

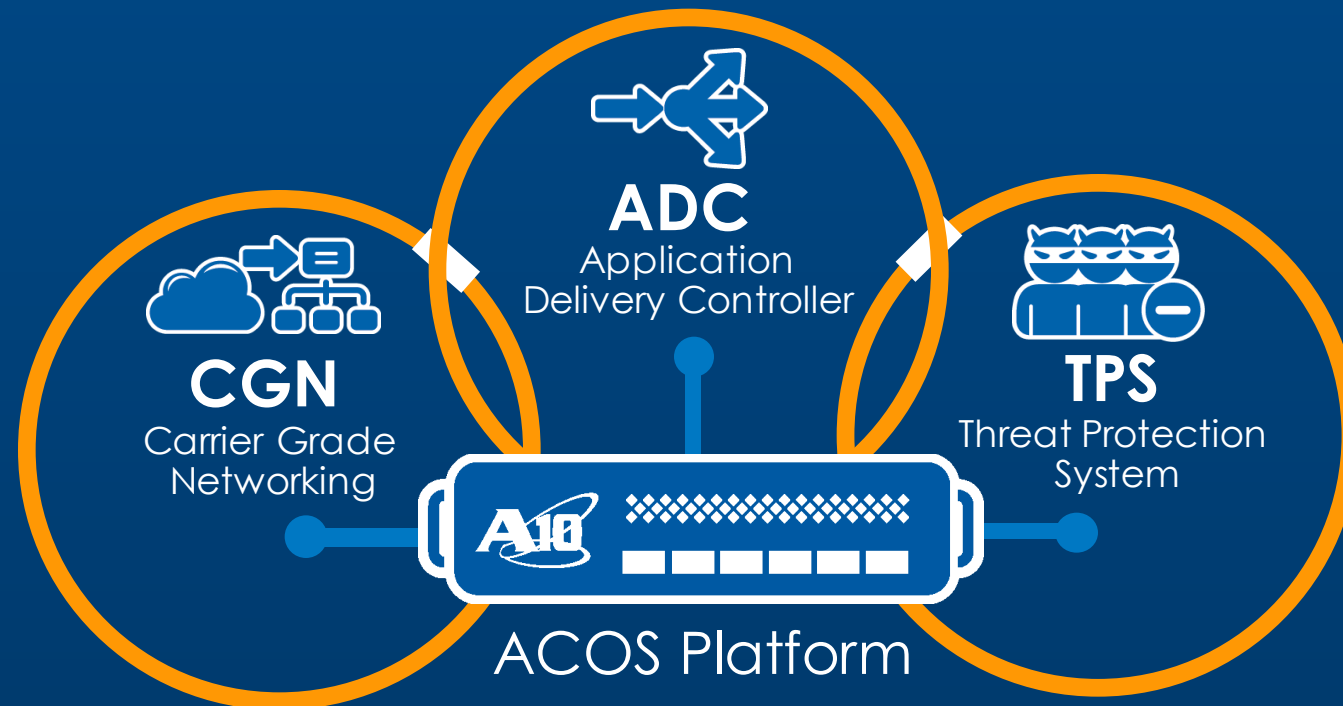
# Multi-vector DDoS Protection with Thunder TPS

October 23, 2015

Florian Hartmann  
Senior Systems Engineer DACH / EE



# A10 Product Portfolio Overview



## Product Lines

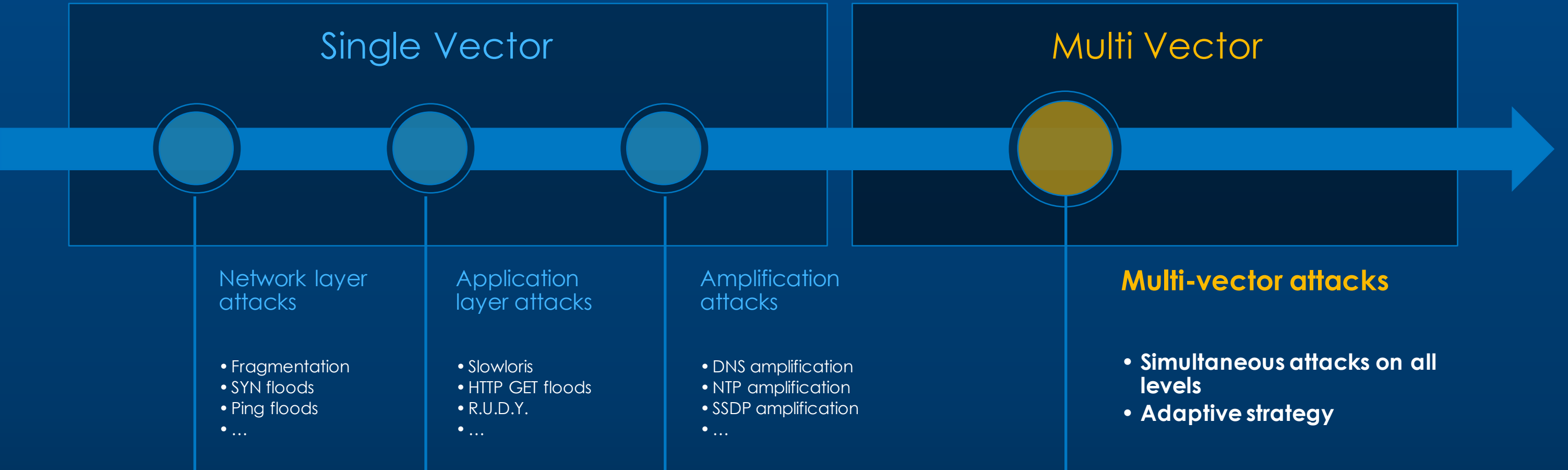
- ADC – Application Acceleration & Security
- CGN – IPv4 Extension / IPv6 Migration
- TPS – Network Perimeter DDoS Security

## Application Networking Platform

- Performance
- Scalability
- Extensibility
- Flexibility

## IT Delivery Models

# DDoS Attacks have Evolved



# Multi-Vector Attacks Are Here

## 5 Vectors

Gambling Site  
100 Gbps  
Q2 2014



**Online gambling site hit by five-vector  
DDoS attack peaking at 100Gbps**



# Multi-Vector Attacks Are Here

## 2 Vectors

**Educational Institutions**

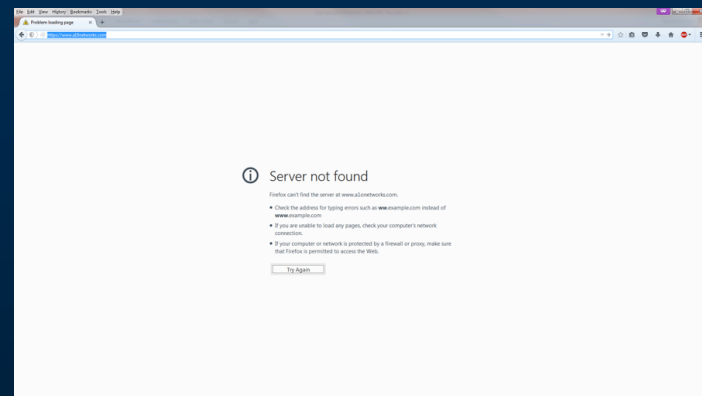
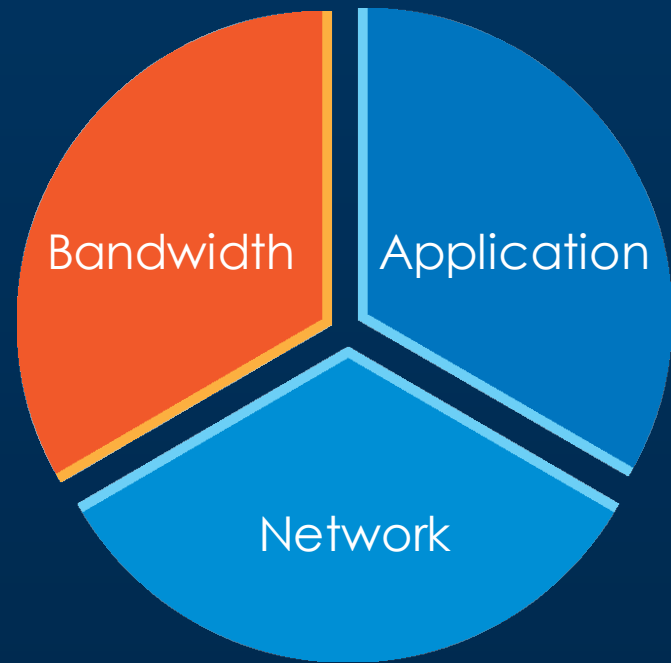
**XOR Botnet**

150+ Gbps attack

Q4 2015

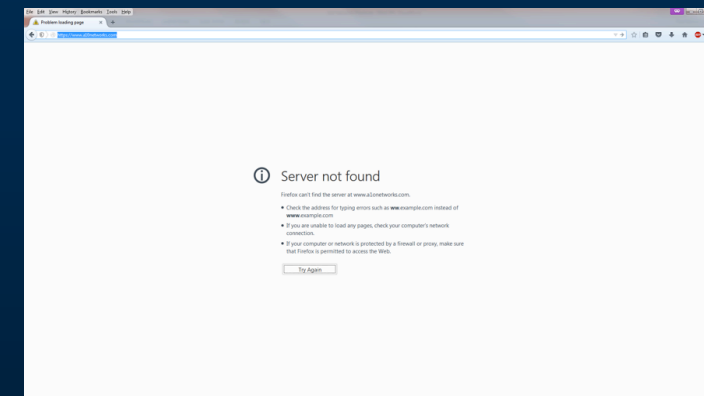
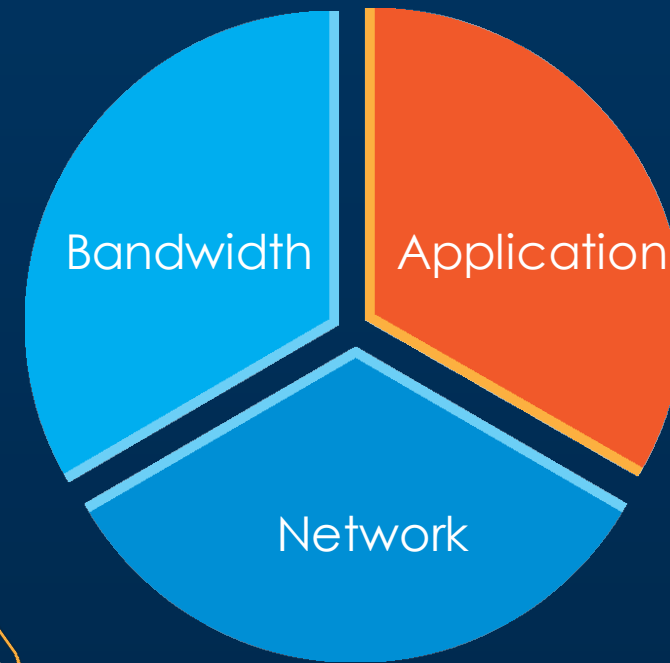
**XOR DDoS Botnet Launches  
20 Attacks A Day**

# Adaptive



and

# Simultaneous



What you need for

# True MVP

---

**Protect**  
against  
**full** attack  
**spectrum**

**Agile** and  
**rapid**  
action

**Efficient**

# Metrics that Matter for True MVP

---

60

Hardware (FTA)  
Mitigations

48

Cores

1.2

Tbps

223

Mpps

64k

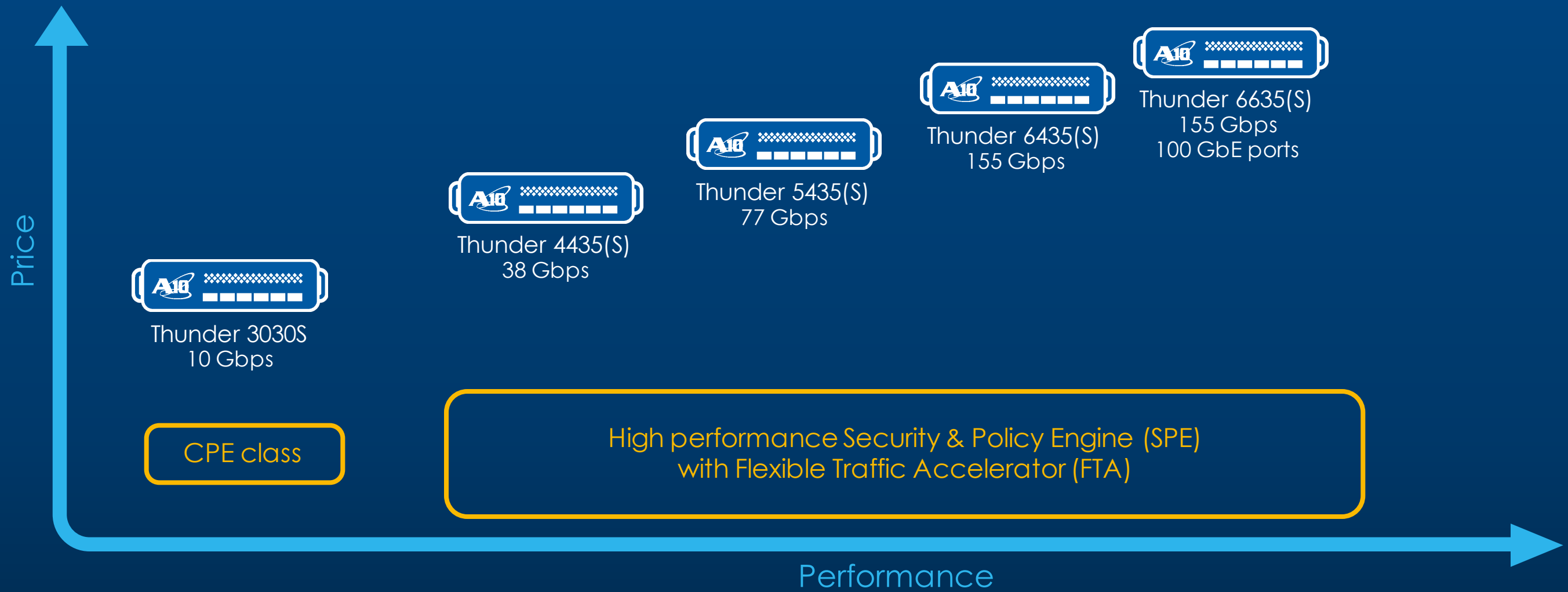
Protected  
Objects

100

GbE  
Ports



# Thunder TPS Appliances

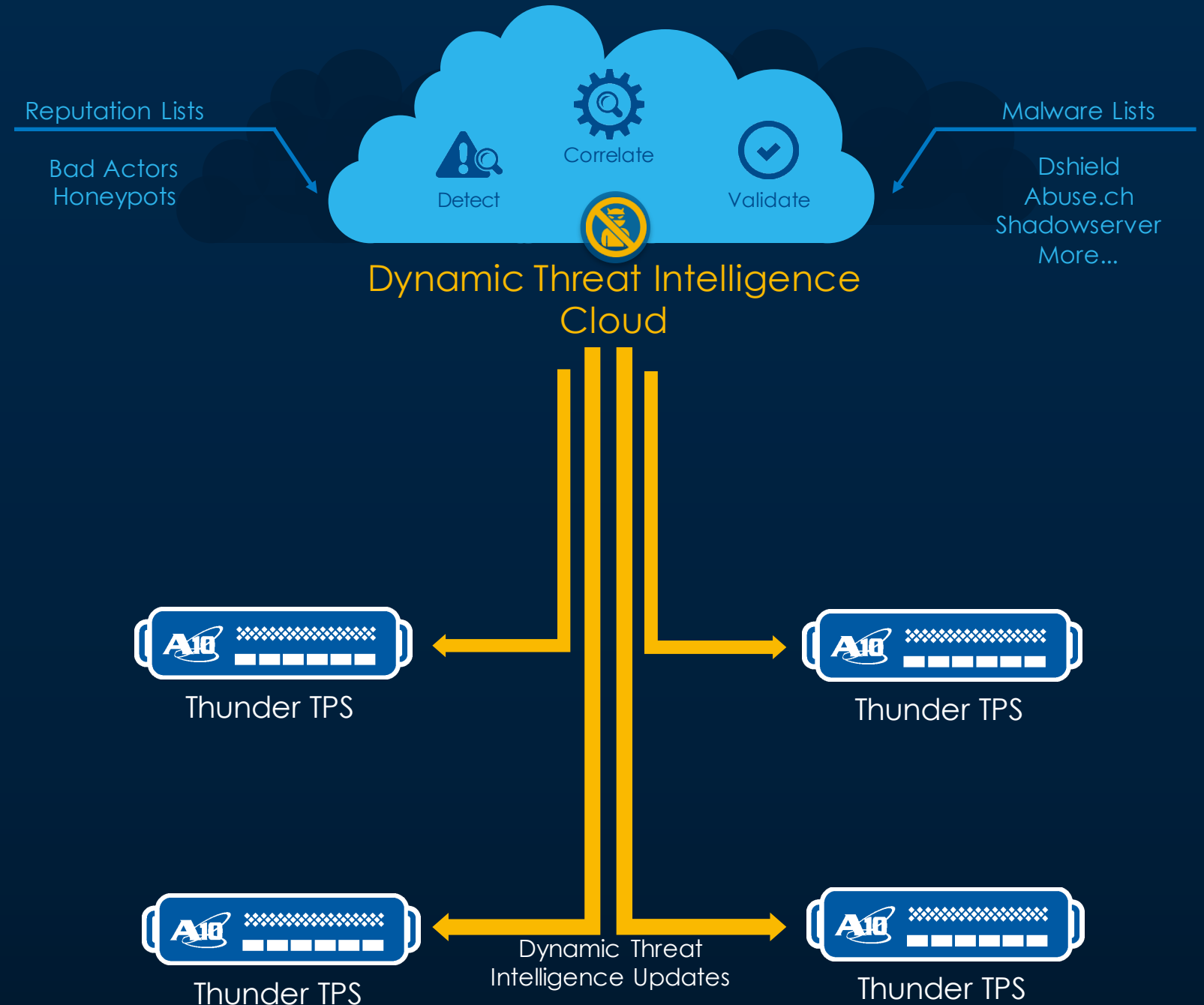


# Increase Security Efficacy with A10 Threat Intelligence Service

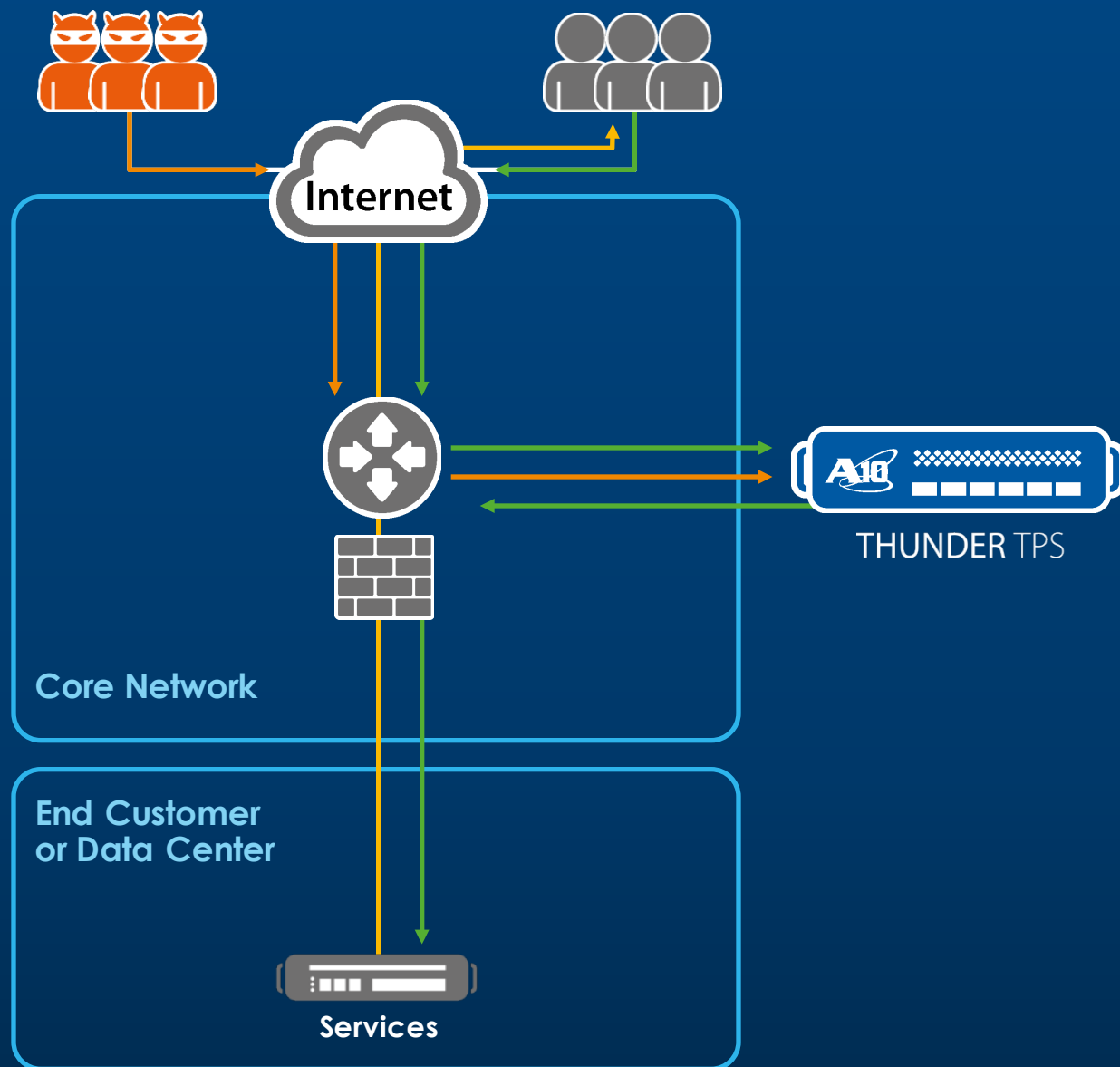
- Collective intelligence from millions of devices
- Block threats before they happen
- Increase TPS effectiveness and capacity



Powered by ThreatSTOP



# Asymmetric Proactive Deployment



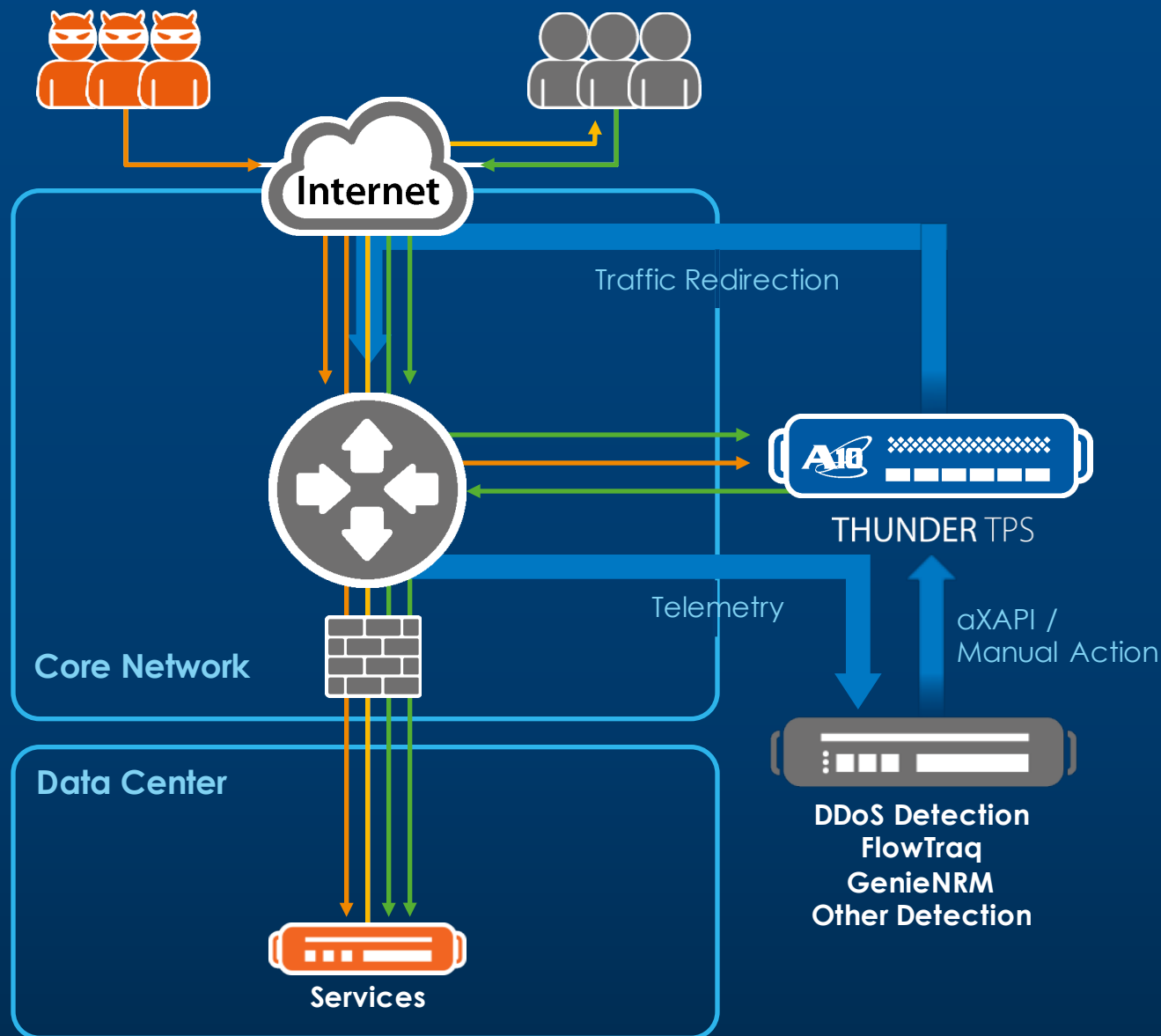
## Preferred deployment model

- Always-on protection
- Full ingress traffic visibility, no sampling
- No 3<sup>rd</sup> party detection required
- Sub-second time to mitigate
- Low latency
  - 60  $\mu$ s average, WAN is milliseconds

## Use Case

- All-in-one network-wide DDoS protection
- Augment/offload legacy DDoS mitigation

# Asymmetric Reactive Deployment



## Flow-based detection

- Scalable, centralized solution for DDoS mitigation
  - Backhaul traffic to a central location
  - Oversubscribed protection bandwidth
  - Not in path during peace time
- Limitations of sampling detection
  - Less accurate
  - Longer time to mitigate
  - Fine for volumetric
  - Not great for slow-and-low application layer attacks
- Detection Partners
  - FlowTraq
  - GenieNRM





Thanks!