AUTOMATED AI-BASED THREAT PROTECTION FOR 5G AND IOT NETWORKS

Ravi Raj Bhat

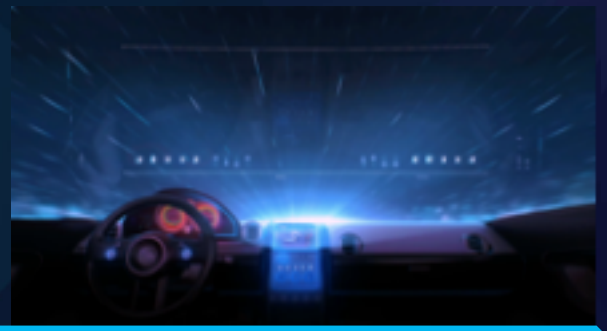
SVP, Global Field CTO, A10 Networks

Reliable Security Always™

AGENDA

- Introduction
- 5G Architecture and Trends
- Security Implications
- Why AI?
- Conclusion

5G: ONE NETWORK FOR ALL



5G GOAL: < 1 MS

ENHANCED MOBILE BROADBAND
(eMBB)

- Low Criticality
- High Throughput
- Low Latency

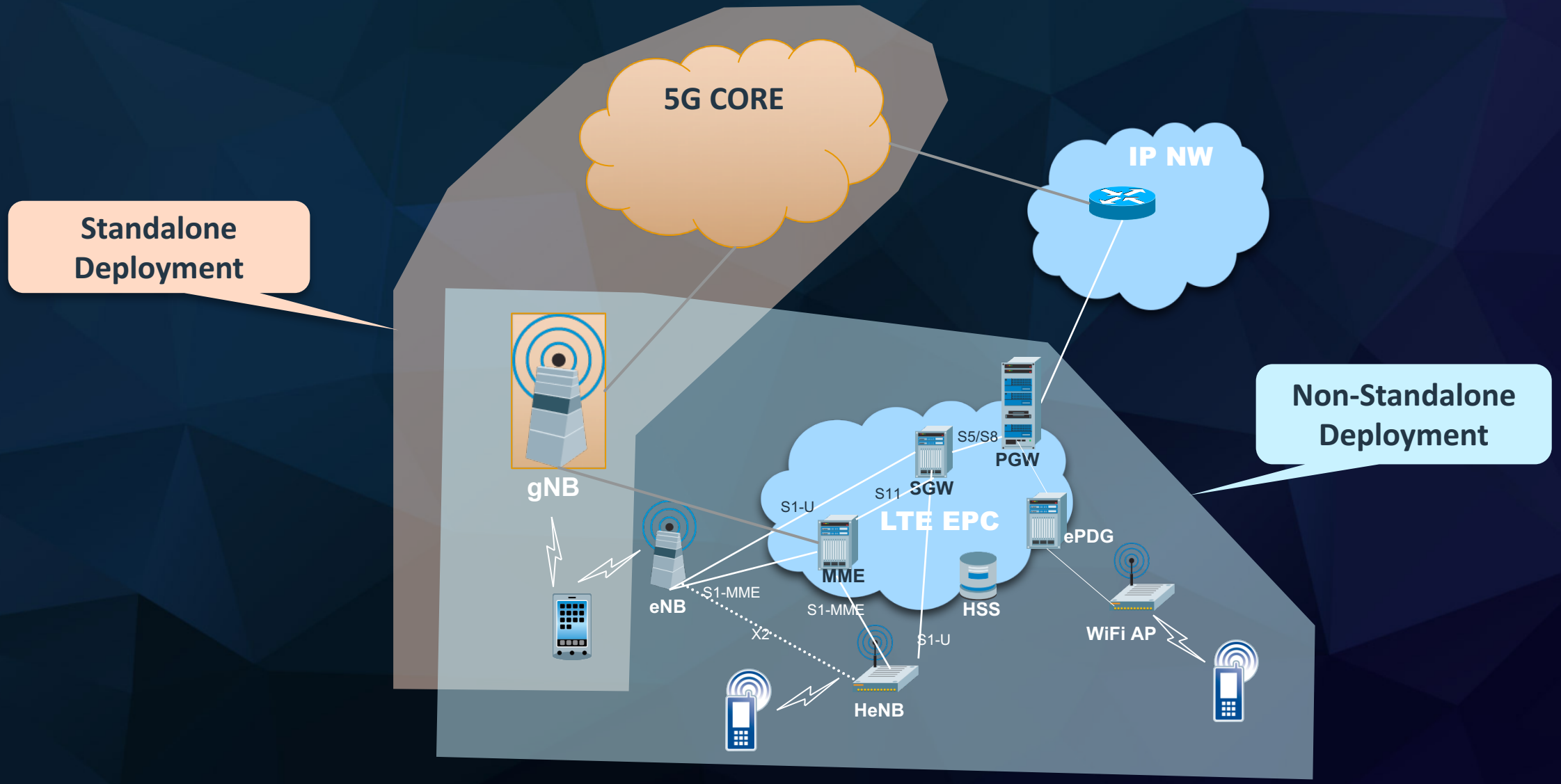
MASSIVE IOT
Massive Machine Type Communications (MMTC)

- Low Criticality
- Low Throughput
- Latency Needs Vary

CRITICAL IOT
Ultra-Reliable Low Latency Communications (URLLC)

- Highly Critical – Life Impacting
- Ultra Reliability
- Ultra Low Latency

5G DEPLOYMENT MODES



EVOLVING ARCHITECTURE AND TRENDS

CUPS / SBA

Telecom vs
IT protocols

SCALE

Higher Data and
attack traffic

IoT Adoption

Billions of IoT's
coming online

Move to MEC

Edge Cloud

IT PROTOCOLS INSTEAD OF TELECOM PROTOCOLS

EVOLVING ARCHITECTURE – CUPS AND SBA

S1AP	GTP
SCTP	UDP
IP	
L2	
L1	

HTTP/2
TLS
TCP
IP
L2
L1

GTP

- GTP is complicated
- Attack vectors are new
- Closed systems

HTTP

- HTTP is simple
- Numerous attack vectors emerging every day
- Open systems

Security through Obscurity is not an option

HIGHER THROUGHPUT, DENSITY AND SMARTER UE'S SCALE

20 X

Speed

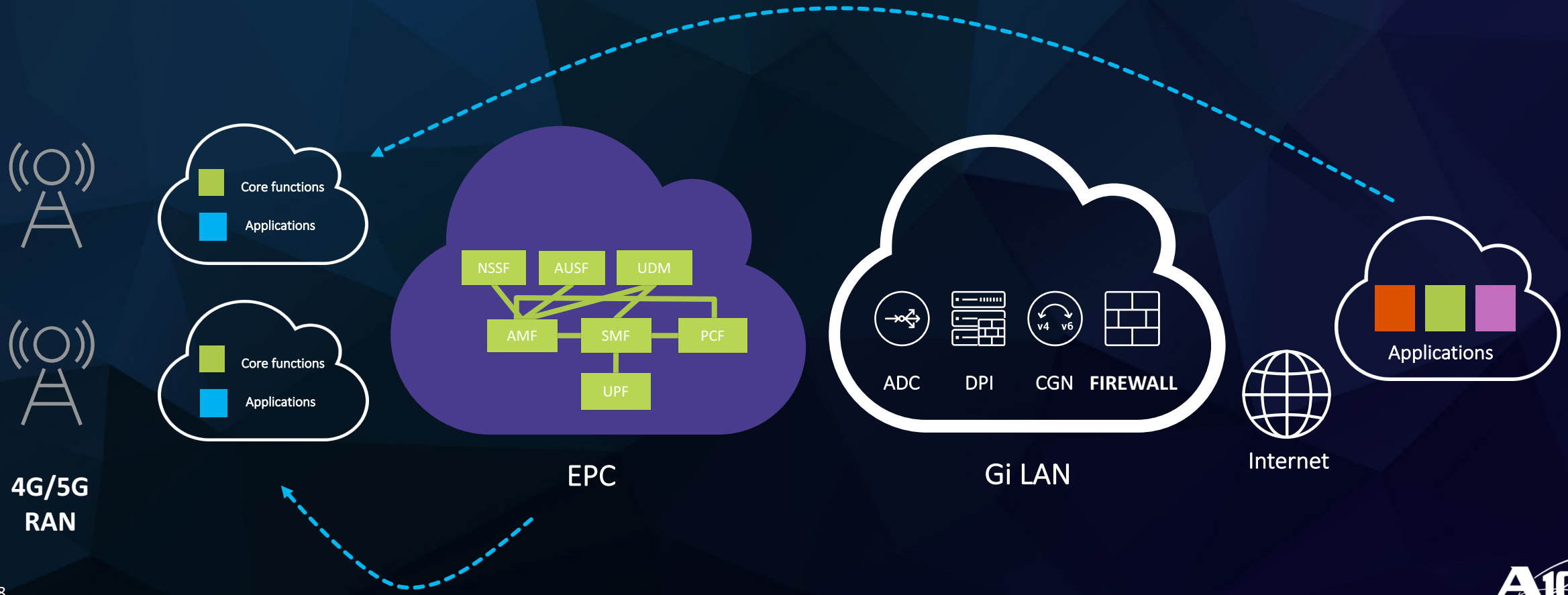
10 X

Density

Smarter UE's

5G enables devices to be colossal threat actors

THE RISE OF MULTI-ACCESS EDGE COMPUTING

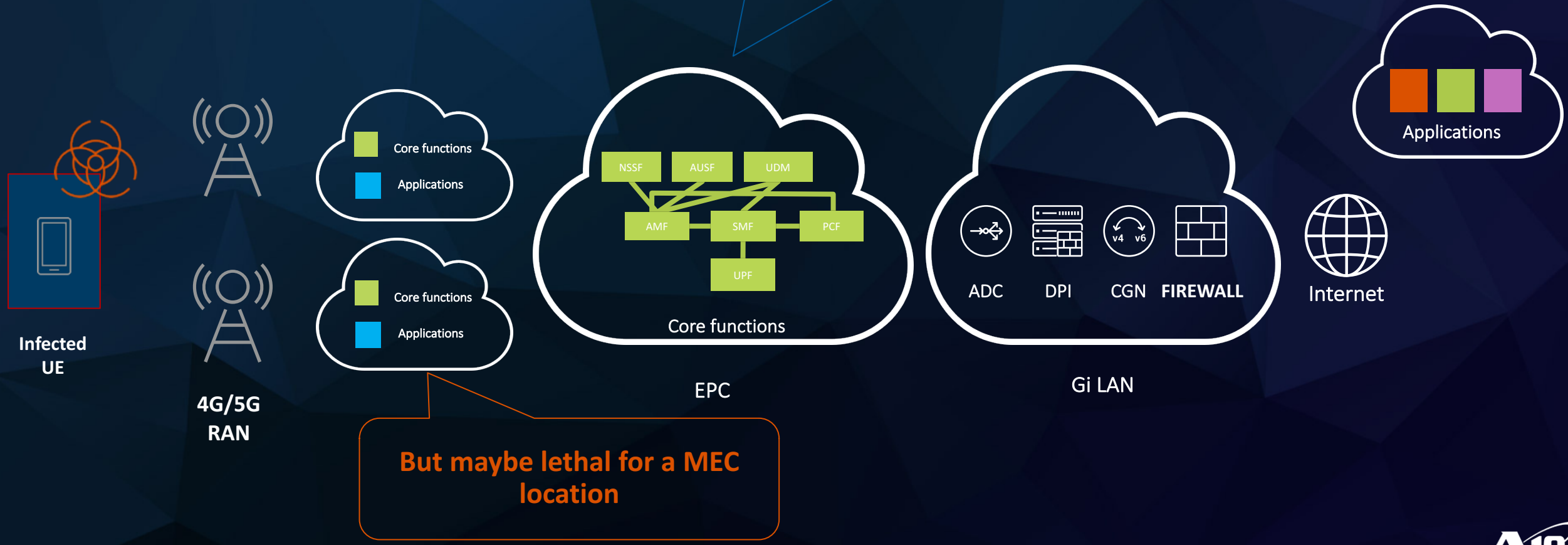


DDOS NOISE BECOMES LETHAL AT EDGE

THE RISE OF MULTI-ACCESS EDGE COMPUTING

Security Implications

1 Gbps attack is noise for the entire packet core



But maybe lethal for a MEC location

SECURITY SOLUTIONS

CONSOLIDATED YET FEDERATED FIREWALL

Scalable L4 Firewall

Scalable L7 FW

GTP / Diameter Inspection

HTTP/2 Protection

IPsec VPN

Scalable TLS Inspection

Carrier Grade NAT

Flexible Form Factors

DDoS detection

Security Edge Protection Proxy

Consolidated functions

Scalable -
Built for Carriers

Protect 4G AND 5G
infrastructure

ADAPTIVE SECURITY MODEL

Machine Learning

Pattern Recognition

Content Patterns

Heuristic Learning

Traffic Behavior

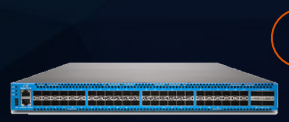
Behavioral Indicators

Behavioral Ratios

Network Learning

Services & Clients

Protected Service

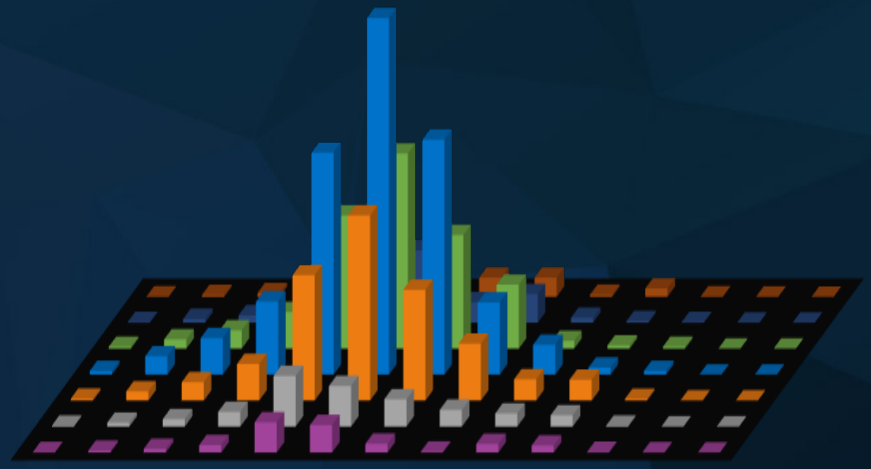


Threat Protection System

DDoS Bot

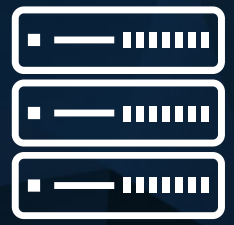
Legitimate User

BEHAVIOR ANOMALY RECOGNITION



Heuristic Behavior Anomaly Detection & Mitigation

- *Packets per Second*
- *Bits per Second*
- *Connections per Second*
- *Concurrent Sessions*
- *Layer 3 and Layer 4*

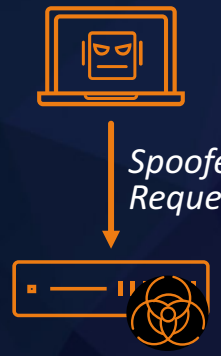


Protected Service

Threat Protection System

Throttle/Pass

Spoofed Request



Reflector

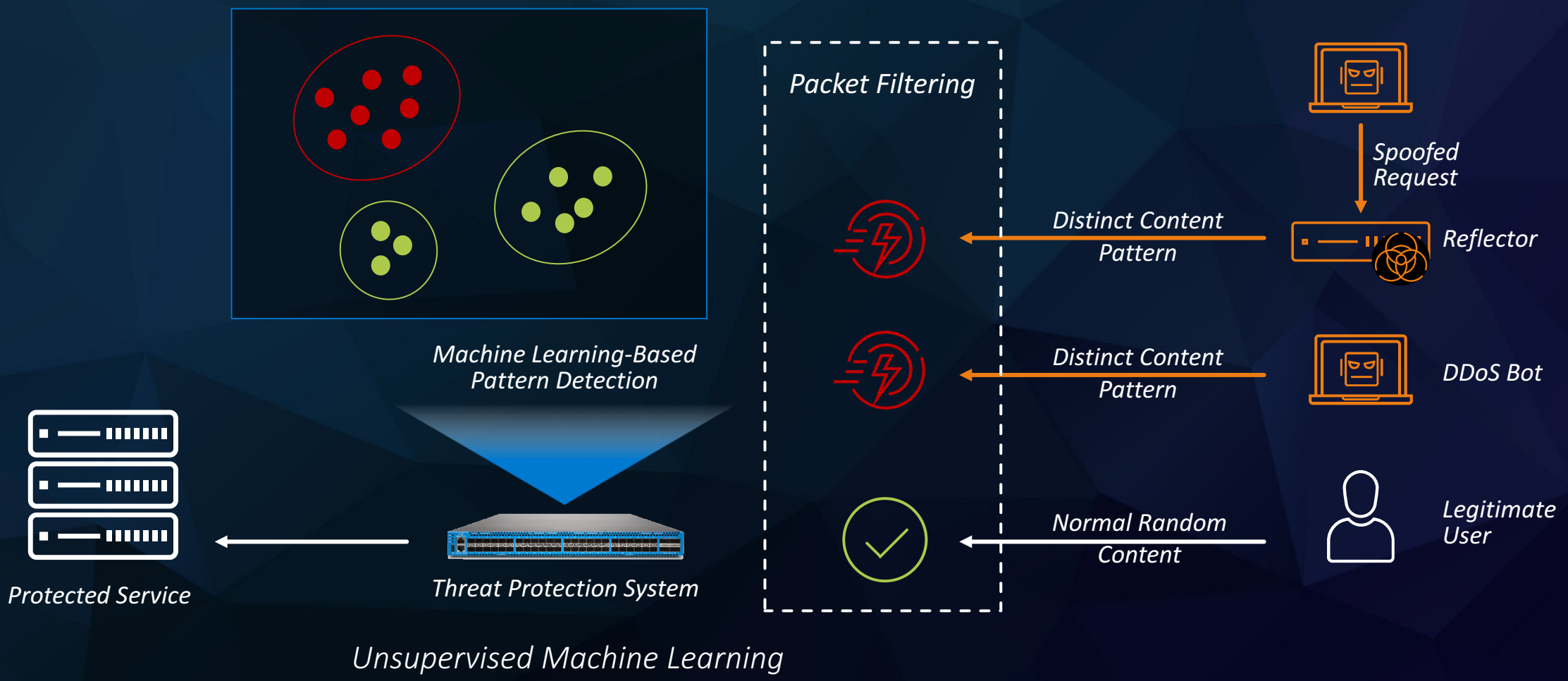
Anomalous Behavior

DDoS Bot

Normal Transmission

Legitimate User

ATTACK PATTERN RECOGNITION



Unsupervised Machine Learning

SUMMARY

- Mobile networks transitioning to open cloud architecture to drive innovation, faster service deployments and cost optimization
- With this transition passive security through obscurity is not an option
- Consolidated yet federated security services are key for meeting stringent 5G latency requirements
- Multifold growth of threat vectors and malicious traffic is the new normal
- ML based threat detection and mitigation at scale are now critical components of an effective 5G threat response strategy

Thank You

A10

Reliable Security Always™