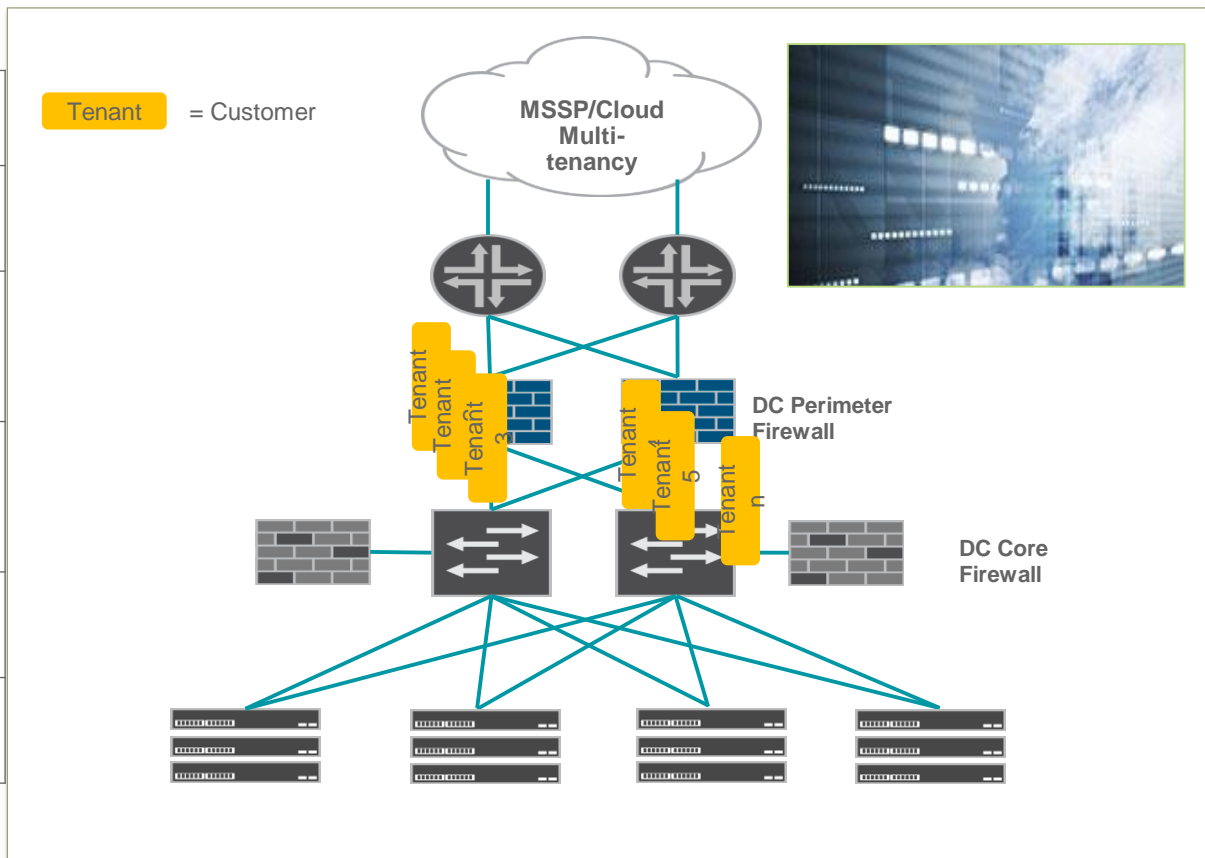


- MEC enables applications to be deployed at the mobile network edge
- Contrail Edge Cloud enables and automates the creation of services chains
- Service chaining is needed to automate the link of IPsec termination (vSEG), MEC server & MEC applications
- vSRX as virtual distributed SEG (Security Gateway) for Edge Security. Security policy: *“Attacks from infected mobile devices should be blocked in the Mobile Hub site”*

## MULTI TENANT SECURITY

### Key Features





- 1 Independent security policy for compliance & control
- 2 Customer are segmented and separated from each other
- 3 Per-tenant configurable compute and memory allocation
- 4 Per-customer monitoring and logging capabilities
- 5 Service resiliency, access to new SW. & PSIRTS patches



### Customer Benefits

- 1 Customers control their security policy & stay compliant
- 2 Data Privacy–Customers don't see each other traffic
- 3 Per Tenant Service Level Agreements are guaranteed
- 4 Customers are able to isolate and fix problems quickly
- 5 Higher uptime & SW upgrades with minimal disruptions

# ENABLING CLOUD-BASED MANAGED SERVICES WITH VCPE/UCPE

JUNIPER CUSTOMER	 at&t	 verizon	 orange Business Services	Major Middle East Telco	Major Tier 2 US SP	Major European Telco	 WOW! INTERNET AND CABLE
<b>PRODUCT/ NETWORK AREA</b>	ATT-Flexware VZ-Virtual Network Services		EasyGo vCPE Services	Cloud CPE – vCPE and uCPE	Managed router	VPN Plus – vCPE/uCPE based services	Virtual Network Platform
<b>BUSINESS DRIVER</b>	Agile services, reduced cost, increase relevance		Address new TAM, increase agility	Telco cloud and managed services transformation	Zero touch provisioning, lower opex, expansion	Simplified, agile global growth with NFV	Simplified, agile growth with NFV
<b>DESCRIPTION</b>	Multi-function/VNF, software based appliance vSRX		Juniper based, multi-vendor VNFs, vSRX, Contrail	Juniper NFX, CSO, Contrail, vSRX, NEC/NC NaaS platform	Juniper NFX, CSO/NSC, Contrail, vSRX VNF	Juniper NFX, CSO, Contrail, vSRX with Multi- vendor VNFs	Contrail Cloud & Service Orchestration &vSRX
<b>LAUNCH/ TRIAL TIMING</b>	2016 deploy		2016 deploy	2017 deploy	2016 deploy	Recent award	2016 deploy/ 2017 expansion
<b>ADDITIONAL INFORMATION</b>	Contrail, NFX, Contrail Service Orchestration, vSRX; 40+ SP in PoC, labs, and trials						



# Summary



# KEY CONSIDERATIONS FOR 5G SECURITY STRATEGY

## •Both Security Performance and Security Operations Need to Scale

- Capacity & Capability
- Unified Security Management

## Network Architecture Evolution and New Enabling Technologies Open New Attack Surfaces

- 5G technology enablers bring in new attack surfaces
- Re baseline security for new architecture and topologies

## Security as a Service Differentiator and Revenue Enabler

- Top most challenge for Enterprise IoT
- Security consideration for industry verticals

# COMPLETE SECURITY PORTFOLIO



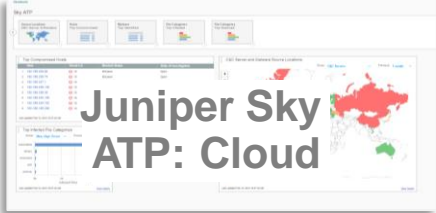
**Security Director  
Policy Enforcer  
Juniper Sky Enterprise**

**Management, Automation**



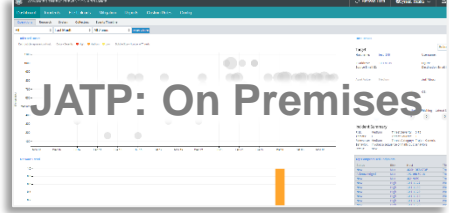
**Secure Analytics**

**SIEM**



**Juniper Sky  
ATP: Cloud**

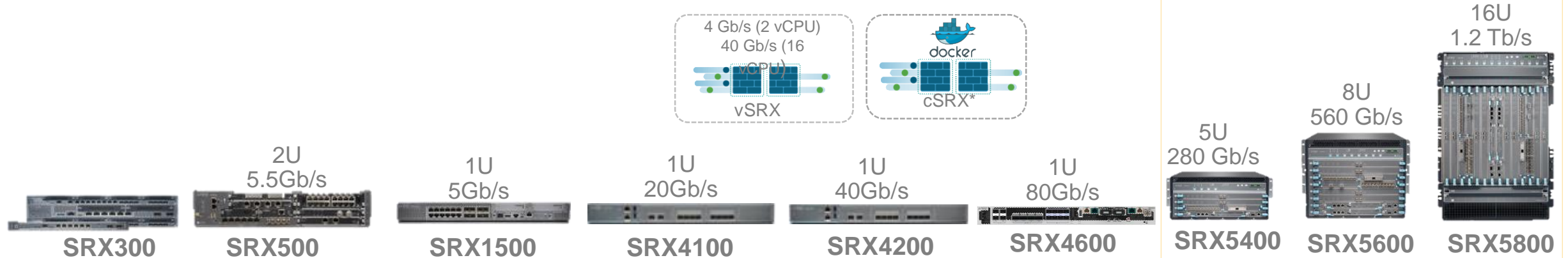
**Advanced Threat Prevention**



**JATP: On Premises**

**IPS/IDS  
Anti Malware  
Application Security  
URL Filtering  
IoT Security**

**Next-Gen Security Services**



**Advanced Security Acceleration (SPA3)**

4 Gb/s (2 vCPU)  
40 Gb/s (16 vCPU)  
vSRX

docker  
cSRX\*

SRX300 (1U)  
SRX500 (2U, 5.5Gb/s)  
SRX1500 (1U, 5Gb/s)  
SRX4100 (1U, 20Gb/s)  
SRX4200 (1U, 40Gb/s)  
SRX4600 (1U, 80Gb/s)

SRX5400 (5U, 280 Gb/s)  
SRX5600 (8U, 560 Gb/s)  
SRX5800 (16U, 1.2 Tb/s)

Branch

Campus

Private Cloud/Multicloud

Large Data Center/Service Provider

Routing/SD-WAN

IPsec/VPN

High Availability

SSL/TLS Proxy



THANK YOU

---

JUNIPER  
NETWORKS

Engineering  
Simplicity