Cyber Security Challenges in 4th Industrial Revolution / DDoS attacks – Protection and Mitigation Measures

Charalampos Gkevrekis

ICT Manager at AdaptIT Group of Companies

Agenda

- Corporate presentation of AdaptIT…briefly
- DDoS attacks – What they are
- DDoS Attacks Trends and Challenges
- ADAPTIT/NETSCOUT Solutions for DDoS Protection
- Indicative customers in Greece

ADAPTIT
EVOLUTION DRIVERS

AdaptIT Group of Companies

ADAPTIT
EVOLUTION DRIVERS

FACTS

ABOUT THE COMPANY

- Established in 2005
- Unique Specializations in Telecom Market
- Over 80 fully qualified employees & certified engineers
- 10 years collaboration with Telco Operators in Greece and abroad
- Extended Support wide area of critical applications

- Present as an exhibitor at major Telecom & IT International Exhibitions

- Participated in 2012, 2013, 2014, 2015, 2016, 2017, 2018 Mobile World Congress in Barcelona.

ADAPTIT
EVOLUTION DRIVERS

ADAPTIT
GROUP OF COMPANIES

The ADAPTIT group is a combination of 4 companies operating as a single entity through a common source of control, with a wide range of activities in telecommunications, technology products, hardware and software production.

It is now an International Group with a strong presence in many countries and with many different companies:

ADAPTIT, TELCOSERV, TELCOSERV CONSTRUCTIONS, HELIOS EUROPE.

FACTS

ACTIVE MEMBER OF :

- Hellenic Federation of Enterprises (ΣΕΒ)
- American Hellenic Chamber of Commerce
- Hellenic Chinese Chamber

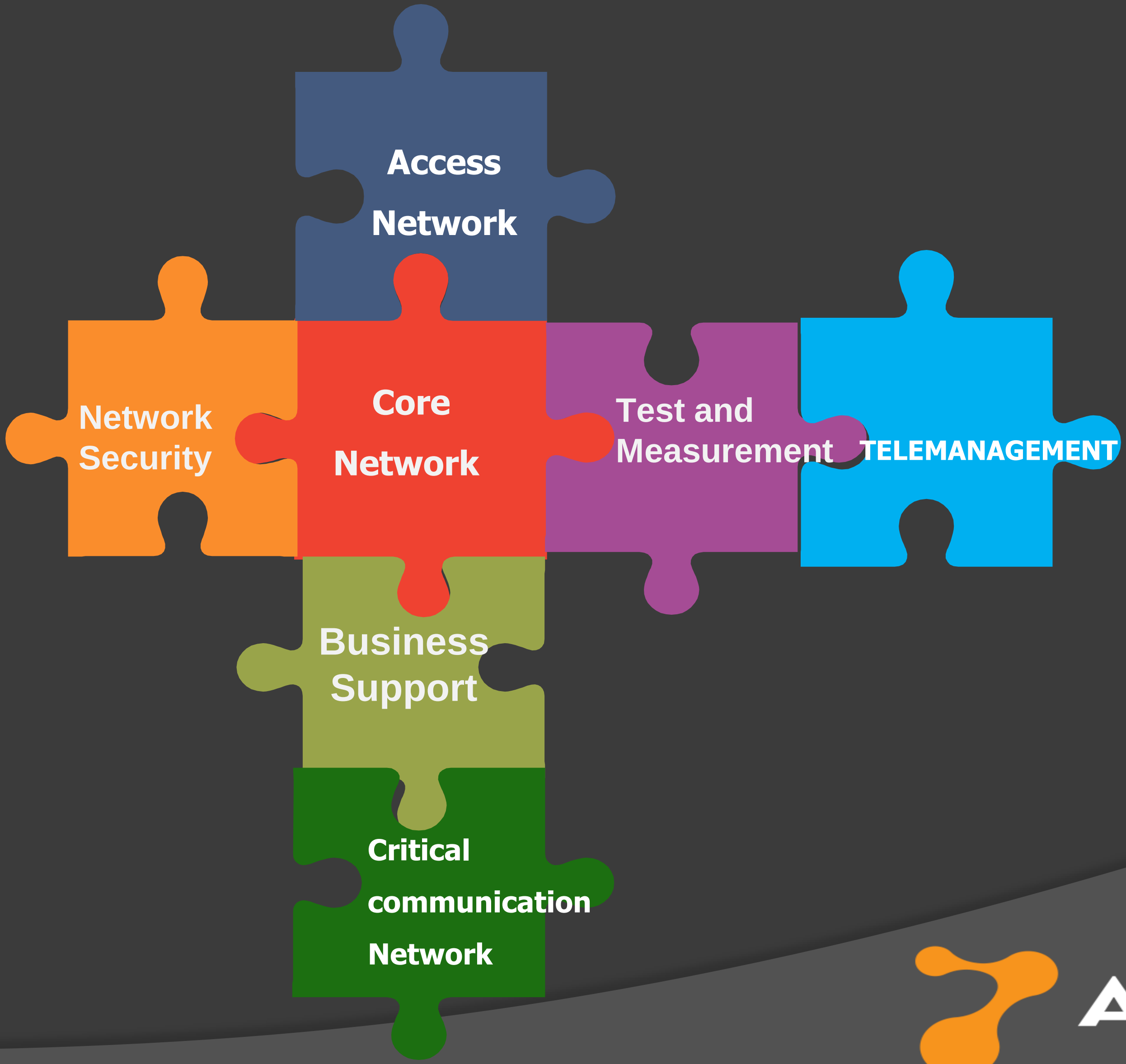
ADAPTIT
EVOLUTION DRIVERS

ADAPTIT : SYSTEMS INTEGRATOR

ADAPTIT is the partner of choice for several reputed ICT solutions manufacturers, while we constantly expand our partners portfolio.

We specialize in combining technology components into an overarching system. We analyze, design and implement turn-key solutions for our clients, while always providing high quality services.

SOLUTIONS FOR:



ADAPTIT
EVOLUTION DRIVERS

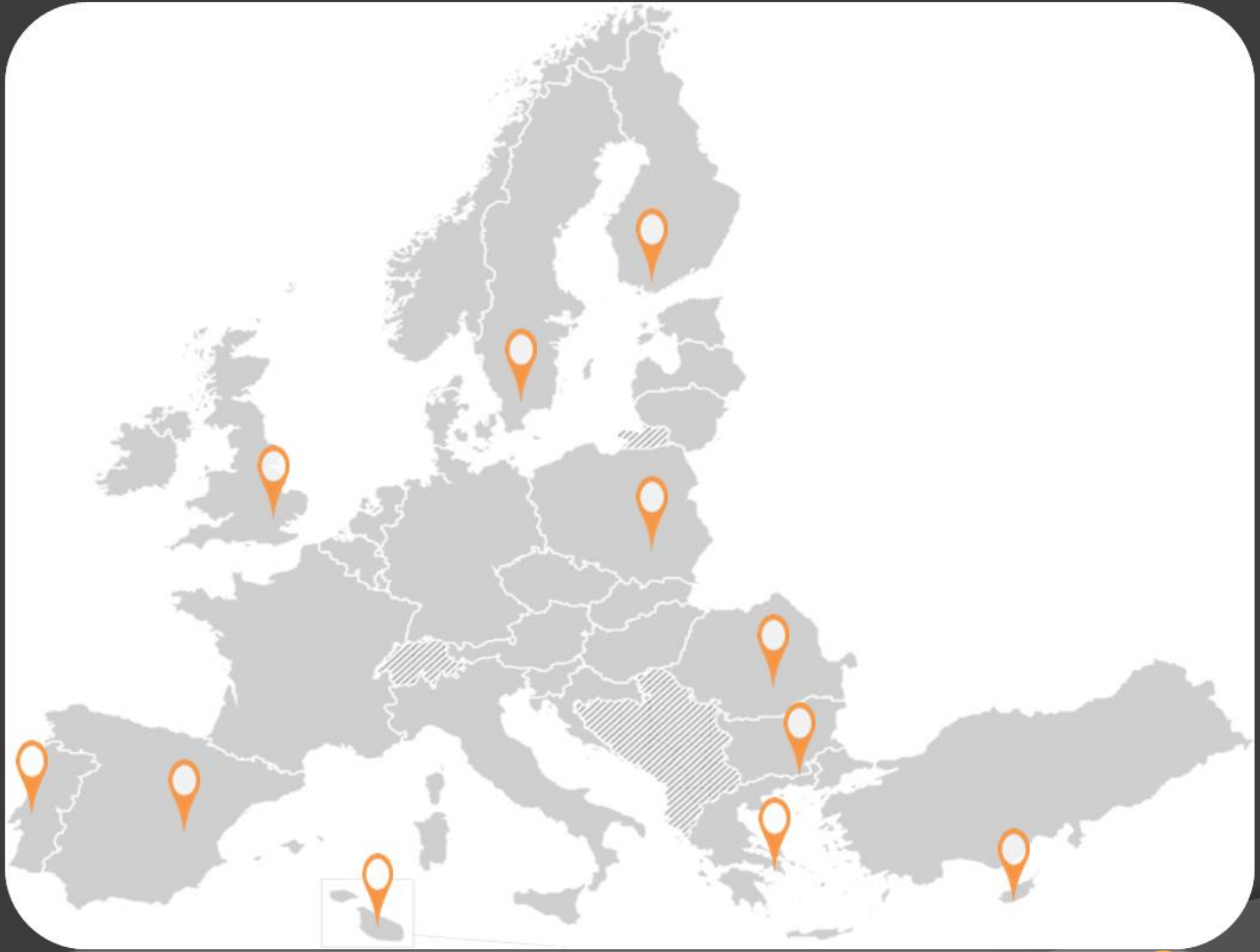
ADAPTIT GROUP:

1. Employs very well educated, trained and experienced personnel.
2. Co-Operates with the most prestigious and well named vendors in the ICT industry.
3. Deliver the most demanding projects on a turn key basis including:

- Solution Design
- Equipment Supply
- Installation – Commissioning
- Operation Support

ADAPTIT
EVOLUTION DRIVERS

ACTIVITY IN THE EUROPEAN REGION



ADAPTIT
EVOLUTION DRIVERS

EU FUNDING PROJECTS

ONTIC : Combining academic and industrial expertise through Europe, ONTIC developed innovative machine-learning (ML) algorithms for IP traffic characterization and demonstrated their applicability in the context of dynamic network management; it also made available a 0.5 PB dataset of actual network traffic traces. ADAPTIT led the Big Data architectural activities and contributed to use case development from the perspectives of a SME solution provider.

Chariot : TELSCOSERV with PANTHORA are participating in an international consortium of companies and organizations including IBM HQ, Trenitalia, AIA, Aspisec. The consortium will develop a secure industrial IoT communication platform. TELCOSERV is the IoT Gateway Provider playing an active role both in the development of specific parts of the solution (API) and in the Livings Labs proposed in the context of the proposal of this particularly important Research Program.

Pelagus: Platform for the sustainable collective use of swimming water and improvement of bathers' experience. The purpose of the PELAGUS Collective Awareness Platform is the sustainable collective use of bathing water, improving the experience of tourists and visitors in the coastal areas of the country, using sensors, IoT technology and crowdsourcing.

ADAPTIT
EVOLUTION DRIVERS

ADAPTIT Consultancy services expertise fields

ADAPTIT professional services department provides high quality consultancy services to vendors and operators in the following fields:

1. SON (Self Optimizing Networks).
2. Geolocation Platforms
3. Radio Network Planning and Optimization.
4. Small Cell and FEMTO networks.
5. Access and Transmission.
6. Network Security.

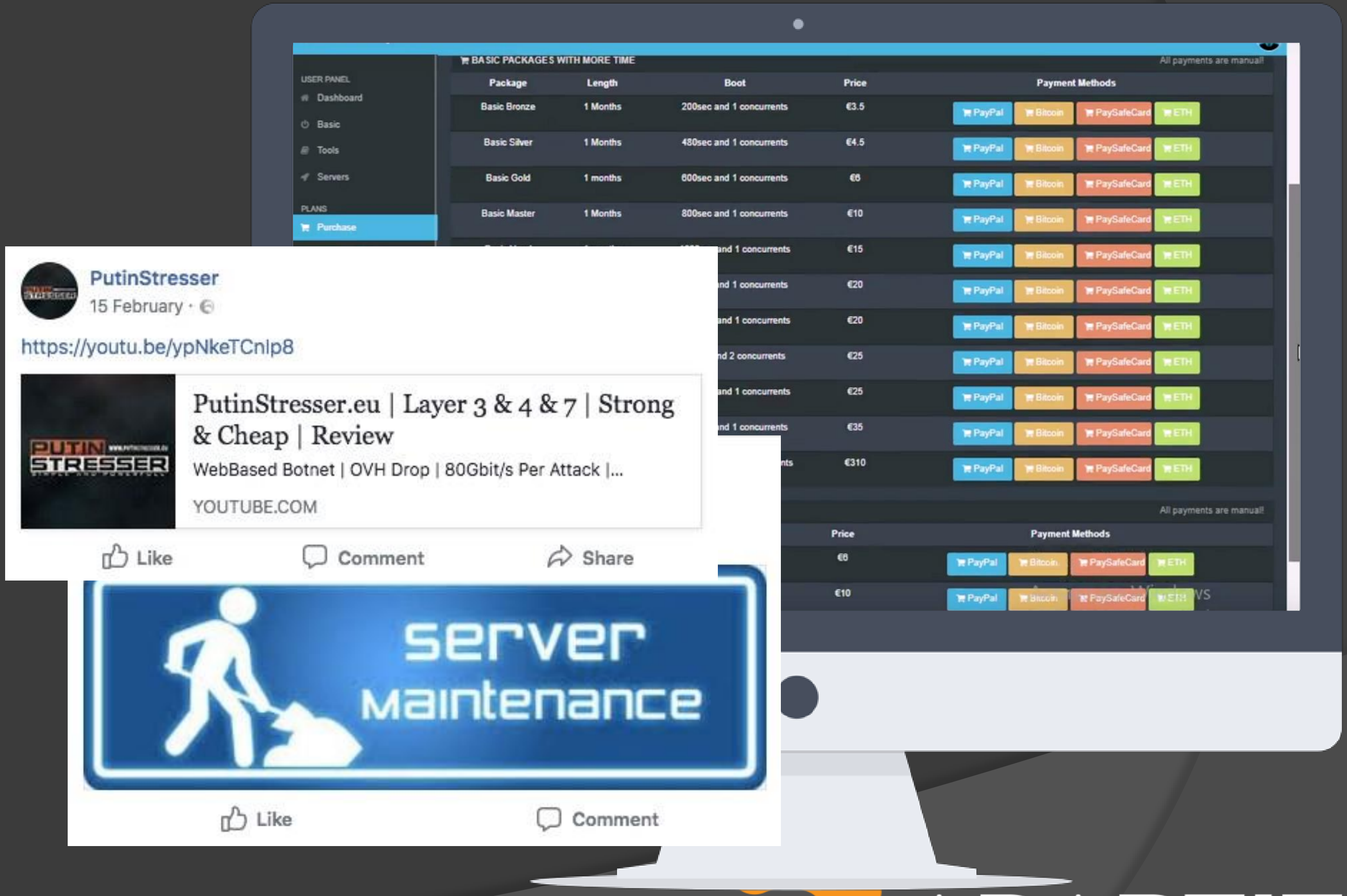
ADAPTIT
EVOLUTION DRIVERS

Discovering DDoS Attacks

ADAPTIT
EVOLUTION DRIVERS

How easy it really is to launch a DDoS? Really, really easy!!!

- Easy to find
- Clear and modern user interface
- Several locations
- Many attack vectors
- Multiple payment options
- Support Center
- Community Manager



BASIC PACKAGES WITH MORE TIME

All payments are manual!

Package	Length	Boot	Price	Payment Methods
Basic Bronze	1 Months	200sec and 1 concurrents	€3.5	PayPal Bitcoin PaySafeCard ETH
Basic Silver	1 Months	480sec and 1 concurrents	€4.5	PayPal Bitcoin PaySafeCard ETH
Basic Gold	1 months	600sec and 1 concurrents	€6	PayPal Bitcoin PaySafeCard ETH
Basic Master	1 Months	800sec and 1 concurrents	€10	PayPal Bitcoin PaySafeCard ETH
		and 1 concurrents	€15	PayPal Bitcoin PaySafeCard ETH
		nd 1 concurrents	€20	PayPal Bitcoin PaySafeCard ETH
		and 1 concurrents	€20	PayPal Bitcoin PaySafeCard ETH
		nd 2 concurrents	€25	PayPal Bitcoin PaySafeCard ETH
		and 1 concurrents	€25	PayPal Bitcoin PaySafeCard ETH
		nd 1 concurrents	€35	PayPal Bitcoin PaySafeCard ETH
		nts	€310	PayPal Bitcoin PaySafeCard ETH

All payments are manual!

Price	Payment Methods
€6	PayPal Bitcoin PaySafeCard ETH
€10	PayPal Bitcoin PaySafeCard ETH

PutinStresser
15 February ·

https://youtu.be/ypNkeTCnlp8

PutinStresser.eu | Layer 3 & 4 & 7 | Strong & Cheap | Review
WebBased Botnet | OVH Drop | 80Gbit/s Per Attack |...
YOUTUBE.COM

ADAPTIT
EVOLUTION DRIVERS

Dutch banks crippled by DDoS Attack
January 2019

Myth: ABN Amro CEO Kees van Dijkhuizen said that “attacks like these probably cost the perpetrators tens of millions of euros”, fueling speculation that the attack had come from a nation state.

Fact: But the truth has proved rather less spectacular when police arrested an 18-year-old known as Jelle S in his hometown of Oosterhout. Jelle claimed to have bought a ready-made “stresser” DDoS package on the dark web for which he had paid €50 data to victims a week to send 50-100Gb/s of data to victims.

What is it used for? Attackers - Victims

- Mafias
- Hacktivists
- Competition
- Gamers
- Students
- Former employee
- Ransom
- Political Statement
- Business impact
- Get rid off the opponent
- To skip tests
- Angry, Vengeance

“A 17-year-old high school boy may face state and federal charges for allegedly having paid a third party to launch a distributed denial of service (DDoS) attack that crippled the West Ada school district in Idaho, US, for a week and a half earlier this month.”

Some students had to take the tests multiple times.

Source: Naked Security

ADAPTIT
EVOLUTION DRIVERS

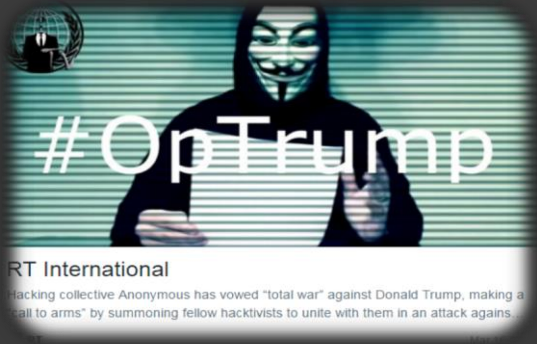
The cyber refection

Every Physical Geo-Political Event…

Has a cyber reflection…

ADAPTIT
EVOLUTION DRIVERS

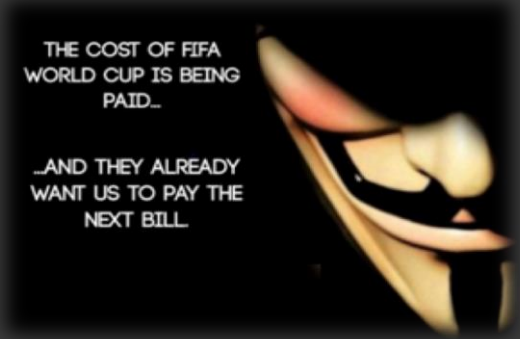
Every event has a cyber reflection



RT International

Hacking collective Anonymous has vowed "total war" against Donald Trump, making a "call to arms" by summoning fellow hacktivists to unite with them in an attack agains...

...onymous - #OpFerguson
WE ARE LEGION • WE DO NOT FORGIVE • WE DO NOT FORGET • EXPECT US • WE ARE ANONYMOUS •



THE COST OF FIFA WORLD CUP IS BEING PAID...

...AND THEY ALREADY WANT US TO PAY THE NEXT BILL.

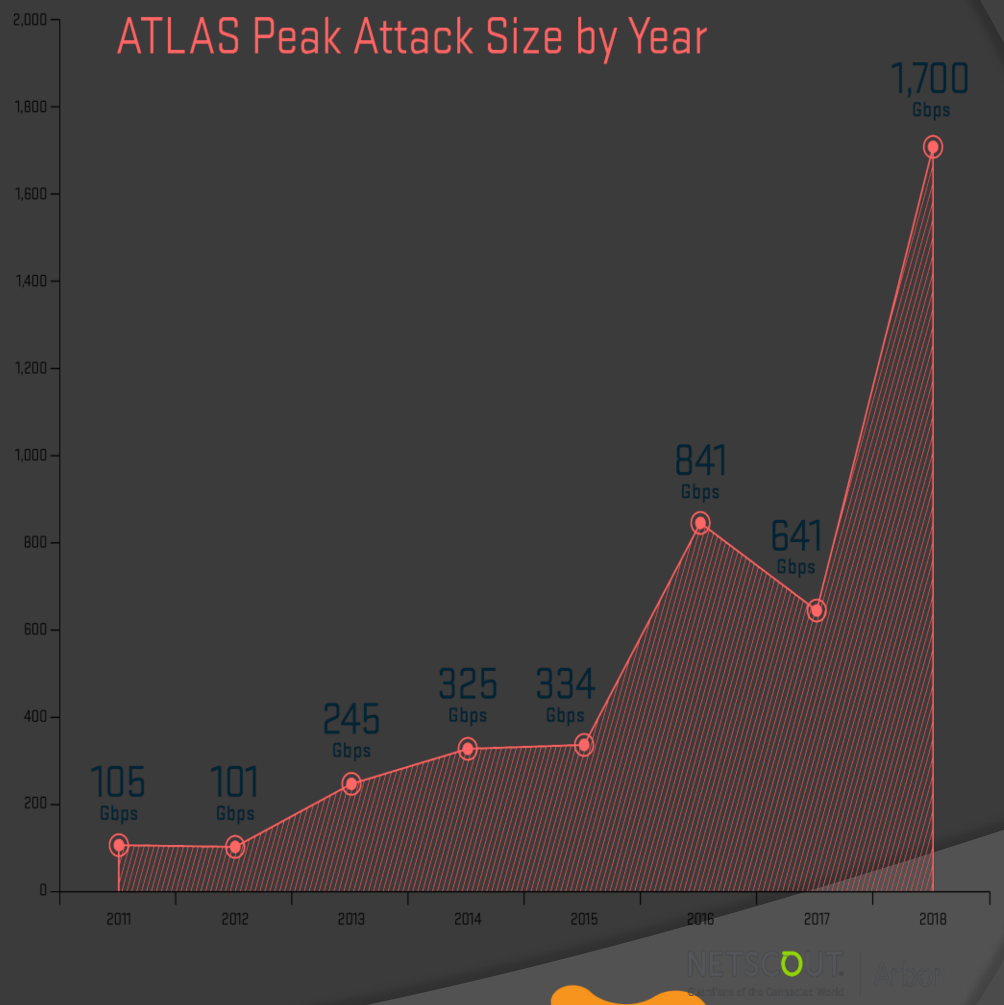
Attack targets were not necessarily the events themselves,

but organizations tangentially associated with the events.

Peak attacks

2018 was a record year…

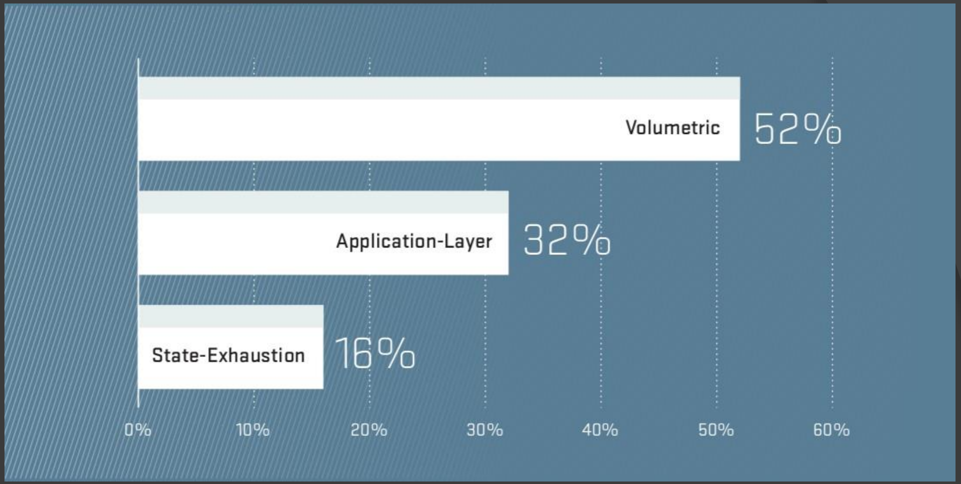
- New weaponized attack vectors like Memcached
- Targets a vulnerability in a Datacenter service used to improve request performance
- Amplification factor can go up to 1:500.000 (maximum achieved in lab environment)
- 1Mbps can generate 50Gbps
- **Not the most dangerous attack**



Complexity and subtlety

DDoS attacks are organic

- DDoS attack change during the attack
- The attacker keeps an eye on the victims resources availability
- The vector will change to defeat the countermeasures
- 48% of attacks can be stopped on site
- 52% may require help from the ISP



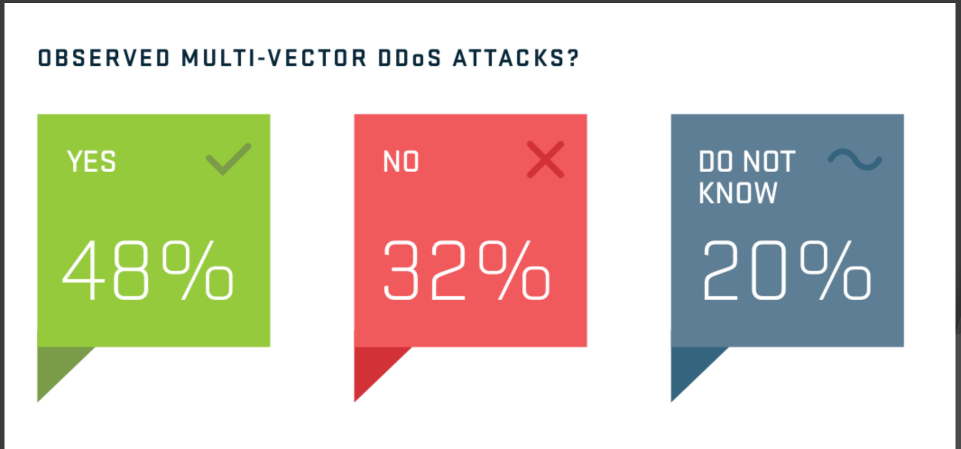
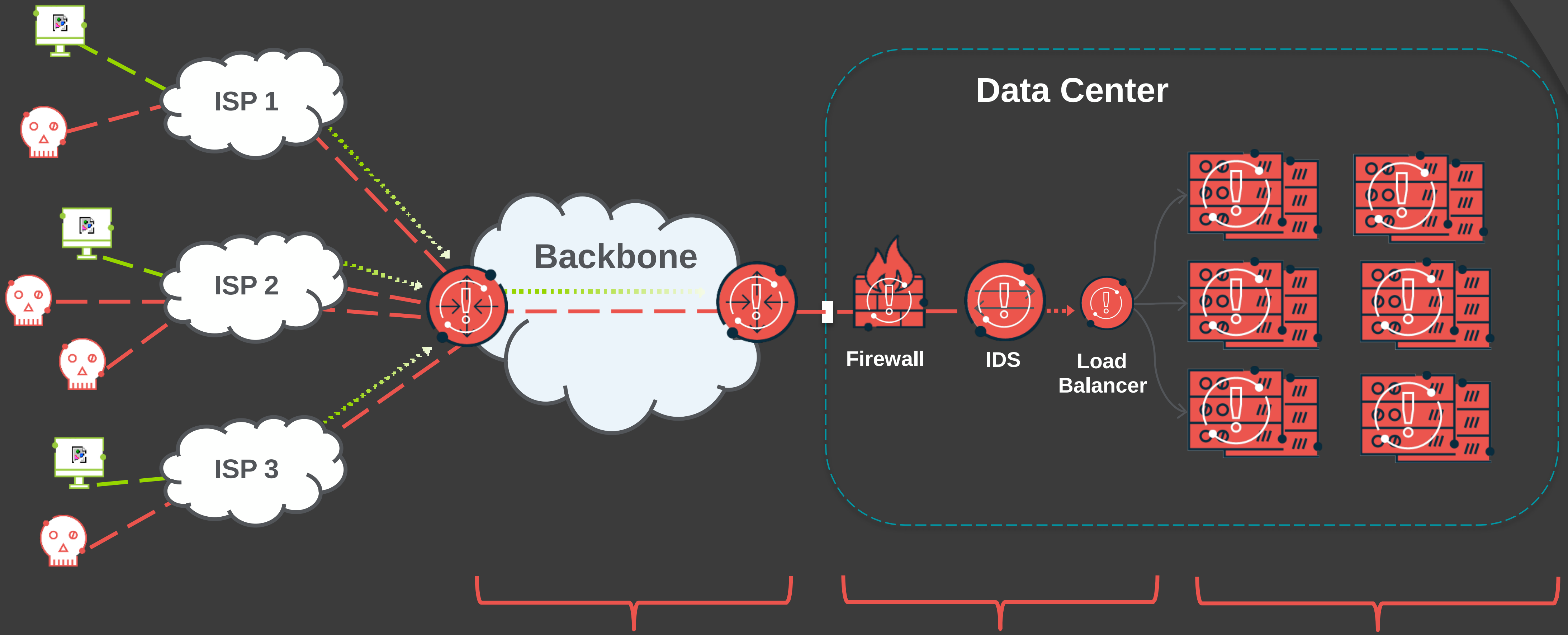


Figure 72 Multi-Vector Attacks

How to counter every type of attack



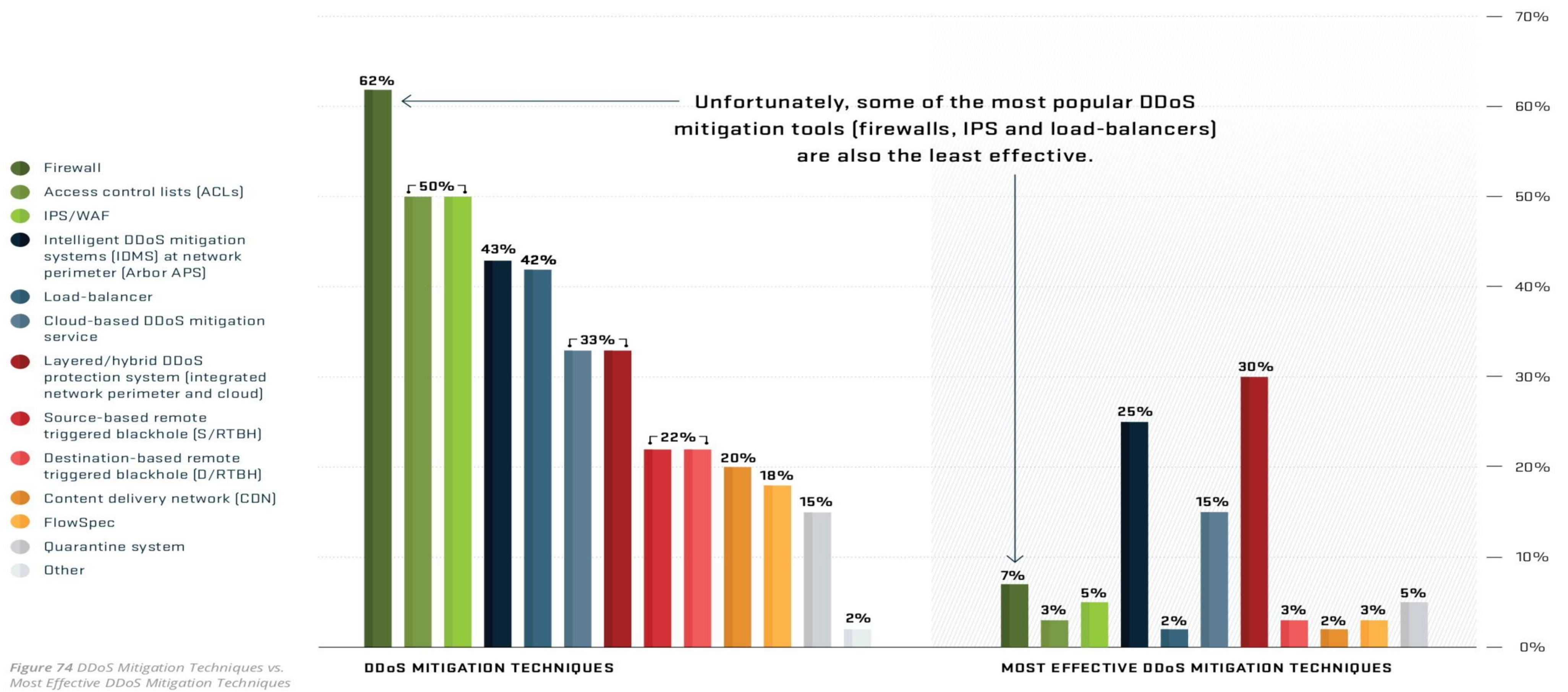
<u>Saturation</u>
Volumetric or Flooding Attack

<u>Exhaustion of State</u>
L4 – L7
Crashes stateful devices (Load Balancers, Firewalls, IPS/IDS)

<u>Exhaustion of Service</u>
L4 – L7
Application Layer or Slow & Low Attack, Crashes application servers

ADAPTIT
EVOLUTION DRIVERS

Most used mitigation tools are the least effective



Unfortunately, some of the most popular DDoS mitigation tools (firewalls, IPS and load-balancers) are also the least effective.

Figure 74 DDoS Mitigation Techniques vs. Most Effective DDoS Mitigation Techniques

ADAPTIT
EVOLUTION DRIVERS

DDoS Attacks Trends and Challenges

ADAPTIT
EVOLUTION DRIVERS

DDoS Attack Trends & Country Targets – 2H 2019

Attacks by Region

Attack Size Trends

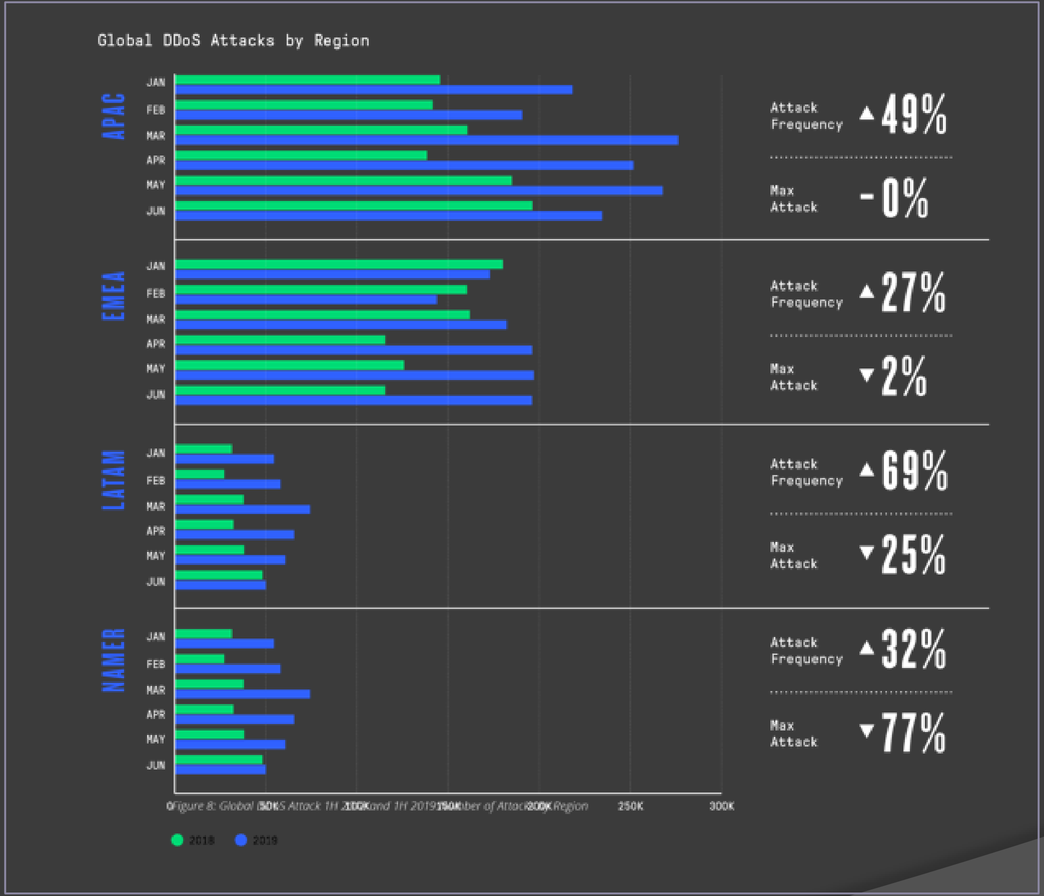
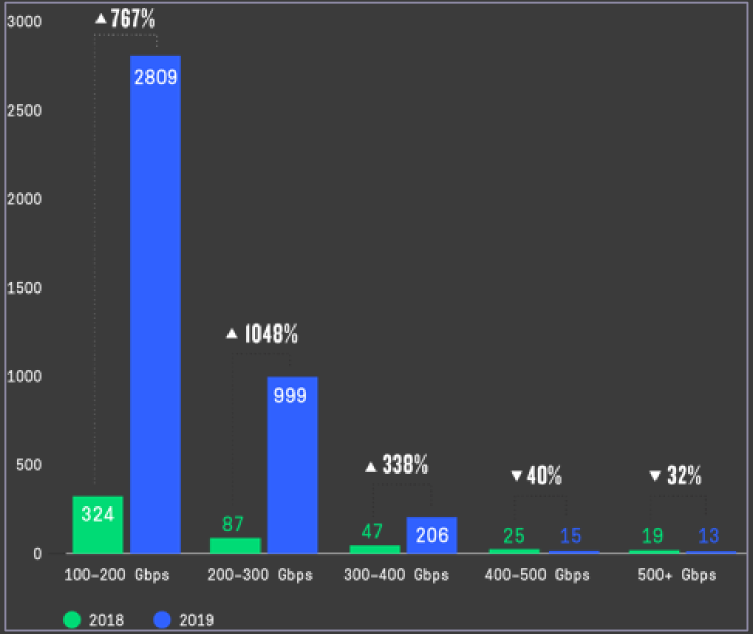
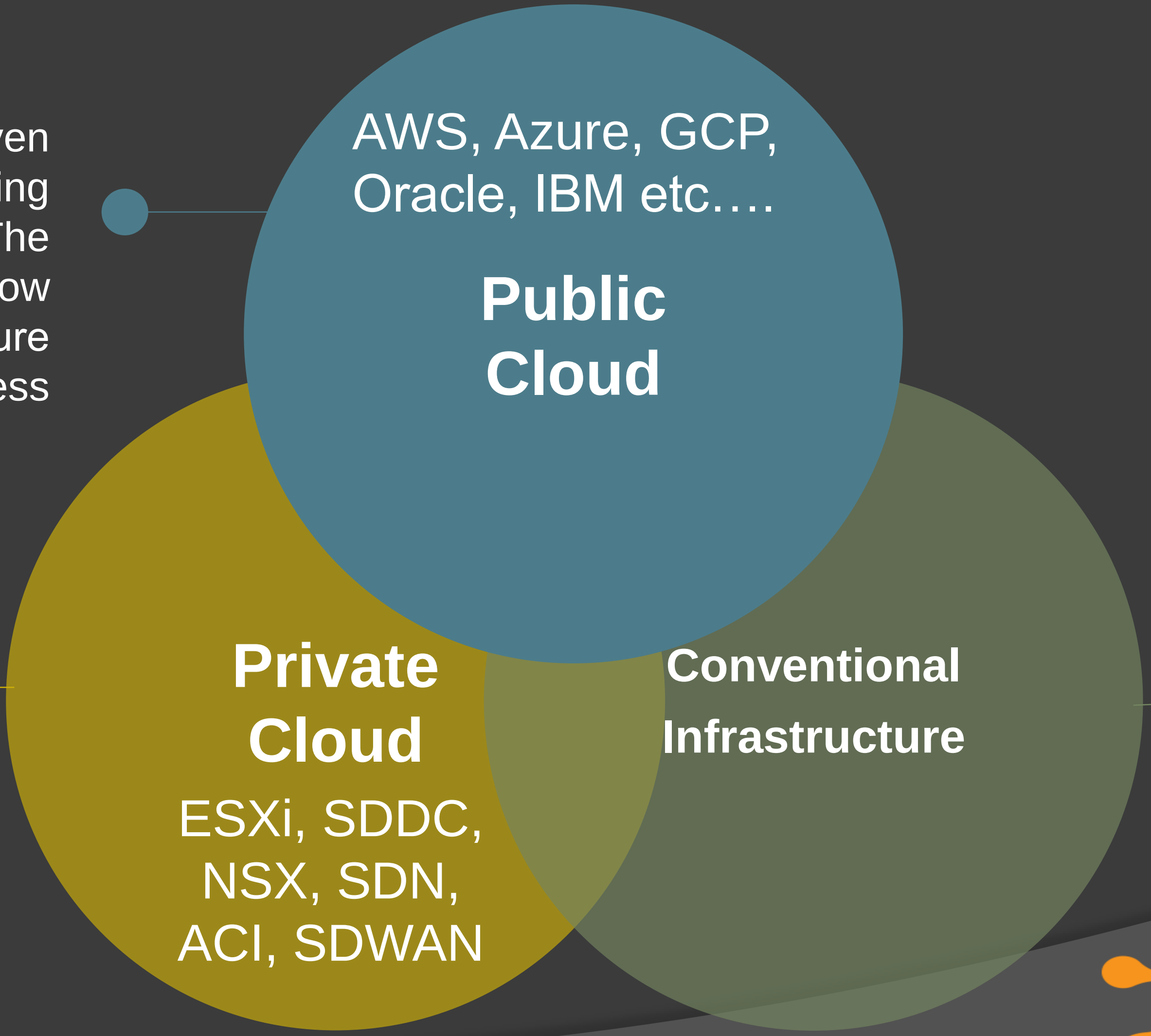


Figure 8: Global DDoS Attack 1H 2018 and 1H 2019 Number of Attacks by Region



ADAPTIT
EVOLUTION DRIVERS

The Hybrid IT Challenge



Often introduced and driven by Line of Business resulting in multiple providers. The birth of Shadow IT – but now a critical part of IT's future success

AWS, Azure, GCP, Oracle, IBM etc.…

Public Cloud

Sometimes equated with virtualization and driven by development and server teams

Private Cloud

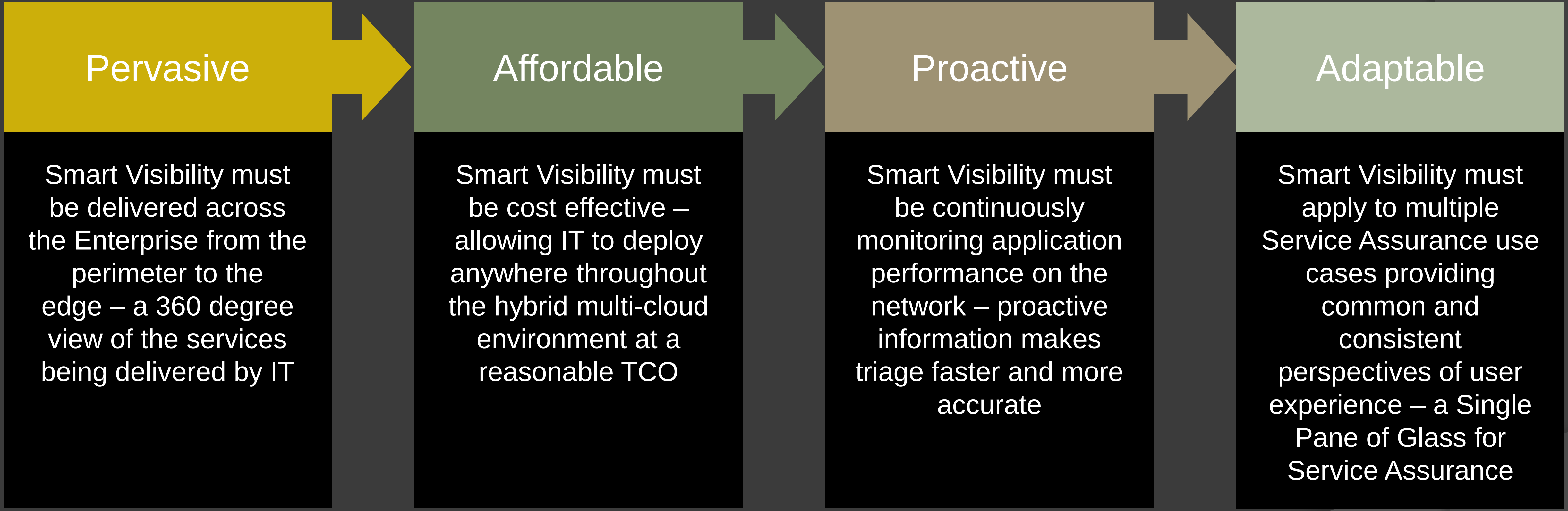
ESXi, SDDC, NSX, SDN, ACI, SDWAN

Conventional Infrastructure

Still a critical part of the service delivery chain and will be in place for many years

ADAPTIT
EVOLUTION DRIVERS

Smart Visibility for Services Assurance



Pervasive

Smart Visibility must be delivered across the Enterprise from the perimeter to the edge – a 360 degree view of the services being delivered by IT

Affordable

Smart Visibility must be cost effective – allowing IT to deploy anywhere throughout the hybrid multi-cloud environment at a reasonable TCO

Proactive

Smart Visibility must be continuously monitoring application performance on the network – proactive information makes triage faster and more accurate

Adaptable

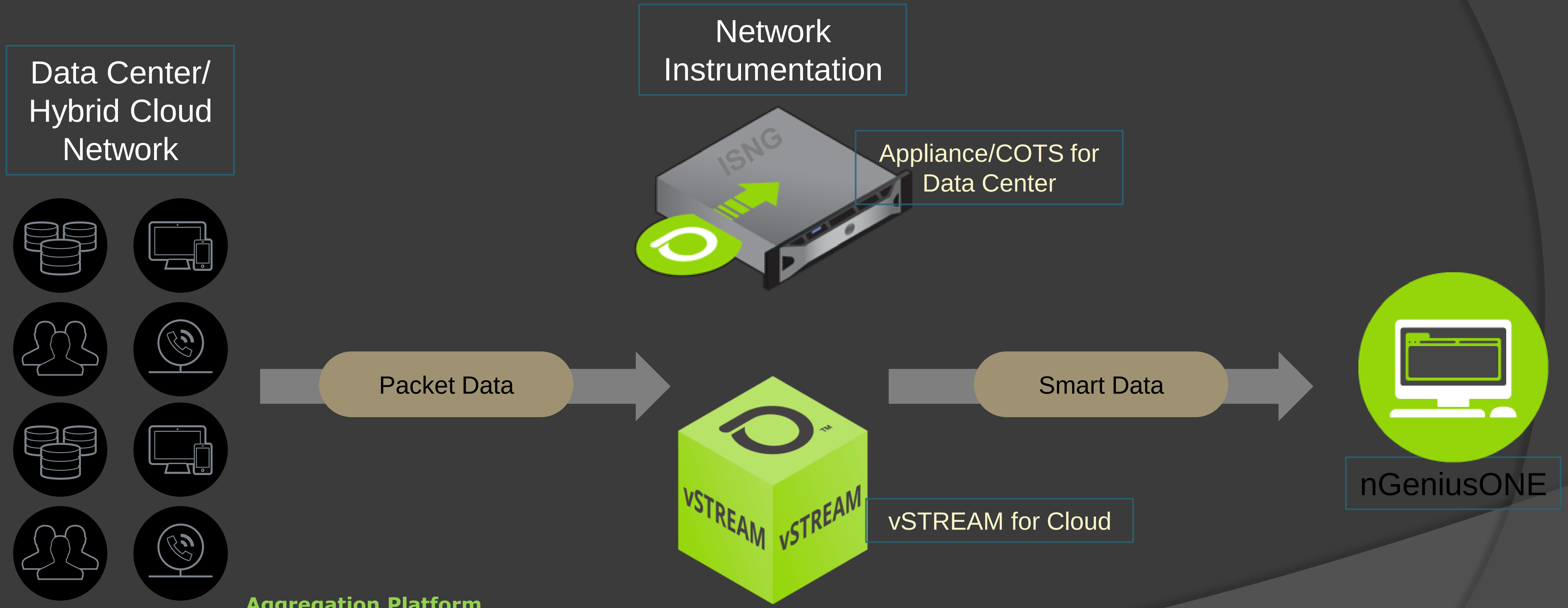
Smart Visibility must apply to multiple Service Assurance use cases providing common and consistent perspectives of user experience – a Single Pane of Glass for Service Assurance

Smart Visibility begins with Smart Data

ADAPTIT
EVOLUTION DRIVERS

Typical Deployment Model for Data Center & Cloud

Shared or Standalone Network Instrumentation



Data Center/ Hybrid Cloud Network

Network Instrumentation

Appliance/COTS for Data Center

Packet Data

Smart Data

vSTREAM for Cloud

nGeniusONE

Aggregation Platform

- **Taps, Spans, Packet Flow Switch**

InfiniStreamNG Probes (ISNG)

- **Appliance, COTS, Virtual**
- **ASI+ - Network, Applications, Security, etc.**

nGeniusONE Application (NG1)

- **HTML5**
- **Apps-Based**

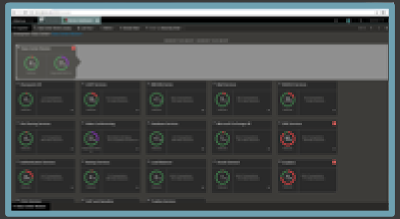
Smart Data

ASI Metrics

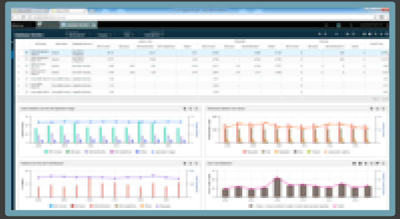
- Rich Meta-Data
  - KPI, Session, Packet
- Advanced Metrics
  - Application Response Time
  - Application Success, Failure
  - Application Errors
  - Network Response Time
  - Per protocol, per Message Type (i.e. URL)
  - Voice and Video QoE Metrics

Smart Data

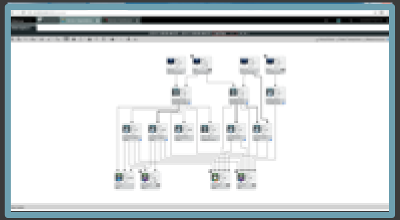
nGeniusONE – Using Smart Data



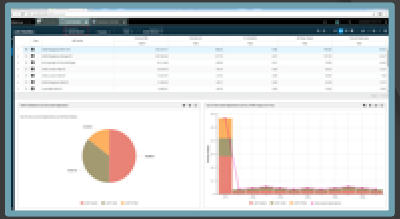
Dashboard



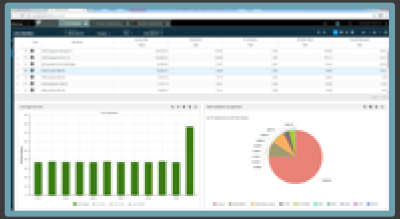
Service Monitor



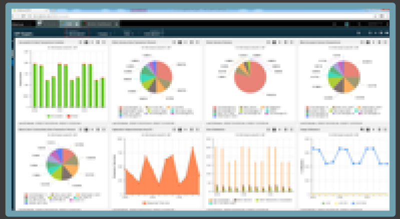
Dependency Map



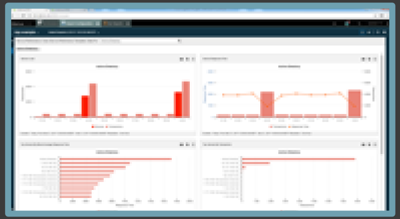
Traffic Discovery



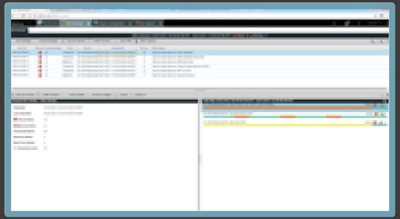
Link Monitor



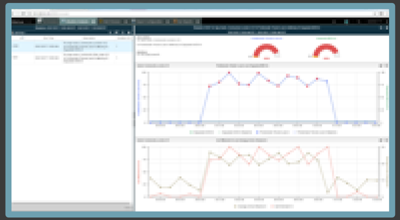
Grid



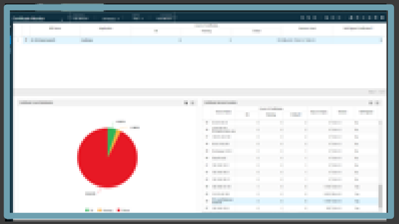
Reporting



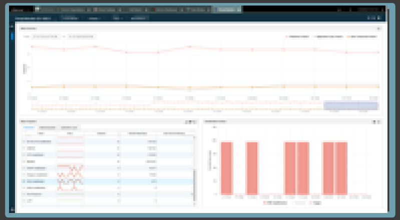
Alerting



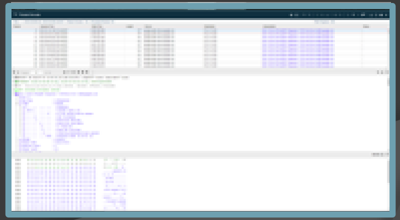
Situation Analysis



Certificate Monitor



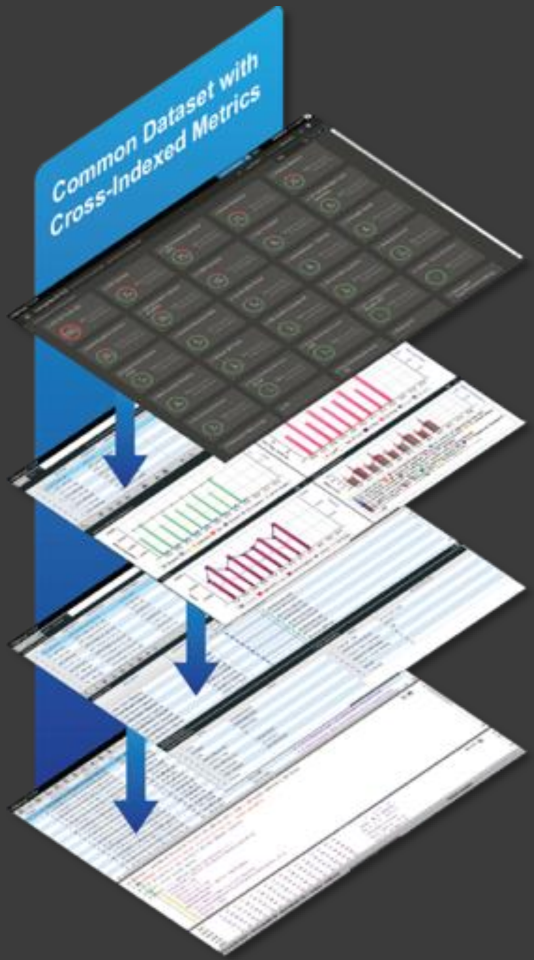
Security



Packet Forensics

ADAPTIT
EVOLUTION DRIVERS

nGeniusONE Service Driven Analysis Model



- **Service Dashboard**
  High-level visibility into critical services and performance issues
- **Service Monitors**
  Service Monitors identify key performance metrics to verify and correlate service Impact
- **Session Analysis**

  Perform granular user session tracing and analysis with hop-by-hop transaction and latency
- **Deep-Dive Packet Analysis**
  Expert packet-level analysis and decode for deep-dive investigation of service performance issues

ADAPTIT/NETSCOUT Solutions for DDoS Protection

ADAPTIT
EVOLUTION DRIVERS

NETSCOUT Solutions for DDoS Protection

18 Number of years Arbor has been delivering innovative security and network visibility technologies & products

#1 Industry leader in DDoS attack protection products.

98% Percentage of world's Tier 1 service providers who are Arbor customers

1/3 Amount of Internet traffic monitored by the ATLAS

September 17, 2019

NETSCOUT THREAT INTELLIGENCE REPORT: POWERED BY ATLAS

Cybercrime's Innovation Machine

Findings from 1H 2019

Key Findings

IoT Botnets Grow Smarter

Geopolitics goes cyber

5 Days

Rapid Weaponization

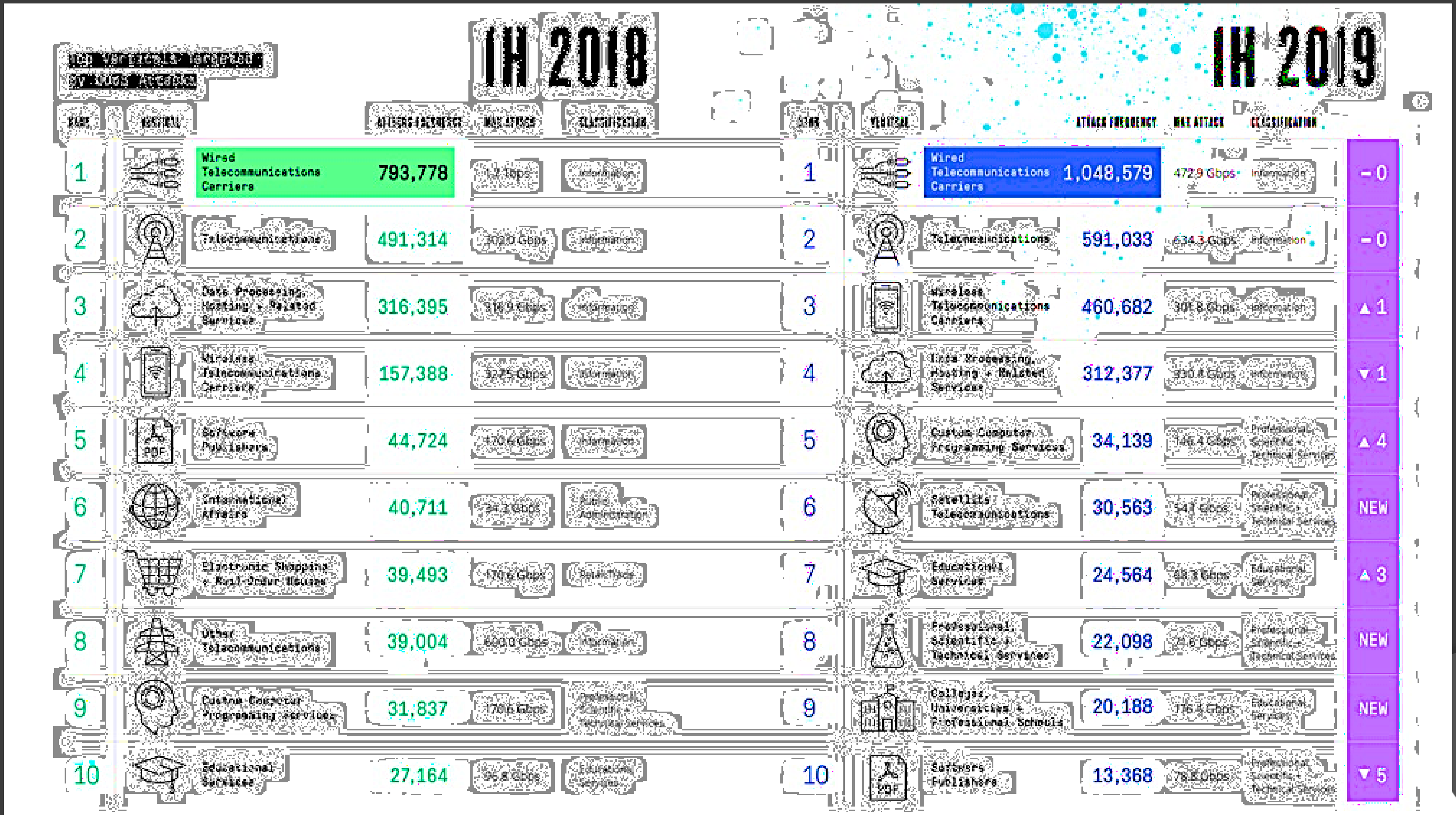
ATTACKS 100-400 GBPS	▲776%
Attacks in 1H 2018	458
Attacks in 1H 2019	4,014

DDoS' juicy middle

Cybercrime's Innovation Engine

ADAPTIT
EVOLUTION DRIVERS

Top Targeted Verticals



Top Verticals Targeted by DDoS Attacks

1H 2018

RANK	VERTICAL	ATTACK FREQUENCY	MAX ATTACK	CLASSIFICATION
1	Wired Telecommunications Carriers	793,778	1.2 Tbps	Information
2	Telecommunications	491,314	302.0 Gbps	Information
3	Data Processing, Hosting + Related Services	316,395	318.9 Gbps	Information
4	Wireless Telecommunications Carriers	157,388	322.5 Gbps	Information
5	Software Publishers	44,724	470.6 Gbps	Information
6	International Affairs	40,711	34.3 Gbps	Public Administration
7	Electronic Shopping + Mail-Order Houses	39,493	170.6 Gbps	Retail Trade
8	Other Telecommunications	39,004	600.0 Gbps	Information
9	Custom Computer Programming Services	31,837	170.6 Gbps	Professional, Scientific + Technical Services
10	Educational Services	27,164	96.8 Gbps	Educational Services

1H 2019

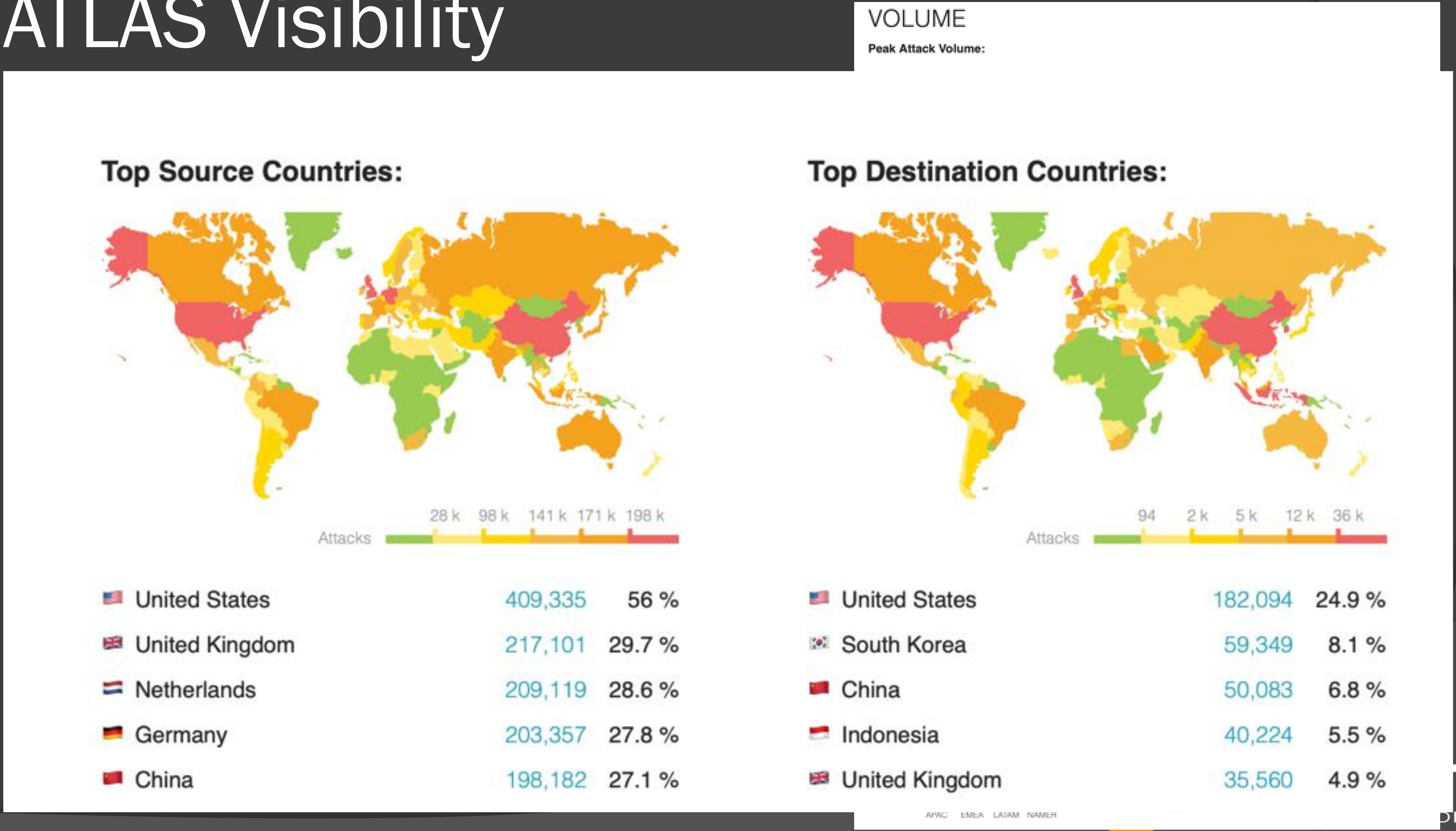
RANK	VERTICAL	ATTACK FREQUENCY	MAX ATTACK	CLASSIFICATION	
1	Wired Telecommunications Carriers	1,048,579	472.9 Gbps	Information	– 0
2	Telecommunications	591,033	634.3 Gbps	Information	– 0
3	Wireless Telecommunications Carriers	460,682	301.8 Gbps	Information	▲ 1
4	Data Processing, Hosting + Related Services	312,377	330.4 Gbps	Information	▼ 1
5	Custom Computer Programming Services	34,139	146.4 Gbps	Professional, Scientific + Technical Services	▲ 4
6	Satellite Telecommunications	30,563	54.7 Gbps	Professional, Scientific + Technical Services	NEW
7	Educational Services	24,564	48.3 Gbps	Educational Services	▲ 3
8	Professional, Scientific + Technical Services	22,098	71.6 Gbps	Professional, Scientific + Technical Services	NEW
9	Colleges, Universities + Professional Schools	20,188	176.4 Gbps	Educational Services	NEW
10	Software Publishers	13,368	78.5 Gbps	Professional, Scientific + Technical Services	▼ 5

New DDoS Vectors in 2H 2019

1. Apple Remote Management Services (ARMS)
2. Constrained Application Protocol (CoAP)
3. Ubiquity Discovery Protocol
4. Web Services Dynamic Discovery (WS-DD)
5. HTML5 Hyperlink Auditing Ping Redirection

ADAPTIT
EVOLUTION DRIVERS

ATLAS Visibility



VOLUME

Peak Attack Volume:

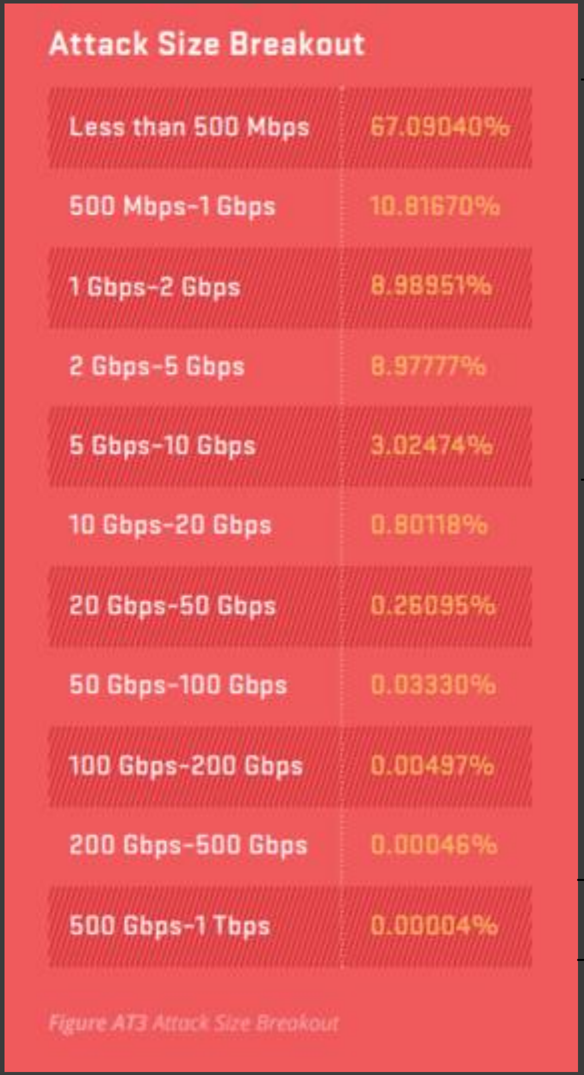
Top Source Countries:

United States	409,335	56 %
United Kingdom	217,101	29.7 %
Netherlands	209,119	28.6 %
Germany	203,357	27.8 %
China	198,182	27.1 %

Top Destination Countries:

United States	182,094	24.9 %
South Korea	59,349	8.1 %
China	50,083	6.8 %
Indonesia	40,224	5.5 %
United Kingdom	35,560	4.9 %

Most DDoS Attacks relatively short and “small”



Attack Size Breakout

Less than 500 Mbps	67.09040%
500 Mbps-1 Gbps	10.81670%
1 Gbps-2 Gbps	8.98951%
2 Gbps-5 Gbps	8.97777%
5 Gbps-10 Gbps	3.02474%
10 Gbps-20 Gbps	0.80118%
20 Gbps-50 Gbps	0.26095%
50 Gbps-100 Gbps	0.03330%
100 Gbps-200 Gbps	0.00497%
200 Gbps-500 Gbps	0.00046%
500 Gbps-1 Tbps	0.00004%

Figure AT3 Attack Size Breakout

99% of attacks
< 10G

0.00004%
News Headlines

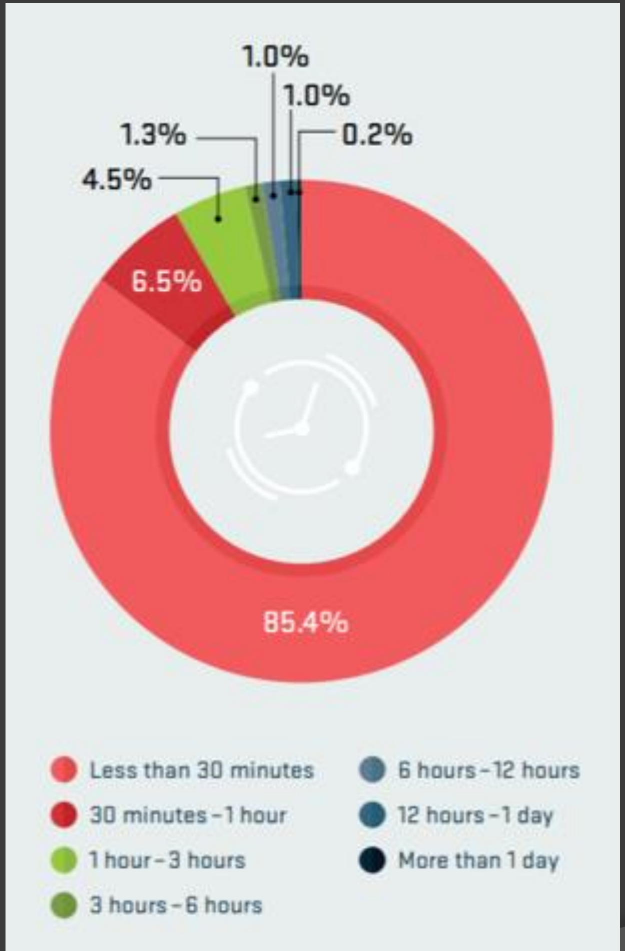


Figure AT10 Attack Duration

85.4% less than 30min
What is your Cloud SLA?

- *Distribution size of attacks,*
- *Worldwide infrastructure*
- *security report, 13th edition.*

ADAPTIT
EVOLUTION DRIVERS

Best Practices

1

- Factor network availability into the design of online services or applications; ***continuously stress-test.***

2

- Develop a DDoS Attack Mitigation Process
- ***Continuously stress-test & refine.***

3

- Utilize flow telemetry (e.g. NetFlow) collection & analysis for attack detection, classification & trace back.

4

Deploy multi-layered DDoS protection which includes:

- On-premises Intelligent DDoS Mitigation Systems (e.g. Arbor APS / TMS products)
- Overlay cloud-based DDoS protection services (i.e. Arbor Cloud or ISP/MSSP)
- Network infrastructure-based techniques such as S/RTBH & Flowspec at all network edges

5

- Scan for misconfigured, abusable services running on servers, routers, switches, home CPE devices, etc. (i.e. TCP 23/2323). Alert users running abusable services – possibly blocking until they are remediated.

ADAPTIT
EVOLUTION DRIVERS

Best Practices

6 NTP Services

- Check *Open NTP Project* for abusable NTP services on your networks.
- Disallow Level 6/7 NTP queries from the Internet.

7 DNS Recursors

- Check *Open Resolve Project* for abusable open DNS recursors on your networks. Ensure only authorized users can query recursive DNS servers.

8

- Ensure SNMP is blocked on public-facing infrastructure/ servers.

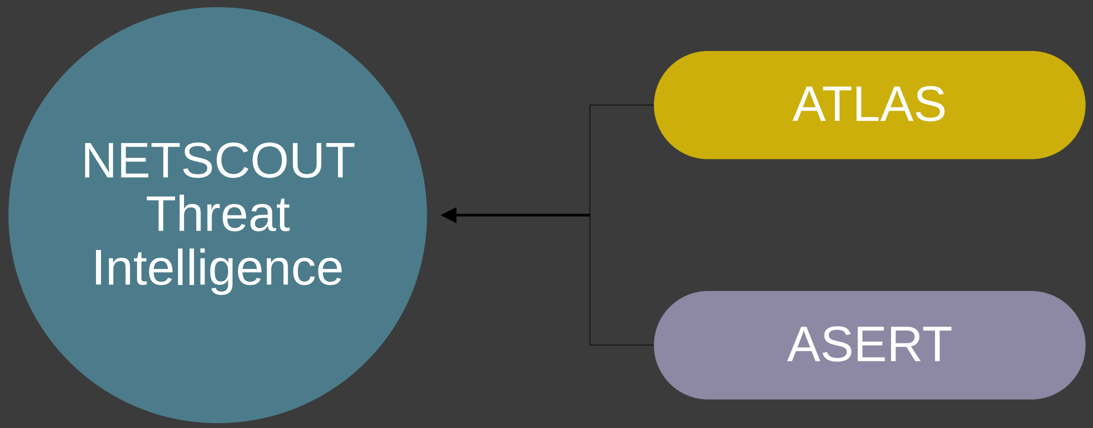
9

- Employ Anti-spoofing mechanisms such as Unicast Reverse-Path Forwarding, ACLs, DHCP Snooping & IP Source Guard, Cable IP Source Verify, etc. on all edges of ISP and enterprise networks.

10

- Participate in the global operational security community and share threat intelligence and defense best practices.

NETSCOUT Threat Intelligence



NETSCOUT Threat Intelligence

ATLAS

ASERT

Advanced Threat Level Analysis System

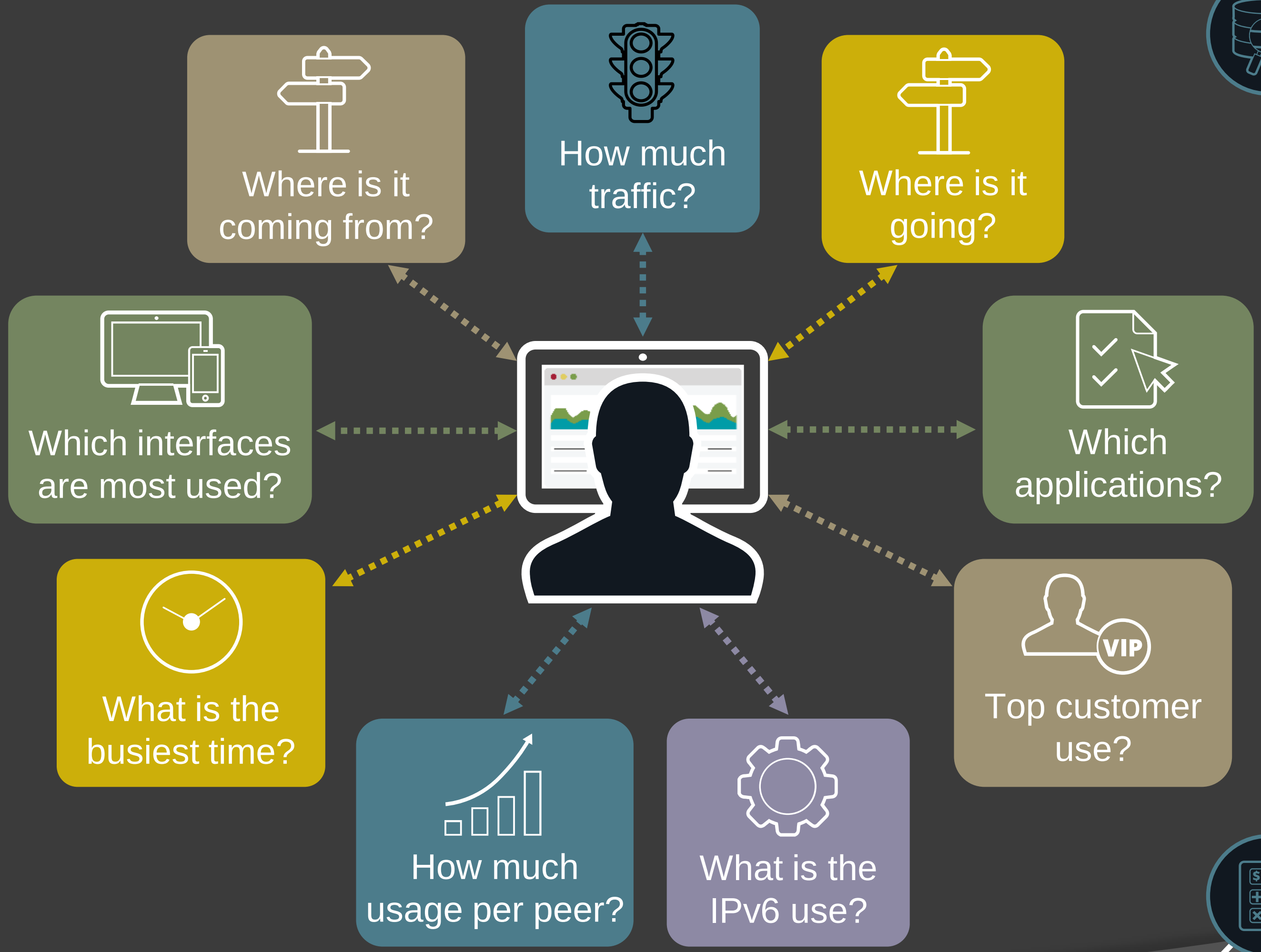
Arbor’s collective threat and traffic data depository that includes traffic stats from over one third of the Internet. Arbor’s unique correlation and analytics make it smart data

ATLAS Security Engineering & Response Team

NETSCOUT’s elite threat research organization that analyzes and curates ATLAS data to provide human and machine readable actionable intelligence to Arbor customers

Arbor Visibility

Actionable Network Visibility and Detection



Where is it coming from?

How much traffic?

Where is it going?

Which interfaces are most used?

Which applications?

What is the busiest time?

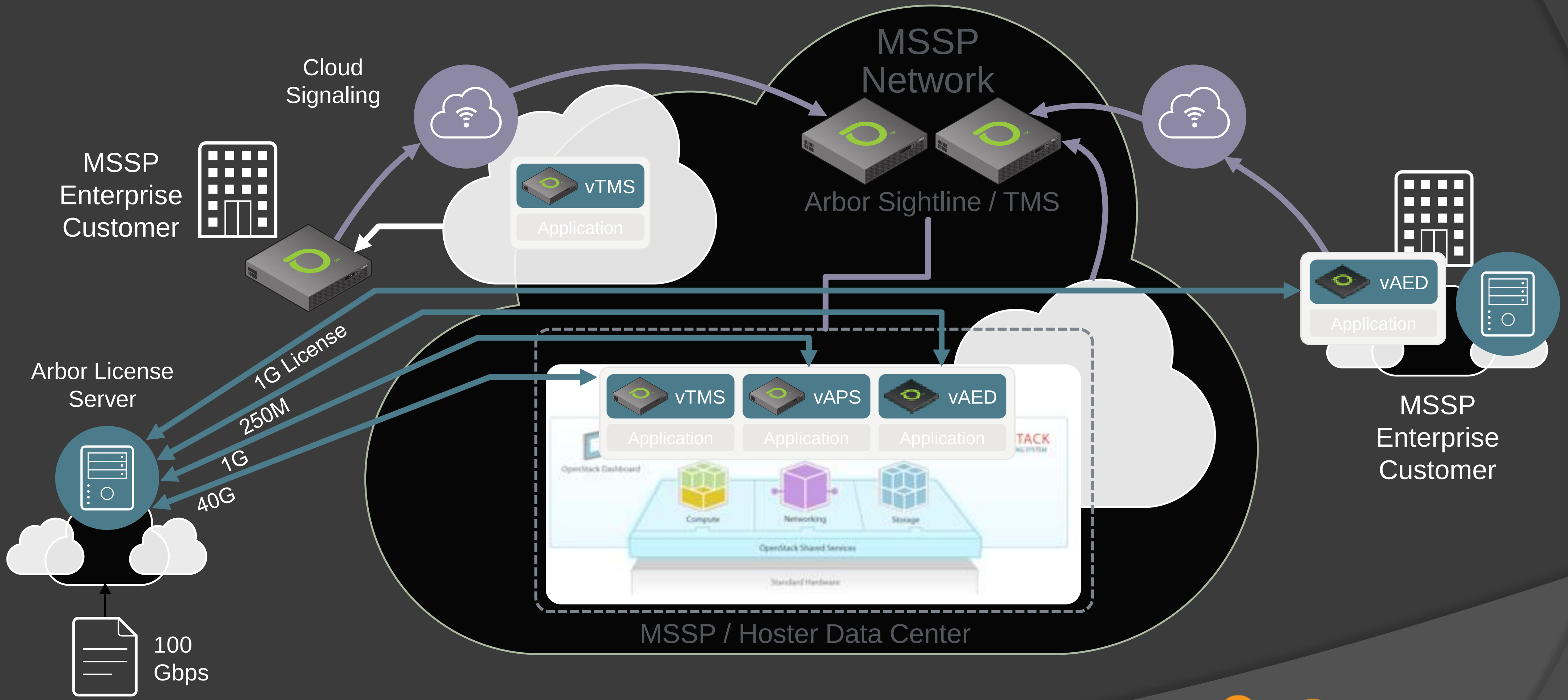
Top customer use?

How much usage per peer?

What is the IPv6 use?

- What is the makeup of the data?
- How is this changing over time?
- Problem Areas → Find and predict
- Congestion → Take corrective action
- Monitor utilization of critical network resources
- Perform effective traffic engineering
- Lower transit expenses

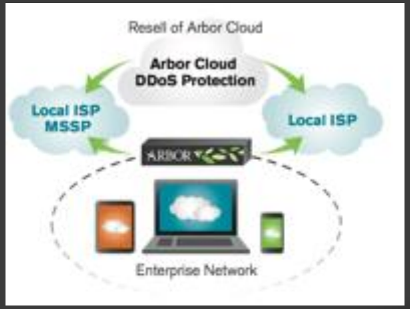
DDoS Protection EVERYWHERE

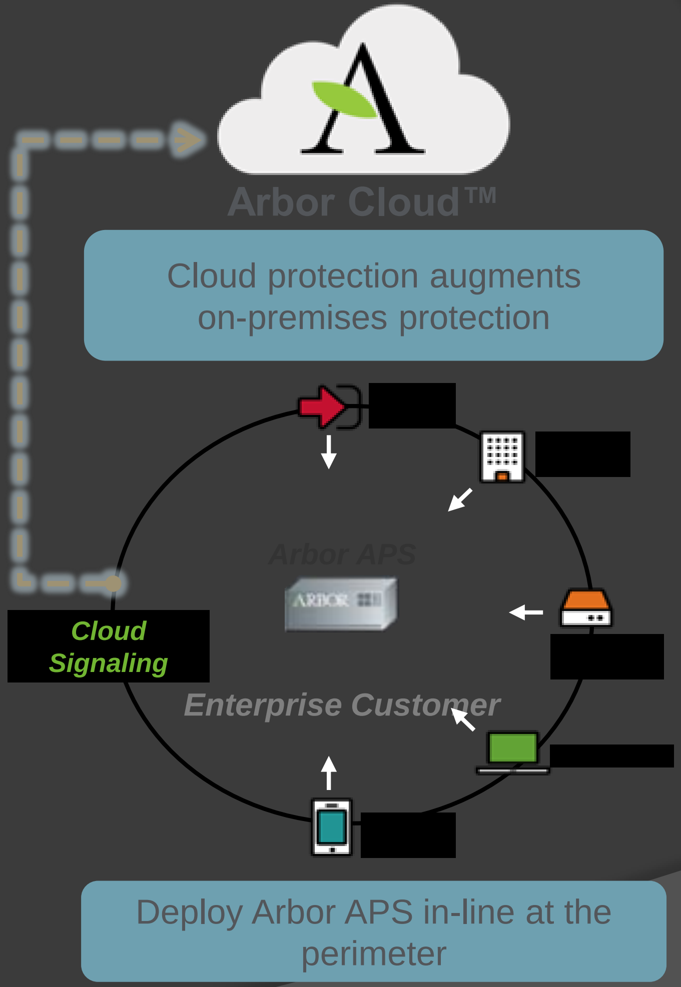


ADAPTIT
EVOLUTION DRIVERS

Arbor Cloud DDoS Mitigation Service

- Global deployment with 11.2 Tbps of mitigation capacity in 14 sites, as of today
- 24x7x365 Arbor Managed SOC
- Transparent operation with clear reporting
- Subscription to service based on volume of clean traffic
- No limit to attack sizes
- Managed APS service
- Industry-leading SLA's
- Uplink Provider Independent





Cloud protection augments on-premises protection

Deploy Arbor APS in-line at the perimeter

ADAPTIT

EVOLUTION DRIVERS

Corporate Customers in Greece

- Fixed line Telecom Operators
  - OTE/Wind/Vodafone/Forthnet
- Mobile Telecom Operators
  - Cosmote/Wind/Vodafone
- Colocation Datacenters
  - MED Nautilus

ADAPTIT
EVOLUTION DRIVERS

Thank you!