Enabling Secured Application Delivery

Hue Fatt Seng

Solution Consultant

IT Challenges in Education Sector

Education sector is <u>NO</u> difference to any Global Companies
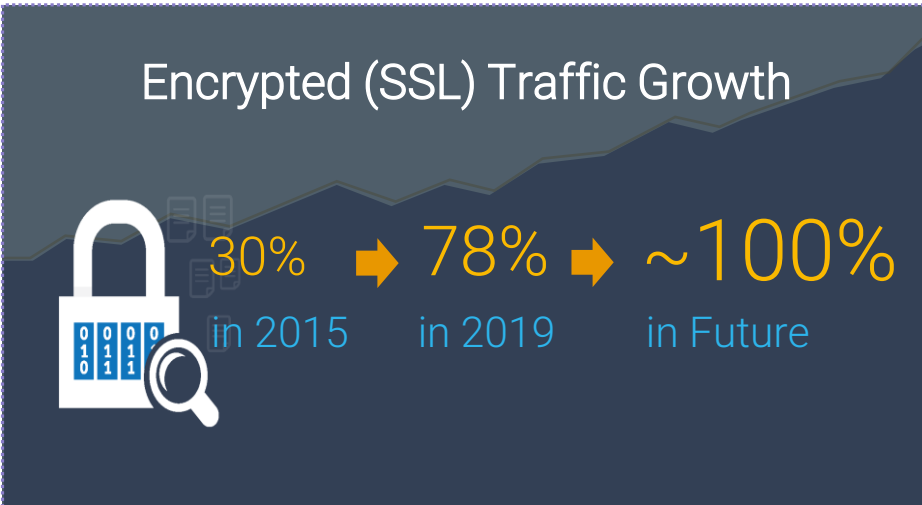
Adoption of Cloud

SaaS

- Requires flexible deployment
- Increases need for VPN
- Burdens perimeter security

Evolving Data Center traffic

East

West

- Cloud computing
- Big data
- Virtualization/HCI
- Mobility

Encrypted (SSL) Traffic Growth

30% ➡ 78% ➡ ~100%

in 2015   in 2019   in Future

Threat Weapons for Hire

US$ 150

Buys **1 week** DDoS attack on the black market
(TrendMicro Research)

~58% of attacked traffic peaked >1Gbps
~52% of attack are Multi-Vector
(Verisign, 2018Q2)

Advantage with A10 Networks Application Delivery

AVAILABILITY
- Safeguard server & datacenter uptime
- Scale web and key infrastructure
- Ensure business continuity
- Minimize server sprawl

ACCELERATION
- Proactive management & monitoring
- Automation of services
- Provide fast and responsive app services
  - Offload overtaxed servers from SSL
  - Technology/Protocol Harmonization

SECURITY
- Decrypt SSL traffic with latest ciphers and upgradability
- Defend multi-vector DDoS attacks, hence ensuring Availability
- Shield against 'zero day' attacks

Visibility
- Centralized control with auto scalability
- App profile visibility with analytics and reporting
- Fully programmable with third-party tool integration
- 100% Security Visibility with SSL Inspection
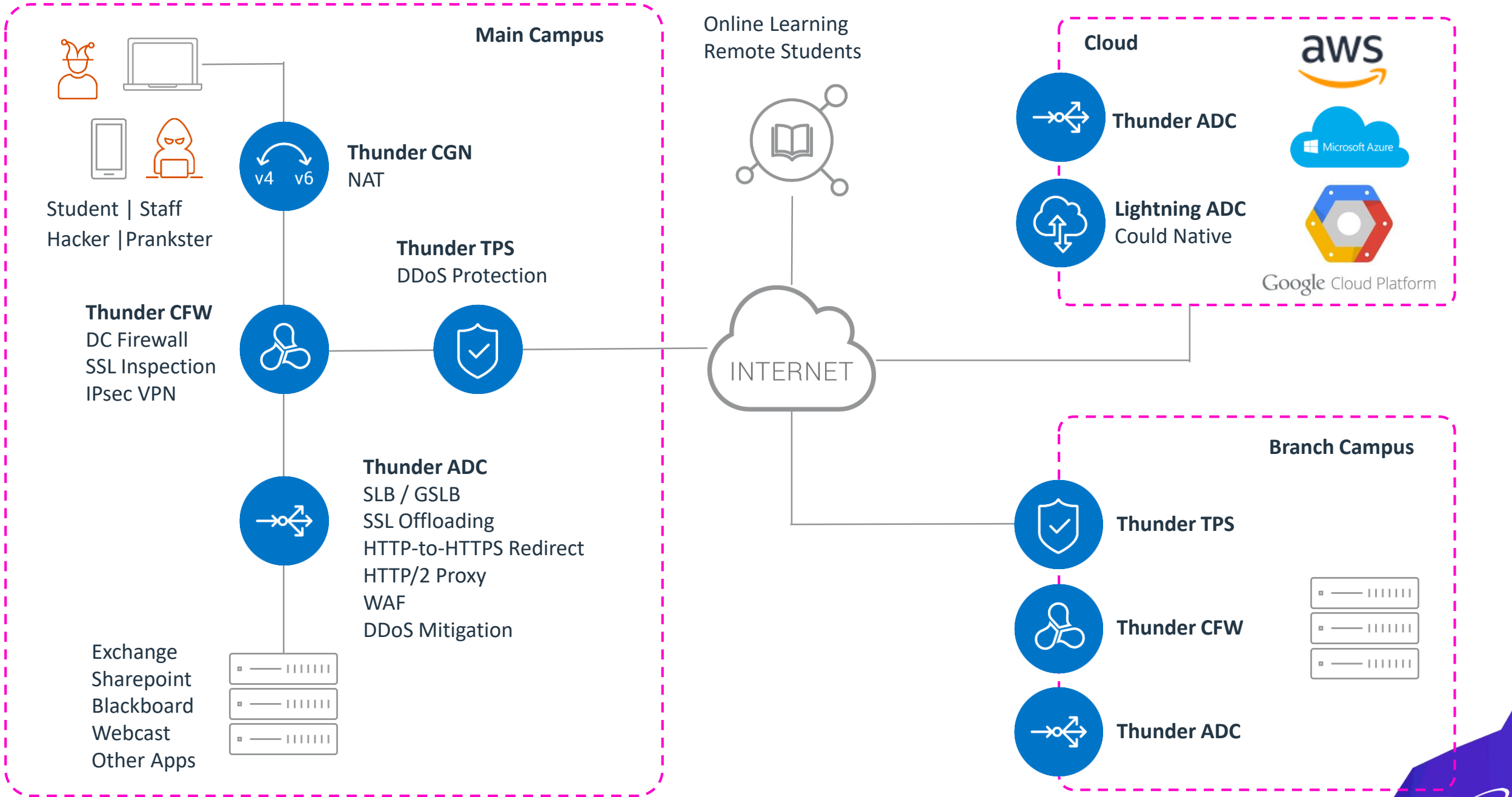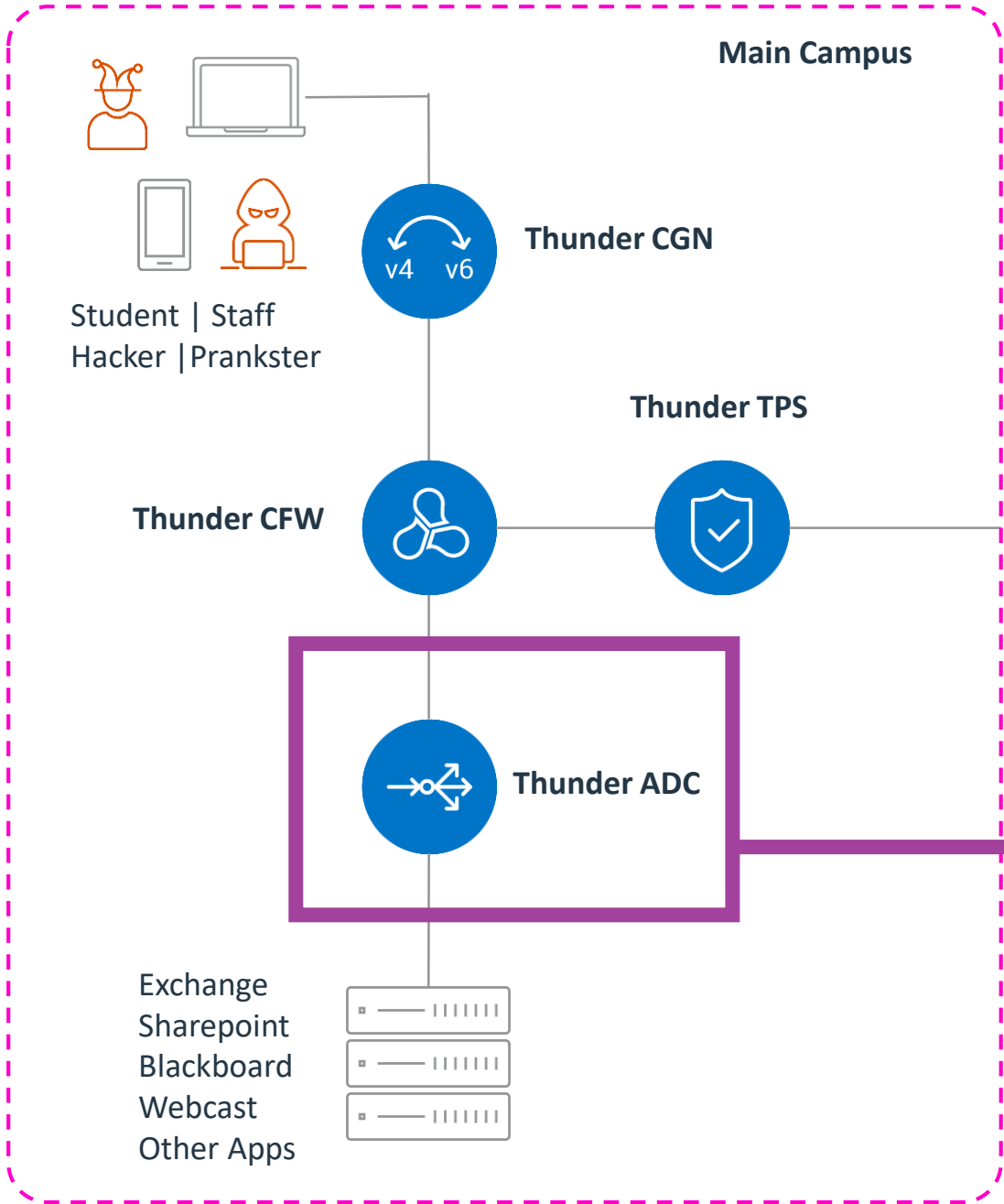
Thunder ADC – App Delivery Controller

- ❑ Application and Server Availability

- ❑ Active-active Multi-Cloud
  - Sub-second seamless Geo-redundancy

- ❑ SSL Offload with A+ Rating by Qualys SSL Lab.
  - Optimize Infrastructure Performance by ~20%
  - Accelerate SSL performance, Improving User Experience

- ❑ Mitigate non-encrypted app access

- ❑ Harmonization: HTTP/2 to HTTP/1.1, and v.v.

- ❑ Protects against OWASP Top 10
  - PCI DSS Compliance and Certified by ICSA Lab
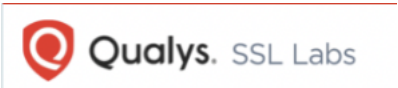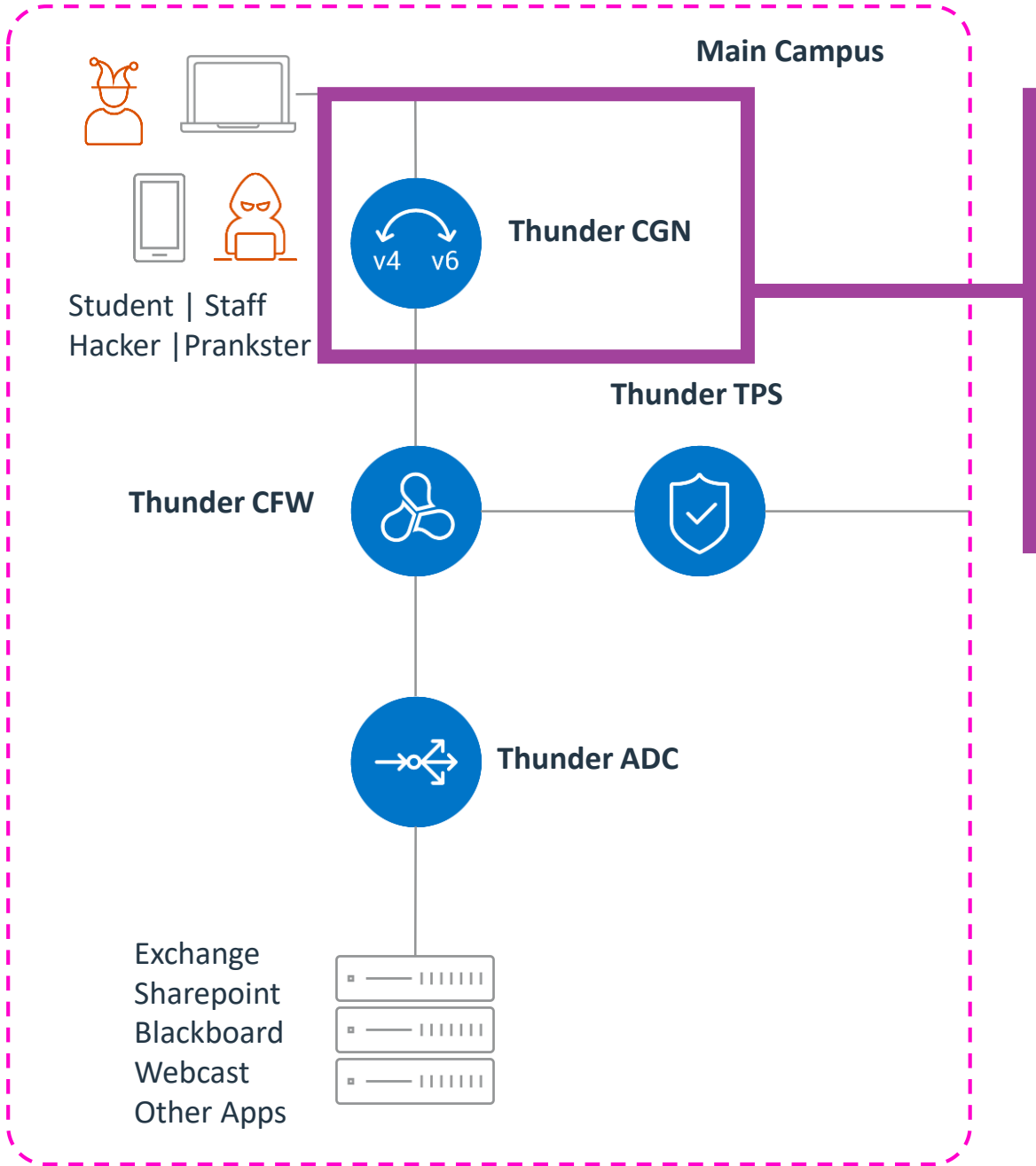
Thunder CGN – Carrier Grade NAT

❑ Providing reliable internet services and connectivity for for everyone in entire campus

❑ IPv4 Preservation

❑ High performance Network Address Translation capability
  • Carrier Grade performance
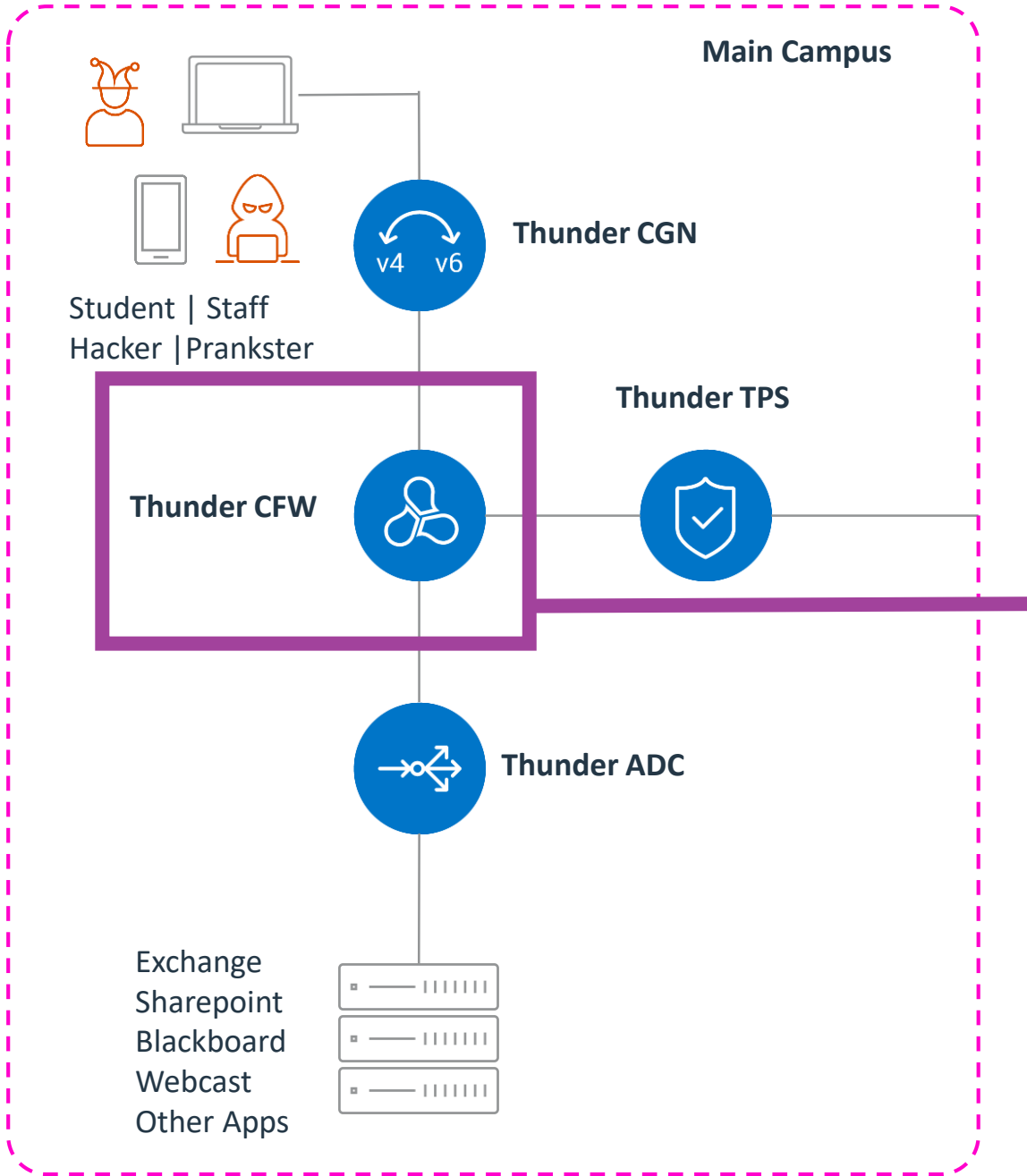
Thunder CFW – Convergent Firewall

- ❑ Tier-1 Firewall with Layer 3

- ❑ Secure Multi-Cloud with IPsec

- ❑ SSL Inspection (and, Service Chain)

  - Enabling best of breed security services

  - Point security is ***COSTLY*** and ***induces LATENCY***
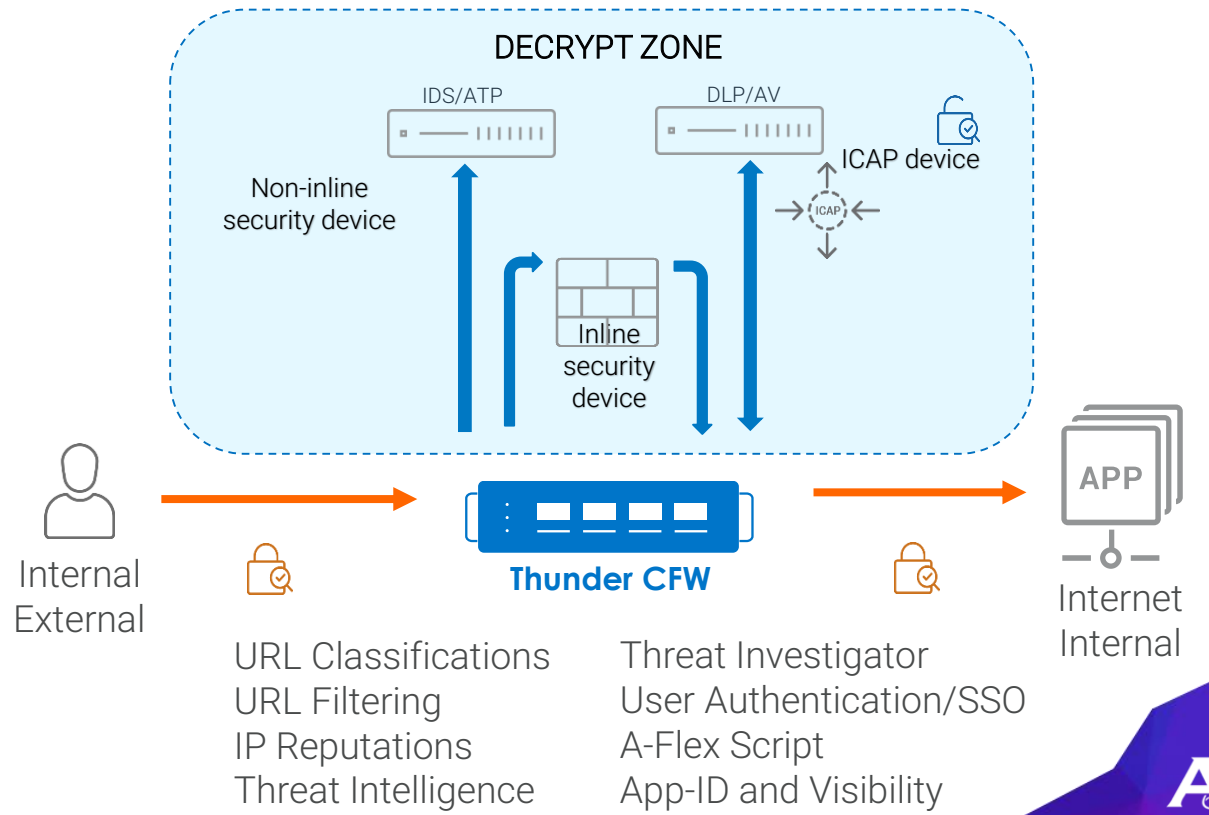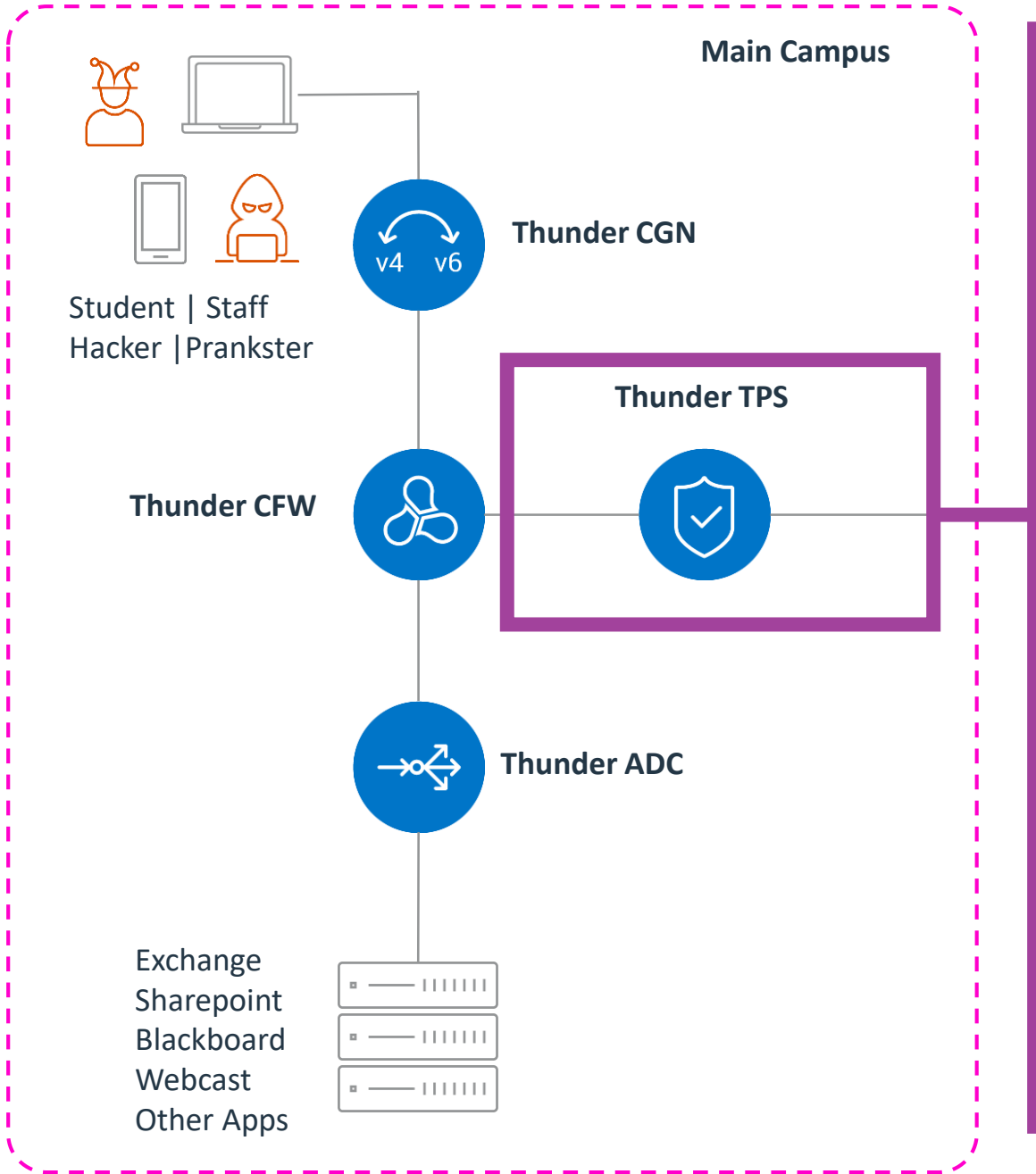
Thunder TPS – Threat Protection System

❑ Defense against Volumetric alone is insufficient

❑ **Multi-Vector DDoS protection** is necessary at ALL Levels - Volumetric, Network and Application

❑ **4 Levels** of Automated Escalation of DDoS Detection and Mitigation

DDoS monitoring & reporting Automation

aGalaxy

Detection

Adaptive Profiling
Performance & Precision
28 DDoS Indicators

Mitigation

Auto and Manual Mitigation
Sub-100ms Mitigation

Main Campus

Student | Staff
Hacker |Prankster

Thunder CGN
v4 v6

Thunder CFW

Thunder TPS

Thunder ADC

Exchange
Sharepoint
Blackboard
Webcast
Other Apps

8
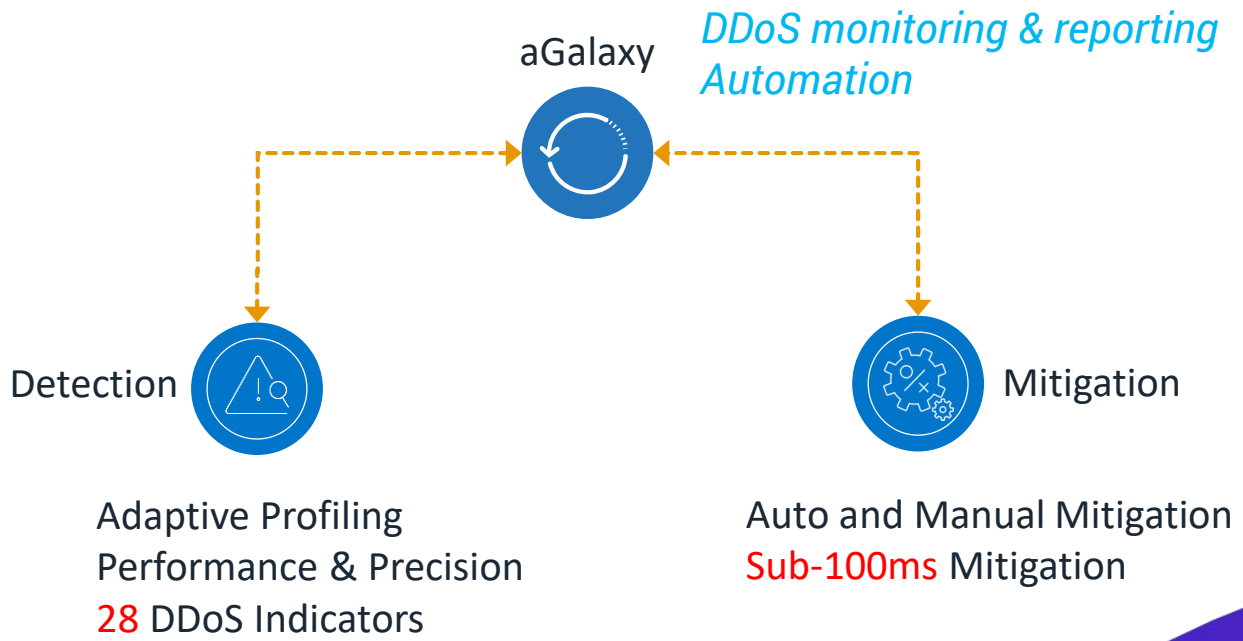
Management Centered on Analytics and Automation

aGalaxy TPS
TPS Management

Harmony Controller
Multi Cloud & Multi Service Management

SECURITY

APPLICATION DELIVERY

TPS

SSLi

CFW

ADC

v4   v6

CGN

Automation

Policy

Detection

Centralized
Management

Self Service &
Automation

Analytics

Harmony Controller Analytics

❑ Access and Transactional Logs

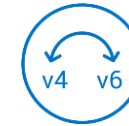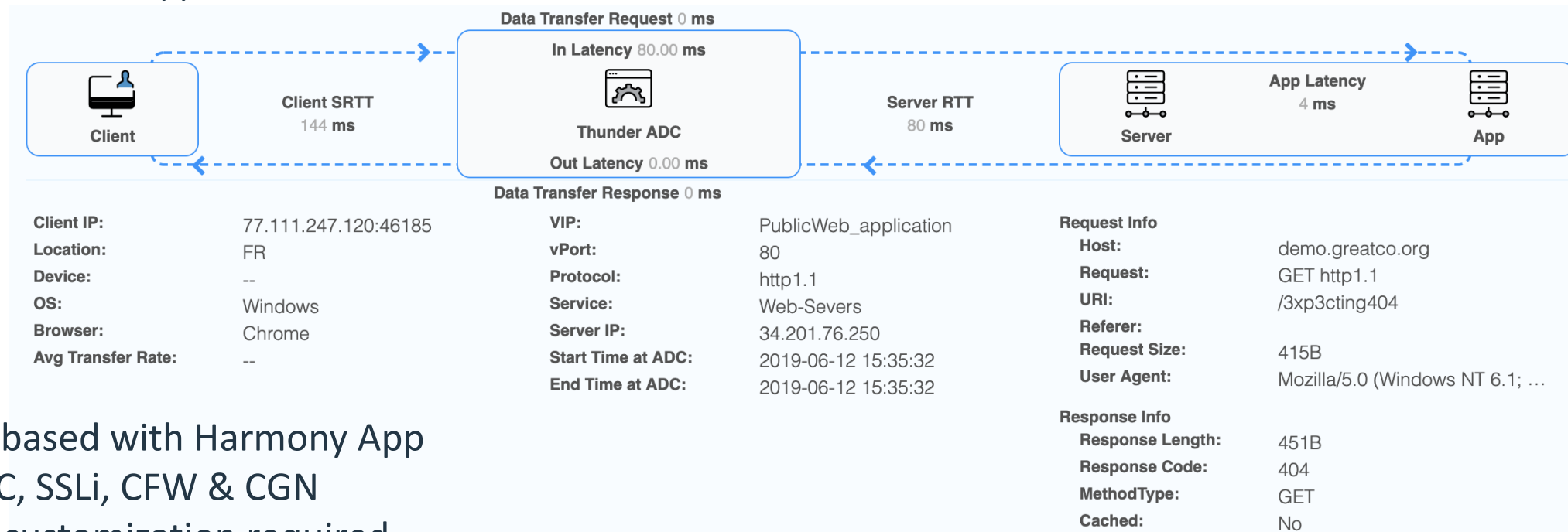|								
▶ 🟢	12/06 15:36:58	45.76.123.211	/index.html	GET	200	10KB	208 ms	Yes
▶ 🟢	12/06 15:36:32	77.111.247.120	/index.html	GET	304	66B	144 ms	Yes
▶ 🟢	12/06 15:35:35	139.59.152.248	/	GET	200	10KB	156 ms	Yes
▶ 🔴	12/06 15:35:33	45.76.123.211	/a39fkapod_aodopjslijas_	GET	404	518B	216 ms	No
▶ 🟢	12/06 15:35:32	77.111.247.120	/index.html	GET	304	66B	144 ms	Yes
▼ 🔴	12/06 15:35:32	77.111.247.120	/3xp3cting404	GET	404	451B	308 ms	No

❑ Per App, Per User, Per URI

Data Transfer Request 0 ms
In Latency 80.00 ms

Client   **Client SRTT** 144 **ms**   **Thunder ADC**   **Server RTT** 80 **ms**   **Server**   **App Latency** 4 **ms**   **App**

Out Latency 0.00 **ms**
Data Transfer Response 0 ms

Client IP:	77.111.247.120:46185	VIP:	PublicWeb_application	Request Info	
Location:	FR	vPort:	80	Host:	demo.greatco.org
Device:	--	Protocol:	http1.1	Request:	GET http1.1
OS:	Windows	Service:	Web-Severs	URI:	/3xp3cting404
Browser:	Chrome	Server IP:	34.201.76.250	Referer:	
Avg Transfer Rate:	--	Start Time at ADC:	2019-06-12 15:35:32	Request Size:	415B
		End Time at ADC:	2019-06-12 15:35:32	User Agent:	Mozilla/5.0 (Windows NT 6.1; …

Response Info
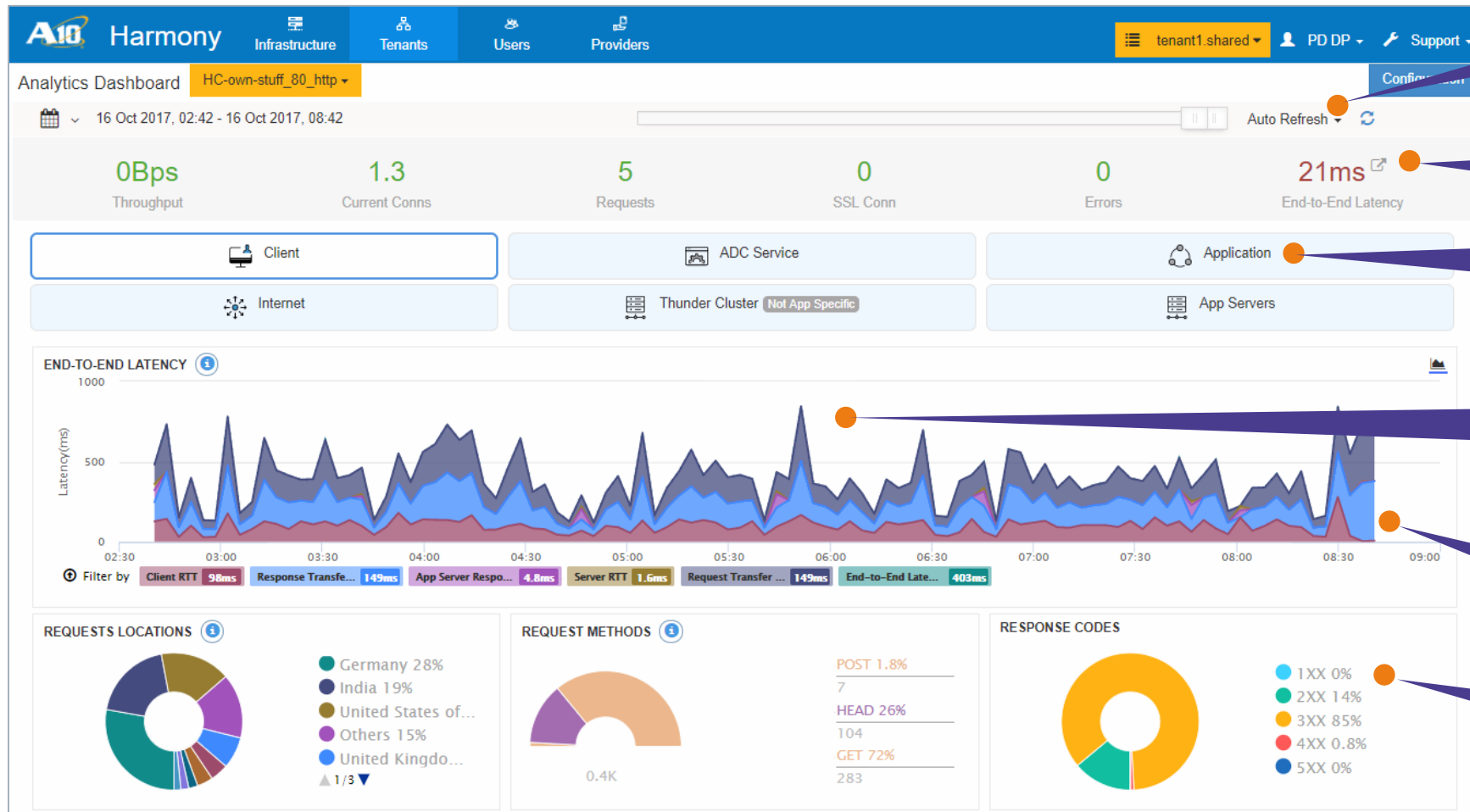Response Length: 451B
Response Code: 404
MethodType: GET
Cached: No

❑ Wizard-based with Harmony App
- ADC, SSLi, CFW & CGN
- No customization required

A10

Harmony Controller

Time selection bar

Real-time ticker for most important parameters

Selection panel for client, ADC, app and their infrastructure

Zoom-in to time by making a rectangle

Detailed section-wise charts and tables

Summary charts of the selected panel

IHL (Thailand) – DDoS Attack

Protected Zone Incident Detail Report

Report Generation Time: 2018-09-21 02:12:33 +07

Summary

Incident Name:	Public_202-28-76-0_24-80-http-180918-111800
Protected Zone:	Public_202-28-76-0_24
Service:	HTTP 80
Status:	stopped
Total Packets (Passed / Dropped):	351.44 M / 59.68 M
Total Bytes (Passed / Dropped):	121.37 B / 87.23 B
Peak Received Rate (pps/ bps):	210.69 K / 853.14 M
Create Time:	2018-09-18T11:18:00 +07
Start Time:	2018-09-18T11:18:00 +07
Stop Time:	2018-09-19T06:05:28 +07
Duration:	18 hrs 47 mins 28 secs
Attack Type:	Malformed Protocol Attack, SlowLoris, SlowPost, POST Flood, Request Flood, SlowRead

200,000+ packets per second
with 850+ Mbps
= 85% of link bandwidth!

Top Sources

Packet Rate   Packet Drop Rate

Nigeria: 1
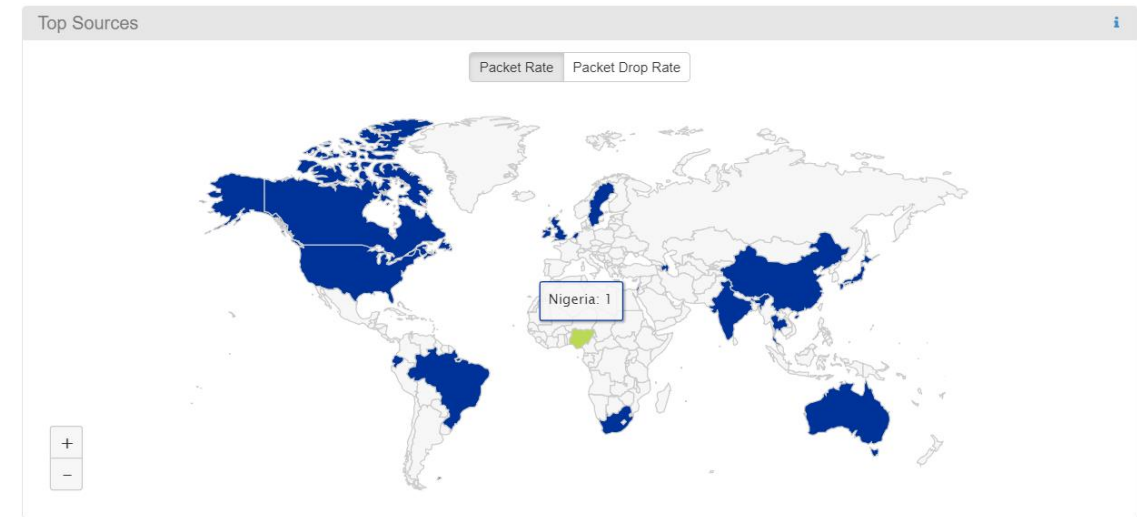
Incoming Request from
Multiple Foreign Countries

12

A10

IHL (Institutions of Higher Learning) : DDoS Attack

Source: The China Post news TW, Sep. 2016

Hackers hit Fu Jen Website to Demand Apology

- Anonymous HK launched DDoS attacks to disable Fu Jen Catholic University's website

- Targeted the university for failing to publicly apologize to a sexual assault survivor and former student.

- The major component of the attack was HTTP Get flood attack.

4500+ Customers Strong

Service Providers

3 of Top 4
U.S. WIRELESS CARRIERS

7 of Top 10
U.S. CABLE PROVIDERS

Top 3
WIRELESS CARRIERS IN JAPAN

comcast
3
中国移动 China Mobile

Enterprises

Microsoft
SEGA
BENTLEY UNIVERSITY
GE Healthcare
SUBARU
SONY PICTURES
GE
VW
Silicon Valley Bank
EMC²
U.S. DEPARTMENT OF ENERGY
CRÉDIT AGRICOLE
WSGR
McAfee
SAMSUNG
TED BAKER LONDON
Sharecompany
HAWKINS
WWE
mevio
ONE CLUB FITNESS
PRINCETON UNIVERSITY
gamania
TEXAS STATE
sesameworkshop
THE HUFFINGTON POST

Web Giants

LinkedIn
Aol.
box
Go Daddy.com
Twitter
YAHOO!
rocketfuel
craigslist
YAHOO! JAPAN
阿里巴巴 alibaba.com
terra
淘宝网 Taobao.com
meebo
shopzilla
BizRate

Enabling Modern and Progressive IT Operations
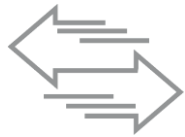
AVAILABILITY	ACCELERATION	SECURITY	Visibility

Drive Agility
Automation Self-service

Support Multiple Environments
Data Centers | Private Clouds | Public Clouds

Achieve Efficiency
Visibility and Analytics, Per App and Per User

Thank You

A10

Reliable Security Always™