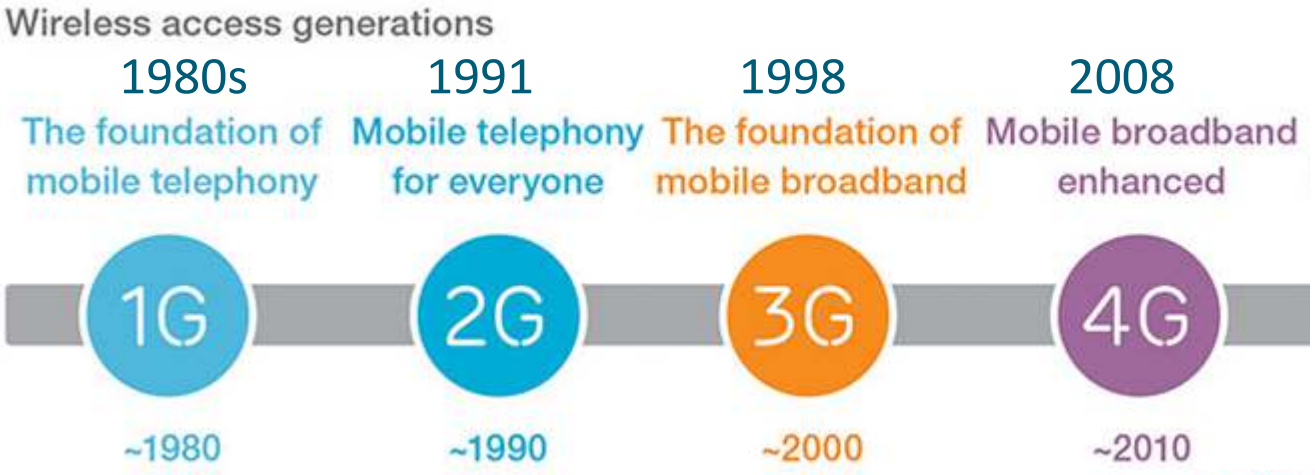
AUTOMATED, AI-BASED THREAT PROTECTION FOR 5G AND IOT

Reliable Security Always™

AGENDA

- 5G Architecture and Trends
- Security Implications
- Security Solution
- Conclusion

JOURNEY TOWARDS 5G



GSM: 9.6kbps
GPRS: 35-171kbps
EDGE: 120-384kbps

UMTS: 384kbps – 2Mbps
HSPA: Upto 42Mbps

Achievable LTE Peak Data Rates

Accounts for overhead at different bandwidths & antenna configurations

	DL		UL
Bandwidth	2x2	4x4	1x2
5 MHz	37 Mbps	72 Mbps	18 Mbps
10 MHz	73 Mbps	147 Mbps	36 Mbps
20 MHz	150 Mbps	300 Mbps	75 Mbps

Texting

Texting Internet Access

Texting Internet Access Video

*Source – Ericsson Mobility Report

5G: ONE NETWORK FOR ALL

5G GOAL: < 1 MS

ENHANCED MOBILE BROADBAND
(eMBB)

- Low Criticality
- High Throughput
- Low Latency

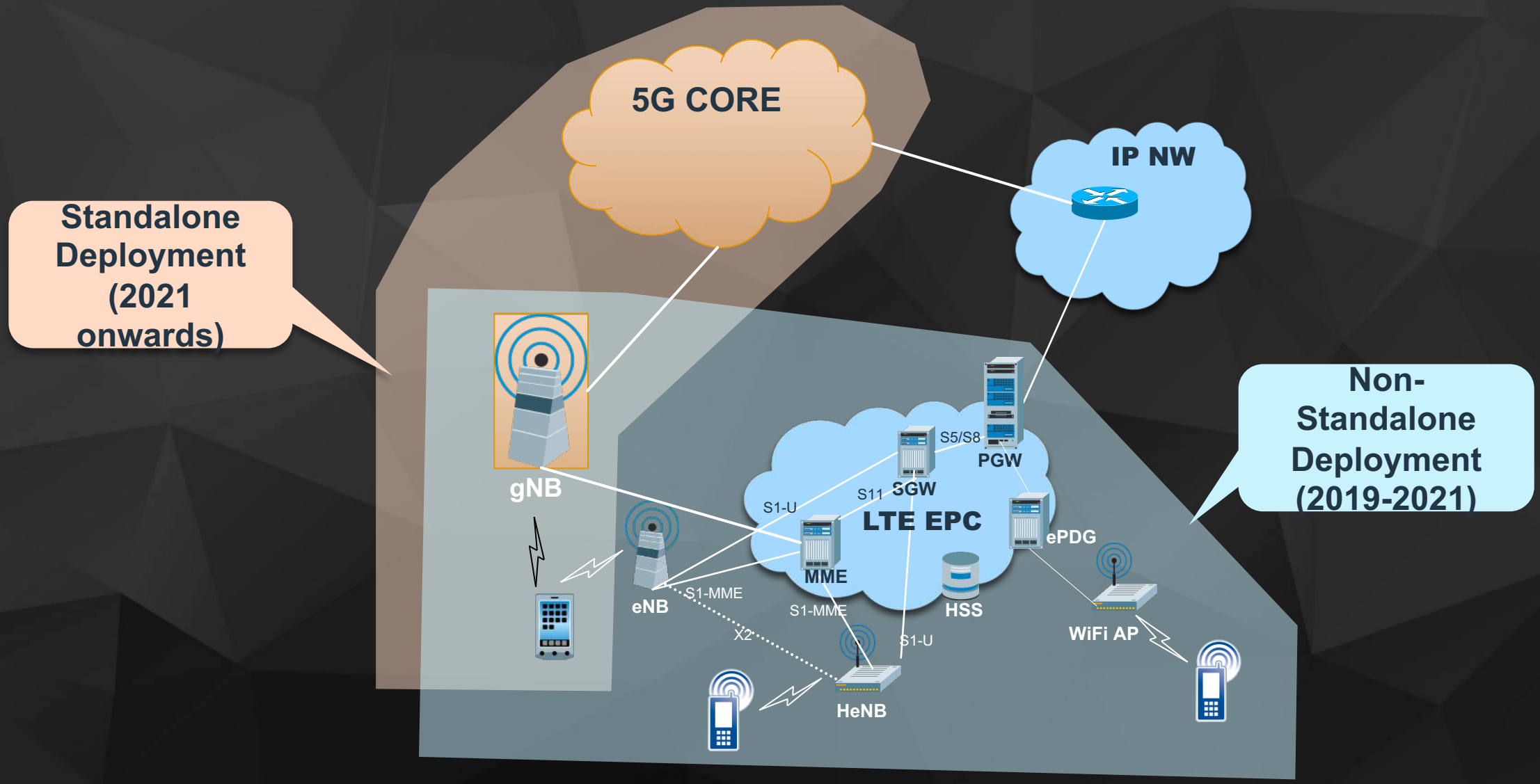
MASSIVE IOT
Massive Machine Type Communications (MMTC)

- 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 WILL TAKE AN EVOLUTIONARY PATH



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

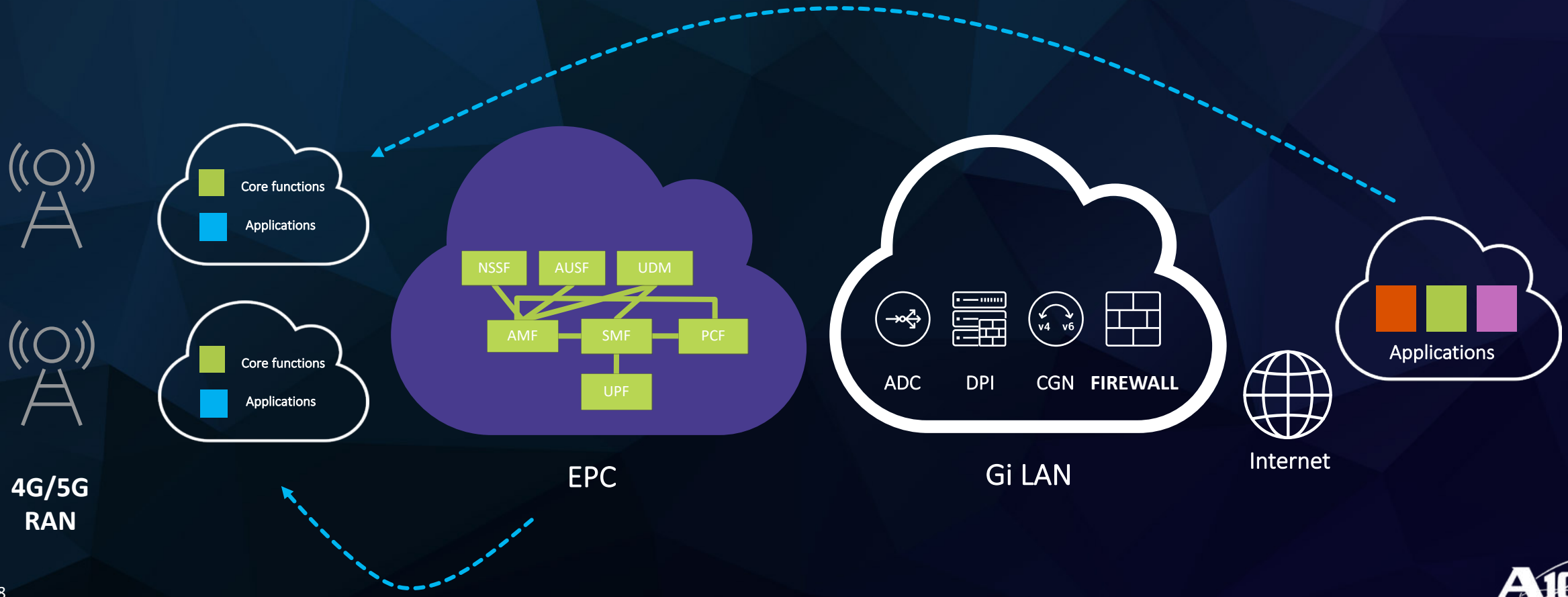
- GTP is complicated
- Attack vectors are new
- Closed systems

HTTP

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

Security through Obscurity is not an option

THE RISE OF MULTI-ACCESS EDGE COMPUTING



SECURING 5G VULNERABILITIES

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

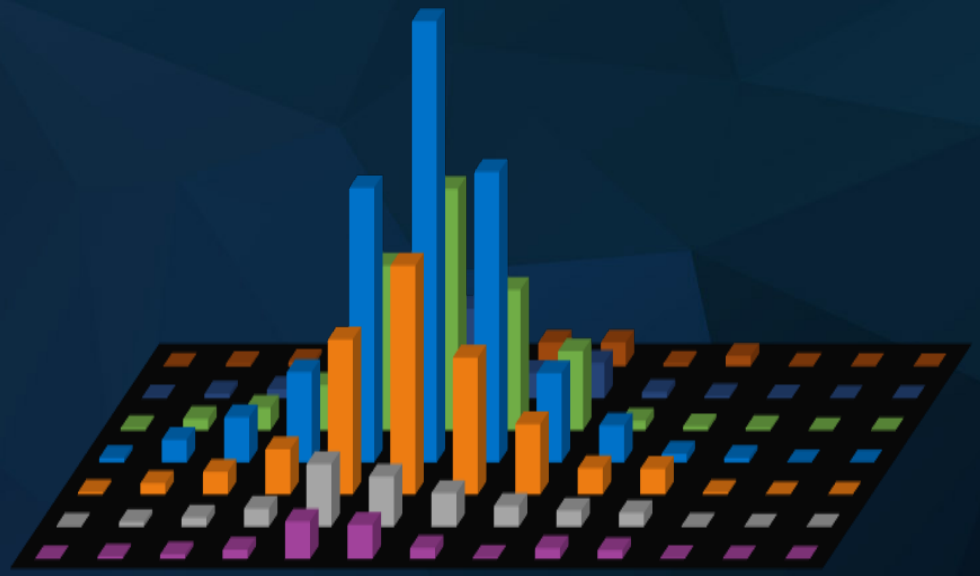
Protected Service

Thunder TPS

DDoS Bot

Legitimate User

ZERO-DAY BEHAVIOR ANOMALY RECOGNITION (ZBAR)



Heuristic Behavior Anomaly Detection & Mitigation

Throttle/Pass

Spoofed Request

Reflector

Anomalous Behavior

DDoS Bot

Normal Transmission

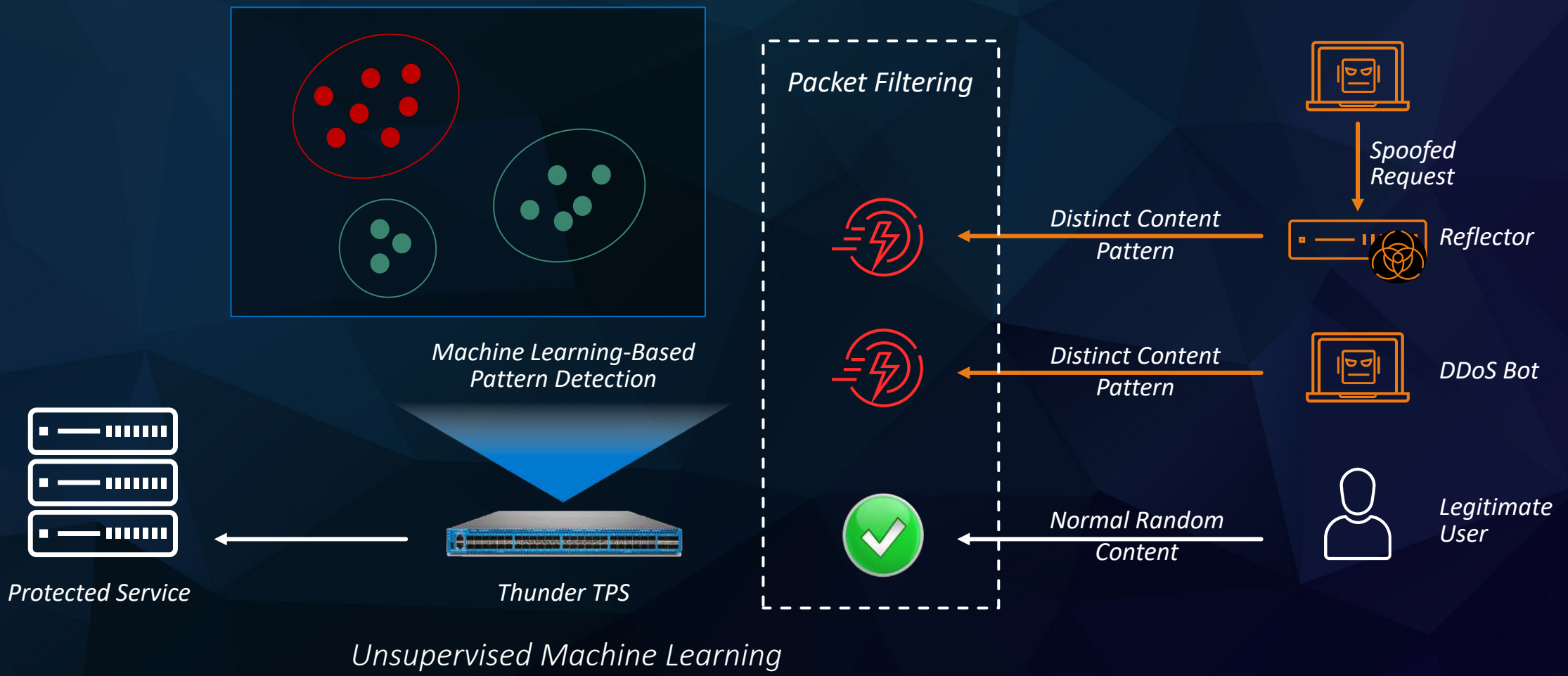
Legitimate User

Protected Service

Thunder TPS

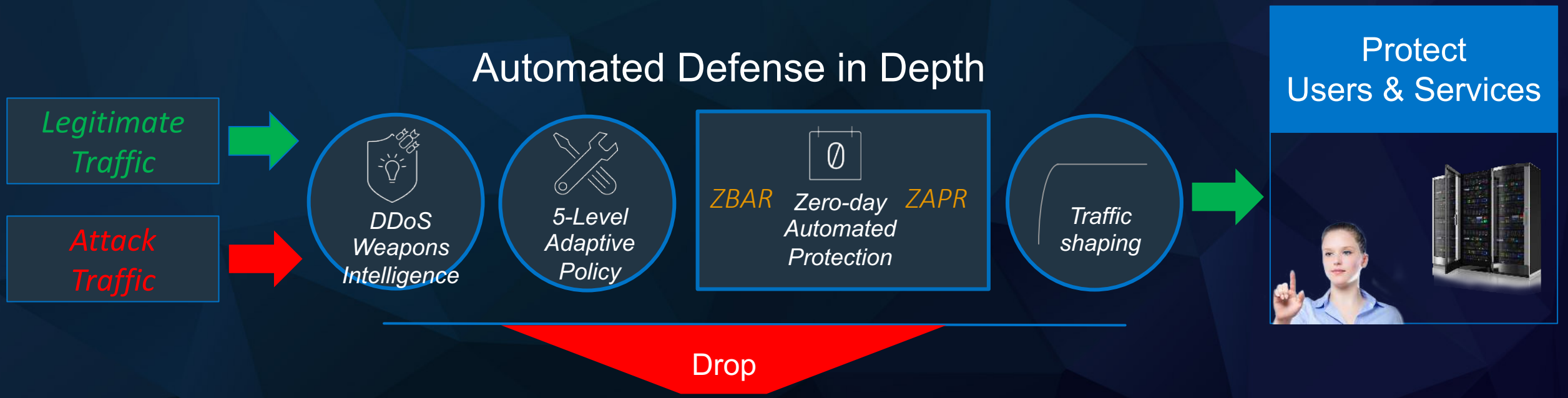
Rapid mitigation under 10 seconds

ZERO-DAY ATTACK PATTERN RECOGNITION (ZAPR)



Unsupervised Machine Learning

A10 MULTI-MODAL DDOS DEFENSE



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™