Adopting cloud technologies & Security in 5G

Shankar Srinivasan
Sr. Solution Architect, APJC
10th Aug 2023

Key areas

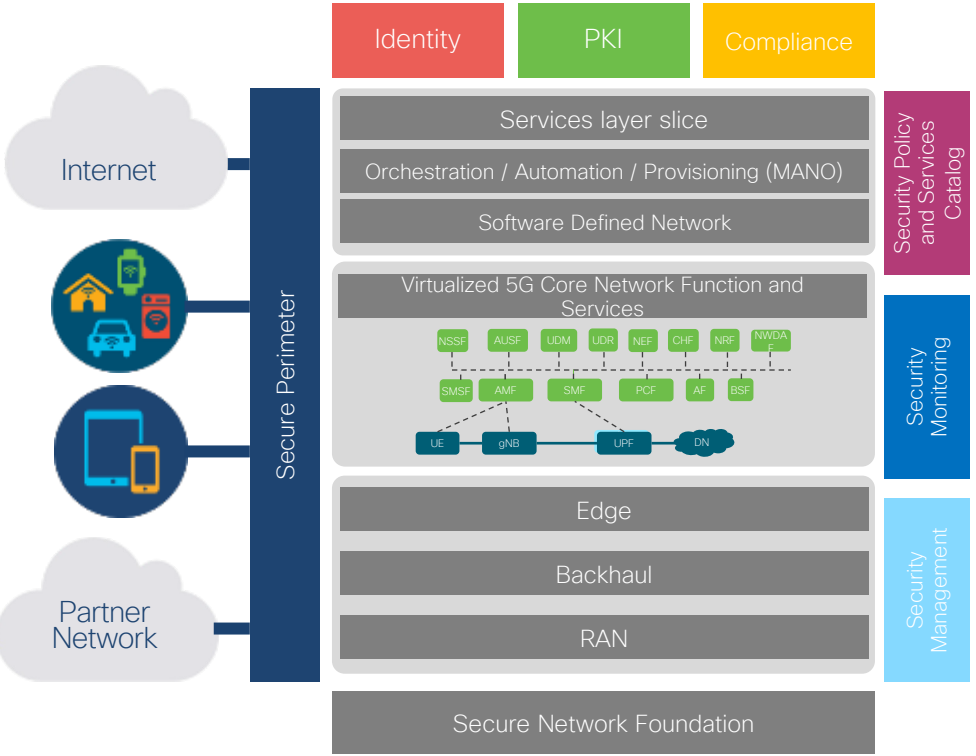
- Guiding principles of security
- Threat landscape in 5G
- Zero trust in the access
- Securing 5G transport
- Securing 5G core
- 5G APIs & security
- Visibility & impact

The 5 Dimensions of Security Resilience

1. **See More:** Activate Billions of Signals
   telemetry across ecosystem, active monitoring and filtering
2. **Anticipate What's Next:** Embrace Shared Intelligence
   actionable intelligence and expertise
3. **Take Right Action:** Prioritize What is Most Important
   risk-based contextual analysis, continuous trust assessment
4. **Close Gaps:** Pervasive Defense Across Ecosystem
   open platform across users/devices/networks/applications
5. **Get Stronger Every day:** Optimize Efficacy
   orchestrate, automate, spring back faster

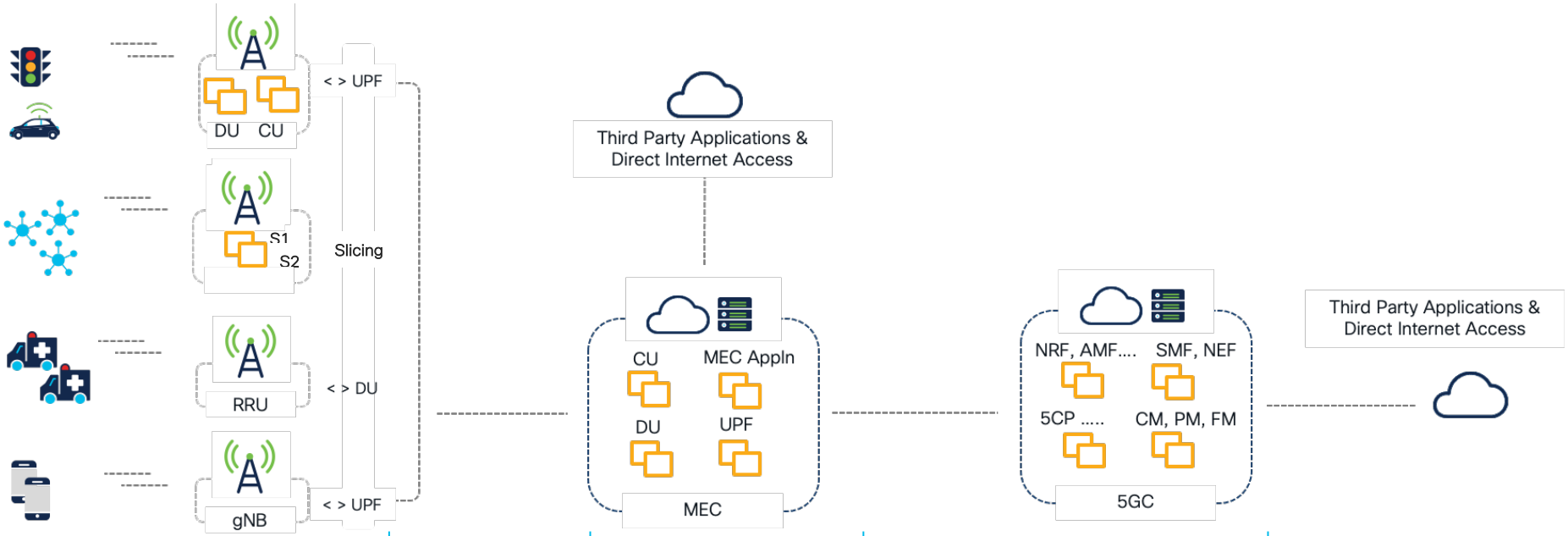
Guiding security principals

- ENISA 5G Threats, 3GPP TS 33.501, NIST 800-207 Zero Trust
- Trust posture and integrity of individual **Network Elements**
  - Identity of every network element and user.
  - Use cryptography to build strong chain of trust.
  - Secure configuration; continuous verification
- Trusted access to resources by Intrinsic **Network Design**
  - Secure external network flows
  - Isolation / segmentation of internal network and services
  - Securing protocols, network services and management.
- Automation security across **entire lifecycle**
  - Security deployed at the same time as the network
  - Monitoring and telemetry to detect security events and anomalies.
  - Integration and automation for rapid response (SOAR)



Evolution of Security controls

Threat landscape in 5G



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
MEC Backhaul sniff
Side Channel attacks
NFVi Vulnerabilities

5G Packet Core & OAM Threats

Virtualisation
LI Vulnerabilities
Improper Access Control
Network Slice security
API vulnerabilities
NEF vulnerabilities
Roaming Partner
DDoS & DoS attacks

SGi / N6 & External Roaming Threats

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

How Zero Trust can be enforced @ the access

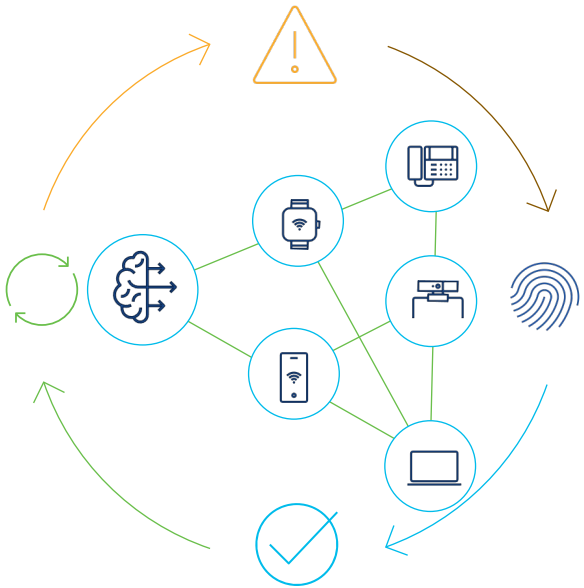
Connecting trusted users and endpoints with trusted resources

Endpoint Request Access

- Endpoint is identified and trust is established
- Posture of endpoint verified to meet compliance

Trust continually verified

- Continually monitors and verifies endpoint trust level
- Vulnerability assessments to identify indicators of compromise
- Automatically Updates access



Endpoint classified, and profiled into groups

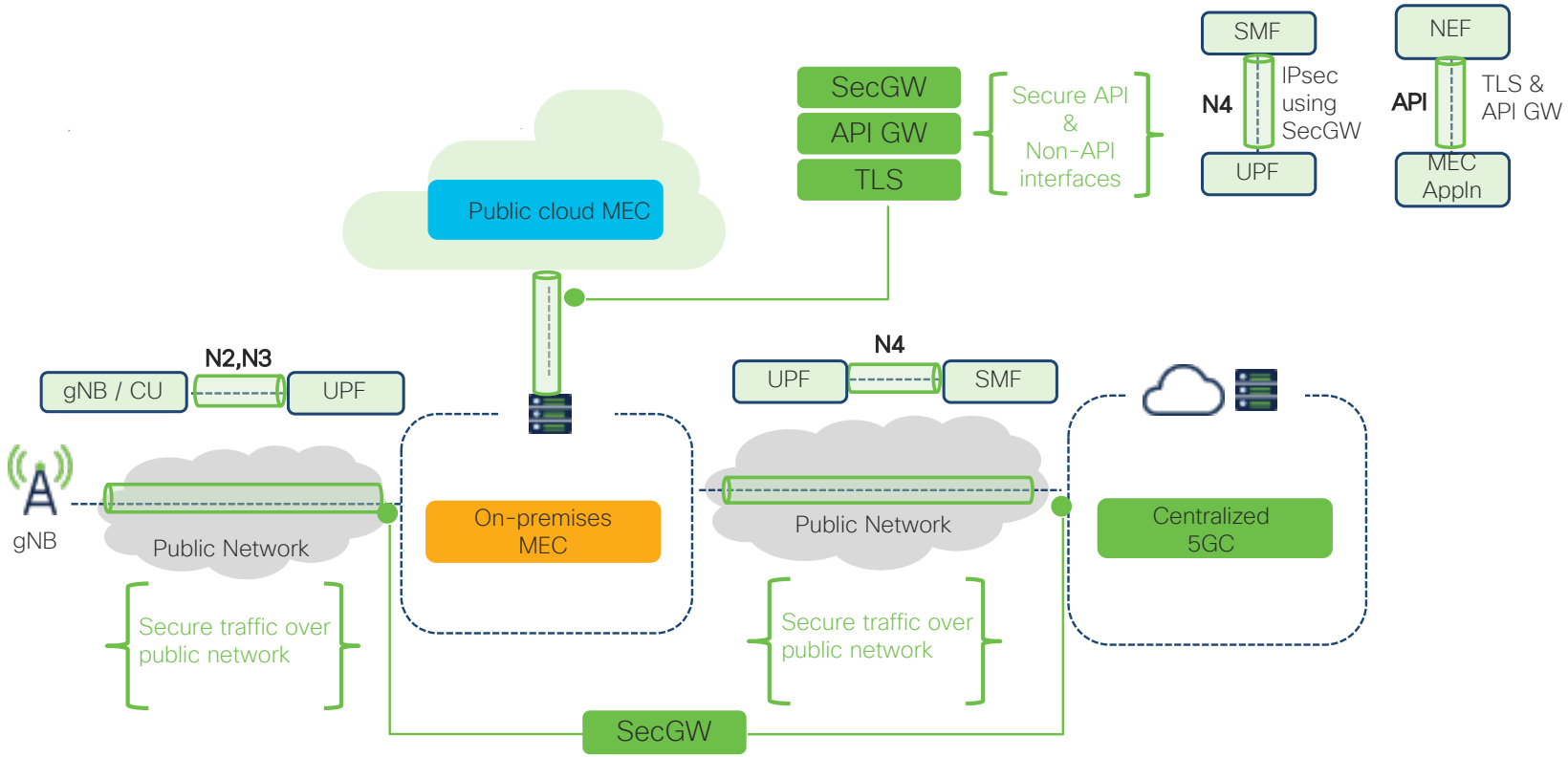
- Endpoints are tagged x/SGTs
- Policy applied to profiled groups based on least privilege

Endpoint authorized access based on least privilege

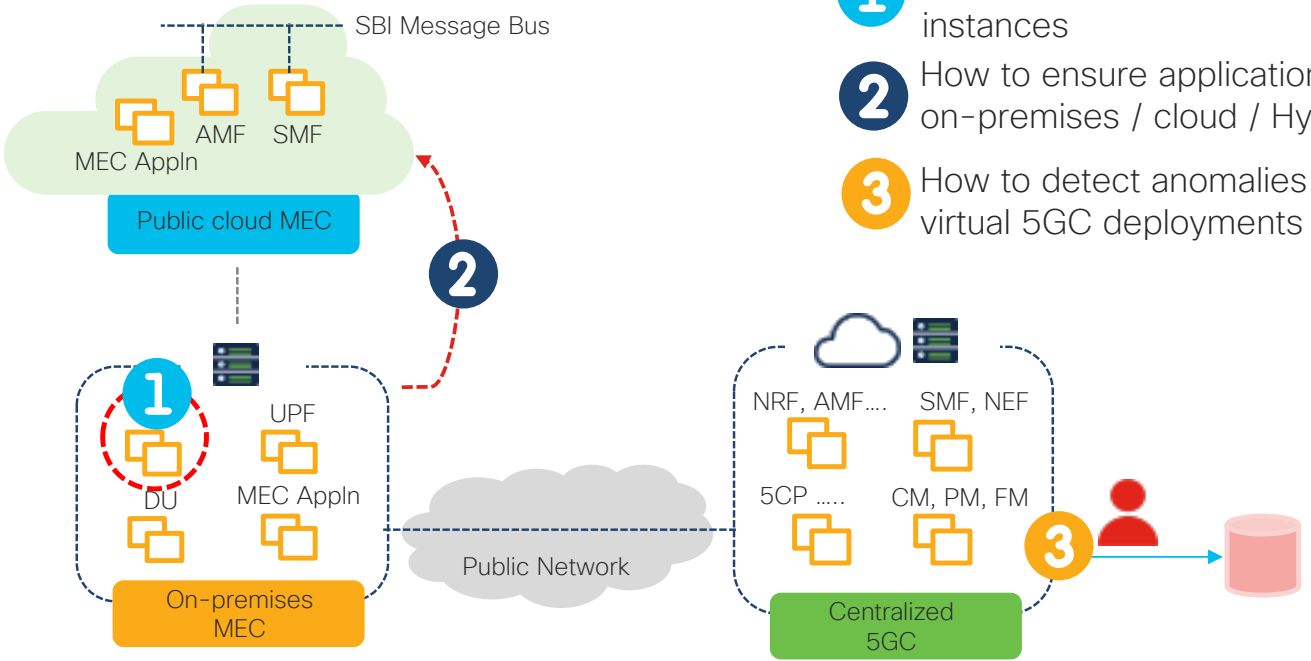
- Access granted
- Network segmentation achieved

Next generation endpoint visibility with AI-driven analytics and network driven deep packet inspection

Securing Transport in 5G



Securing the 5G core & challenges



1. How to detect vulnerable / malicious 5GC instances
2. How to ensure application policy enforcement in on-premises / cloud / Hybrid 5GC instances
3. How to detect anomalies and data exfiltration in virtual 5GC deployments

Securing VNFs

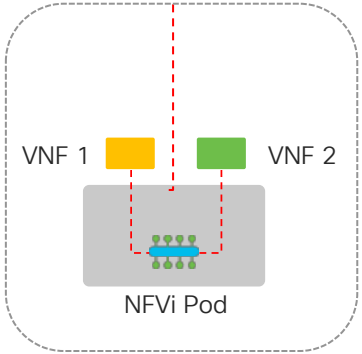
Policy enforcement on VM's & containers

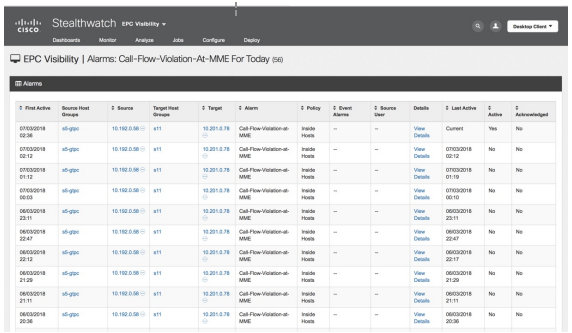
DNS Layer Security

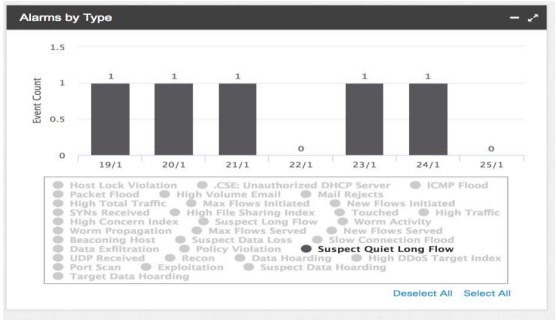
Access to malicious server blocked

Command & Control servers

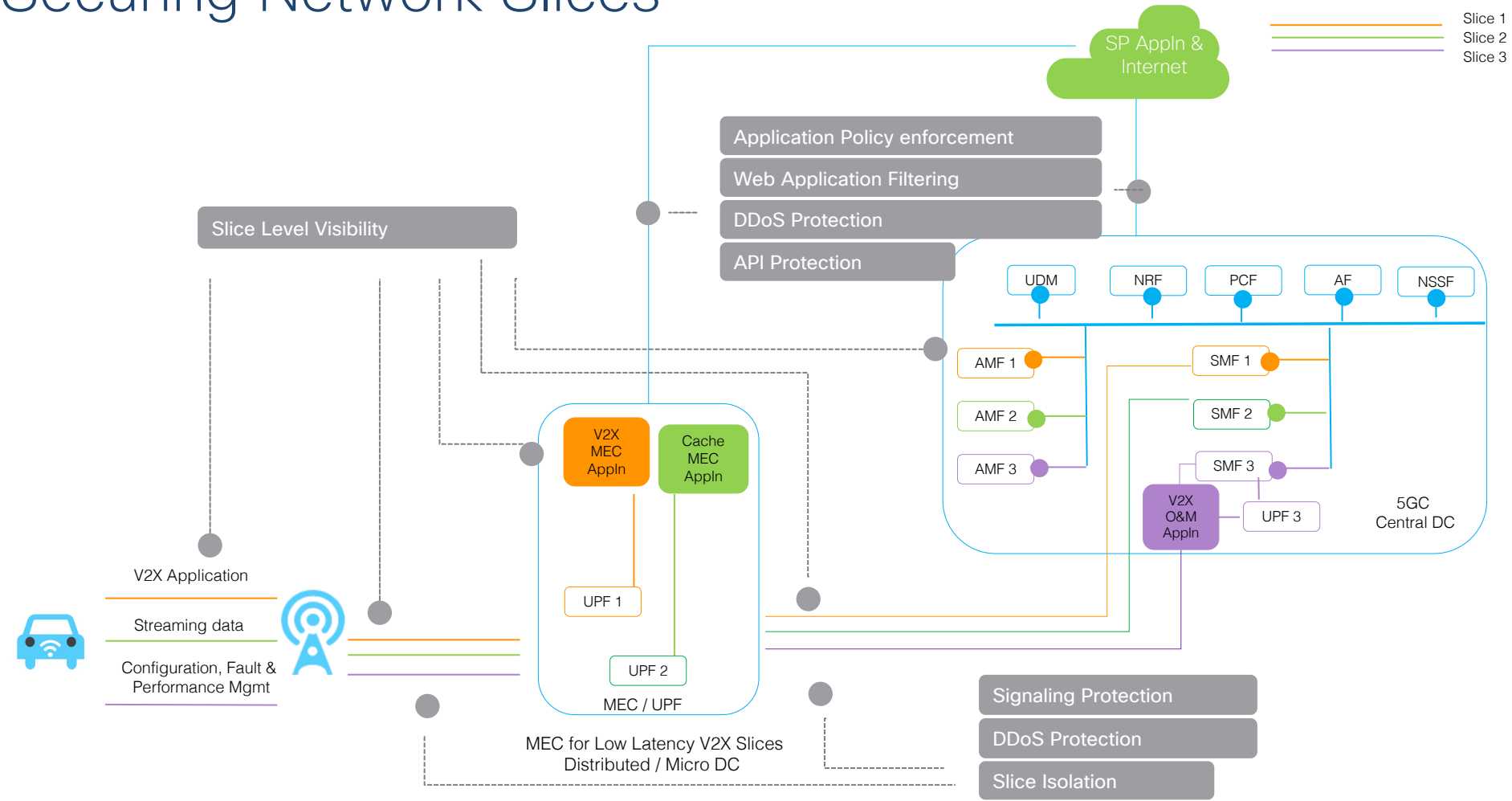
Detection of abnormal flows



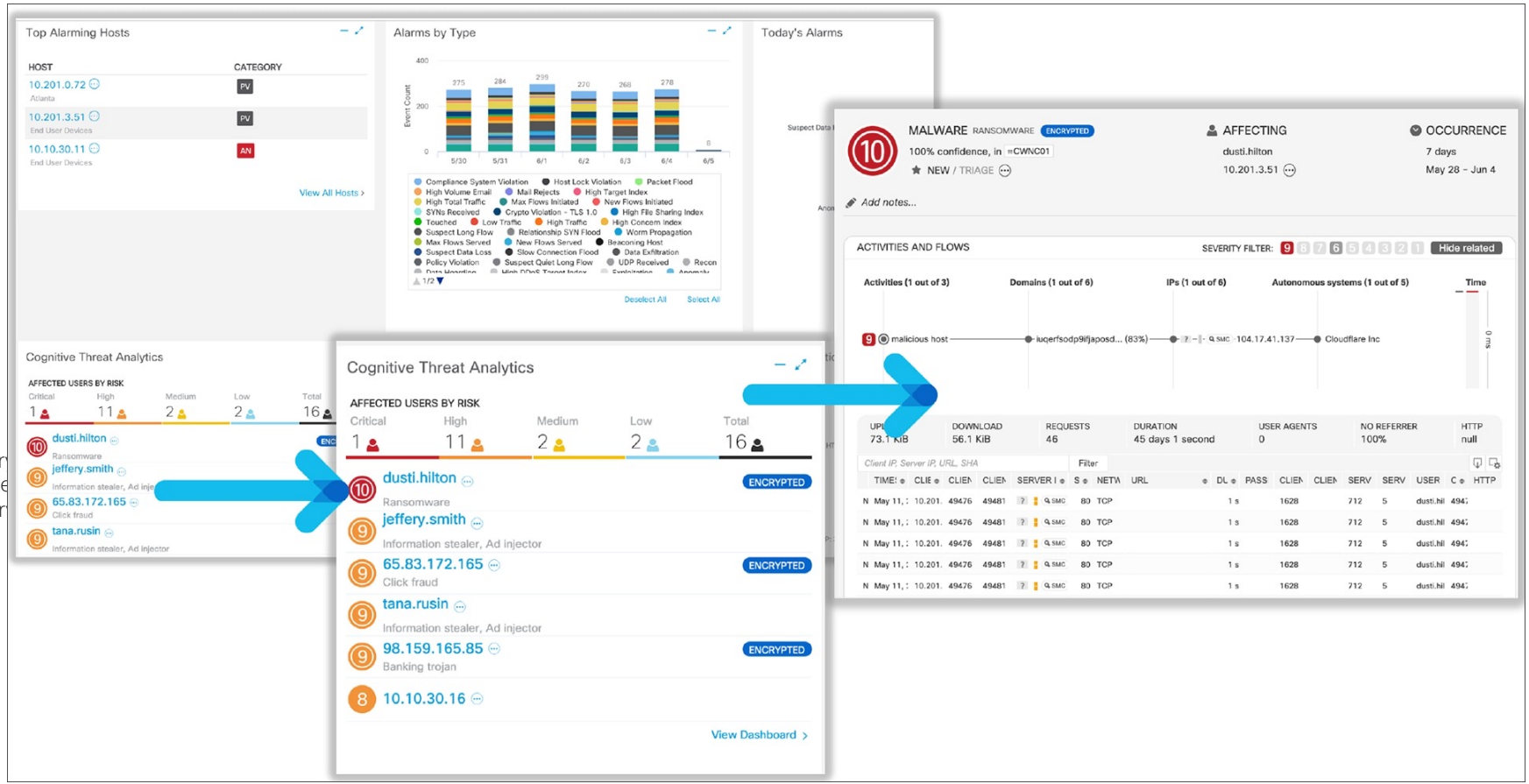


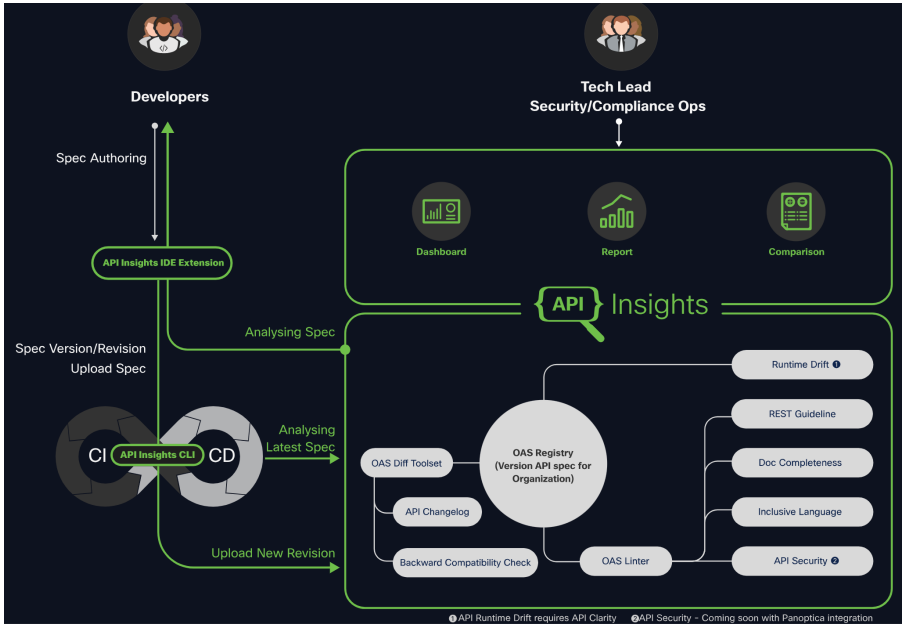


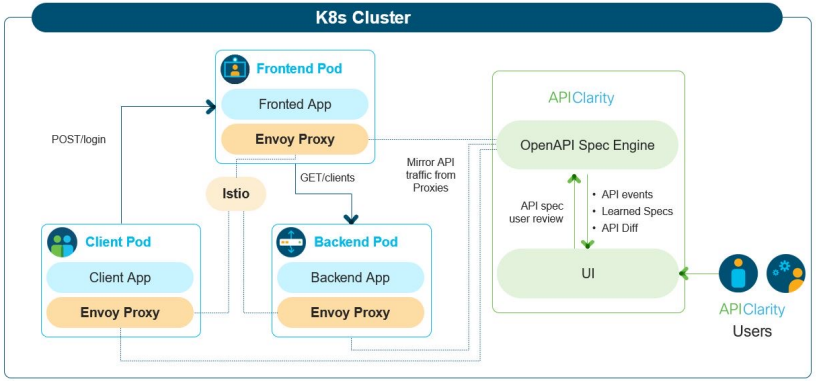
Securing Network Slices



Secure 5G API & non-API communications







API Insights

Validates and scores APIs

API Insights validates and scores API definitions against an organization's guidelines. This allows you to track and improve API quality consistently and efficiently.

Built for your CI/CD pipeline

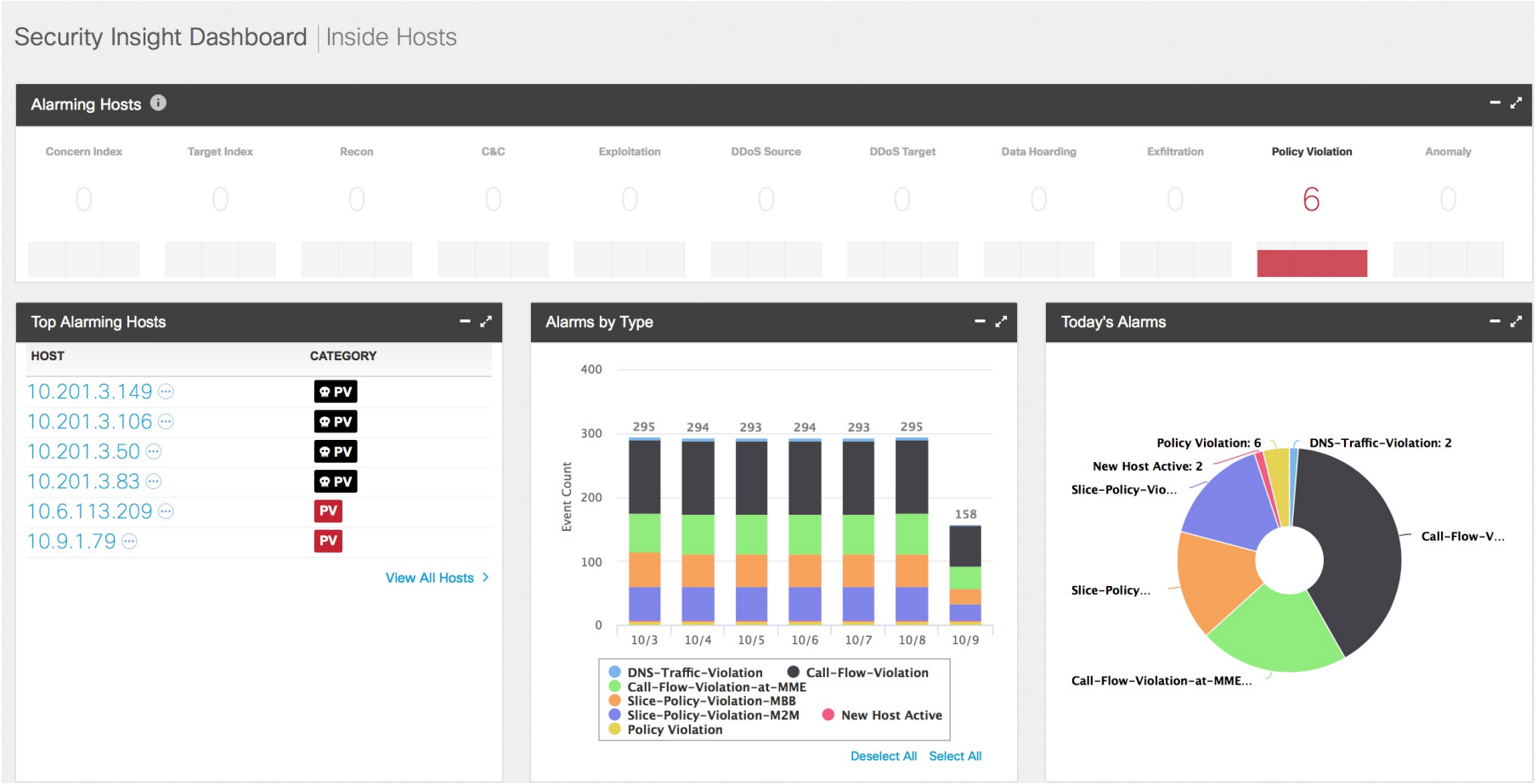
Developers can use API Insights through its own interface or as part of their CI/CD pipeline.

API Lifecycle Management

Provides a trend timeline of API quality, and generates both API changelogs and diff comparisons of API versions to identify breaking changes.

APIClarity

Visibility & impact



Visibility & impact

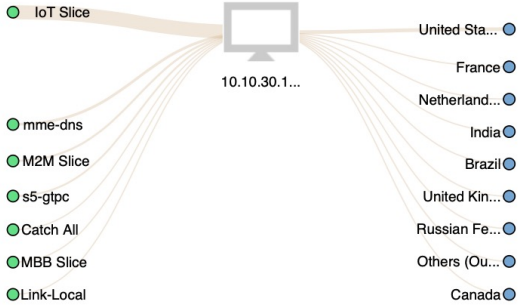
Host Summary

Host IP
10.10.30.16

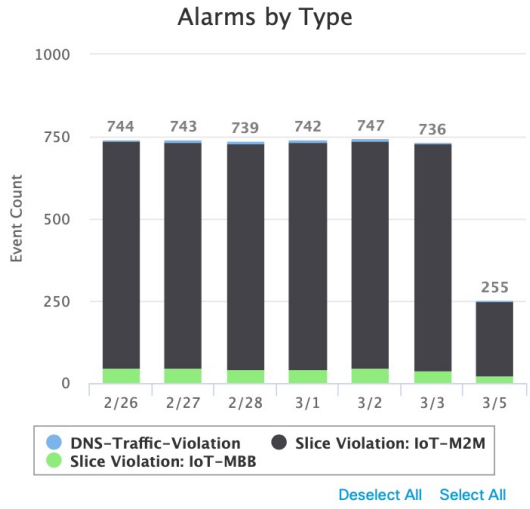
Flows | History

Status:	Active
Hostname:	--
Host Groups:	IoT Slice
Location:	RFC 1918
First Seen:	8/30/18 1:31 AM
Last Seen:	3/5/19 2:10 AM
Policies:	Cisco_SP_Circle_1,Inside
MAC Address:	--

Traffic by Peer Host Group (last 12 hours)



Alarms by Type (last 7 days)

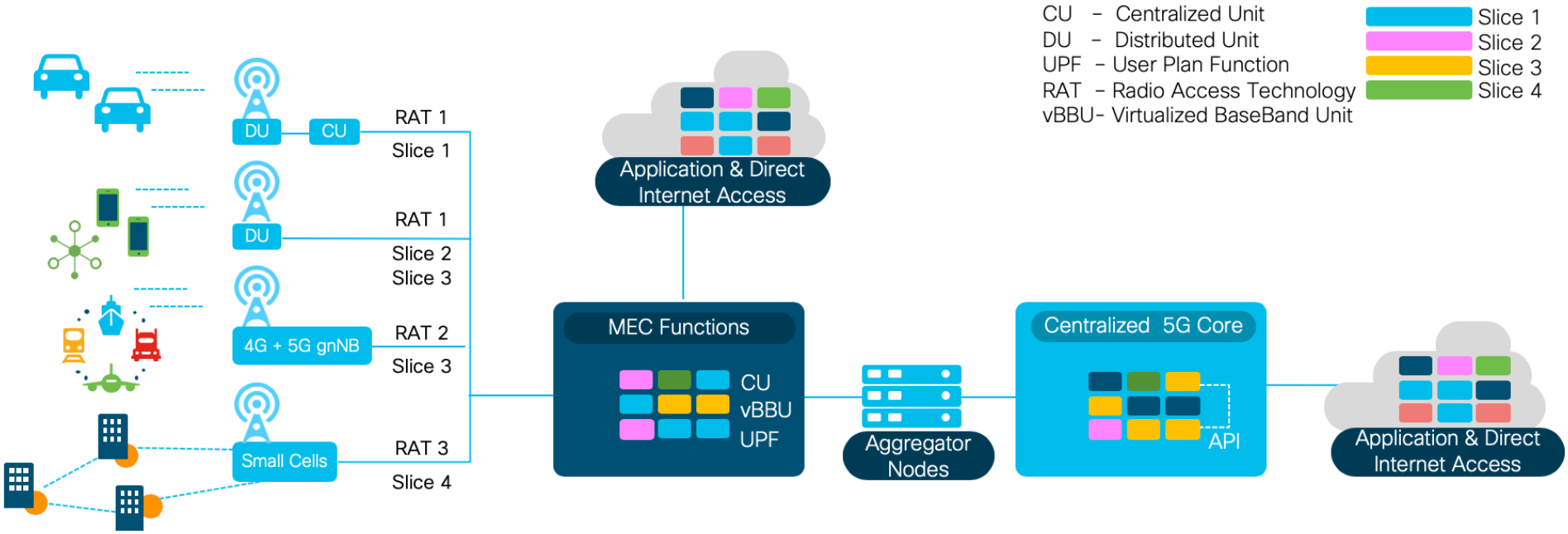


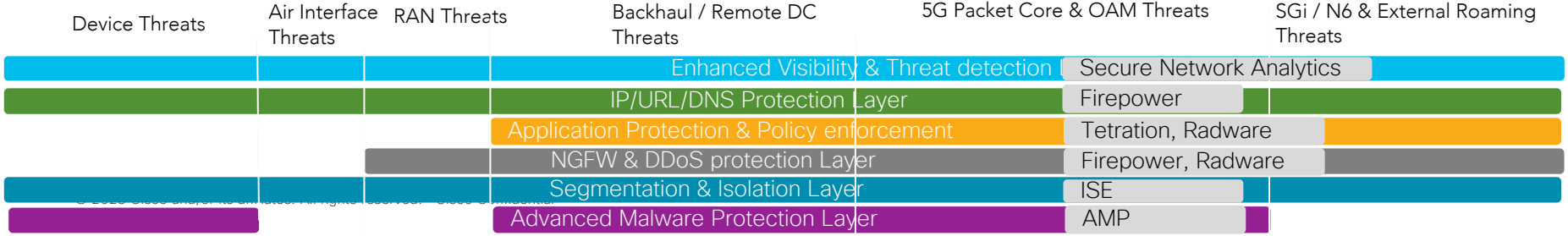
Top Security Events for 10.10.30.16

Source (10) | Target (10)

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	TARGET HOST	TARGET HOST GROUP	ACTIONS
Slice Violation: IoT-M2M - 4359	10	0	03/04 4:04:20 PM	10.10.100.70	M2M Slice	
Slice Violation: IoT-M2M - 2240	50	0	03/04 4:34:27 PM	10.10.100.66	M2M Slice	
Slice Violation: IoT-M2M - 67	1	0	03/04 5:55:01 PM	10.10.100.254	M2M Slice	

End to End Threat Mitigation






CISCO