A10

Always Secure. Always Available.

Advanced DDoS Defenses for Data Center Providers

Taka Mitsuhata

Director, Technical Marketing

Terry Young

Director, Service Provider Product Marketing

Speakers

Taka Mitsuhata

Director, Technical Marketing

A10 Networks

Terry Young

Director, Service Provider Product Marketing

A10 Networks

Agenda

- Introduction
- DDoS Trends
- What is DDoS?
- Data Center Providers Challenges and Strategies
- A10 DDoS Defense Overview
- Data Center Provider Case Study
  - Monetizing Security Investment
- Summary
  - 3 Steps to Stronger Security
  - Choosing the best DDoS protection

A10 Networks and Intel

Huge DDoS Attacks Continue To Make Headlines

CPO MAGAZINE HOME NEWS INSIGHTS RESOURCES

CYBER SECURITY NEWS · 3 MIN READ

New Zealand Stock Exchange Shut Down by DDoS Cyber Attack

ALICIA HOPE · SEPTEMBER 3, 2020

LATEST

Hardware Security Risks: Plans for Reentering the Workplace With Compromised Devices

Internet Society's "Intern… Impact Assessment Toolkit" Aims to Protect t… Future of the Internet

CBR Computer Business Review

Favourites

Favorite list is empty.

Latest News on CBR

Enginuity CIO David Ivell

EMERGING TECHNOLOGY CLOUD IOT CYBER SECURITY BIG DATA ENTERPRISE IT INDUSTRY BOARDROOM VIDEO WHITE PAPERS SEARCH

Follow Us

THREATS Back to Home

AWS Hit With a Record 2.3 Tbps DDoS Attack

ED TARGETT EDITOR 13TH JUNE 2020

INCREASE / DECREASE TEXT SIZE

MOST READ

Adobe Flash is Abou… Is Your Business Rec…

ED TARGETT 23RD JUNE

Apple Confirms its B… Much-Hyped Pivot t…

ED TARGETT 23RD JUNE

Microsoft: Here's how we stopped the biggest ever DDoS attack

Microsoft details how Azure helped mitigate a 3.47 terabytes per second distributed denial of service (DDoS) attack.

RELATED

ITPro. Business Cloud Hardware Infrastructure Security Software Technology Resources .co.uk

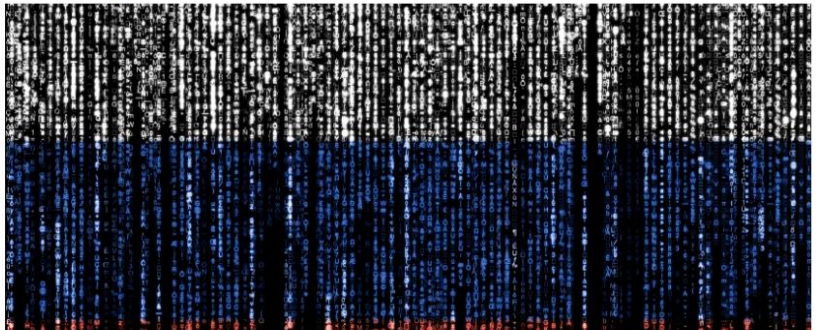
IT Pro is supported by its audience. When you purchase through links on our site, we may earn an affiliate commission. Learn more

NEWS Home > Security > Hacking

Russian hackers declare war on 10 countries after failed Eurovision DDoS attack

Italian police thwart cyber attacks on Eurovision's voting systems from the Russian-linked hacker group Killnet after the same group targeted public sector institutions days earlier

by: Connor Jones 16 May 2022



Business Continuity Management / Disaster Recovery , Cybercrime , DDoS Protection

CISA Warns of Increased DDoS Attacks

Security Experts Say Remote Workforce, Online Learning Create Opportunities

Doug Olenick (DougOlenick) · September 10, 2020

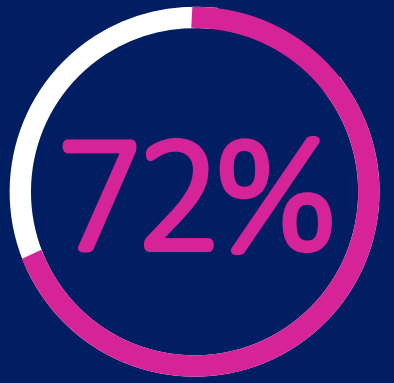
Twitter Facebook LinkedIn Credit Eligible Get Permission

Most Attacks are Small, Frequent, and Target Downstream Subscribers

341% Increase in DDoS Attacks

1,400 Attacks per Day against a large Cloud Provider

Reported DDoS attacks that were under 10 Gbps



Can only blackhole suspicious IP traffic

Sources:
IDC
Pulse Survey "Core Network Investments for Rural Broadband"
"Annual Threat Report 2020", NexusGuard, June 2021

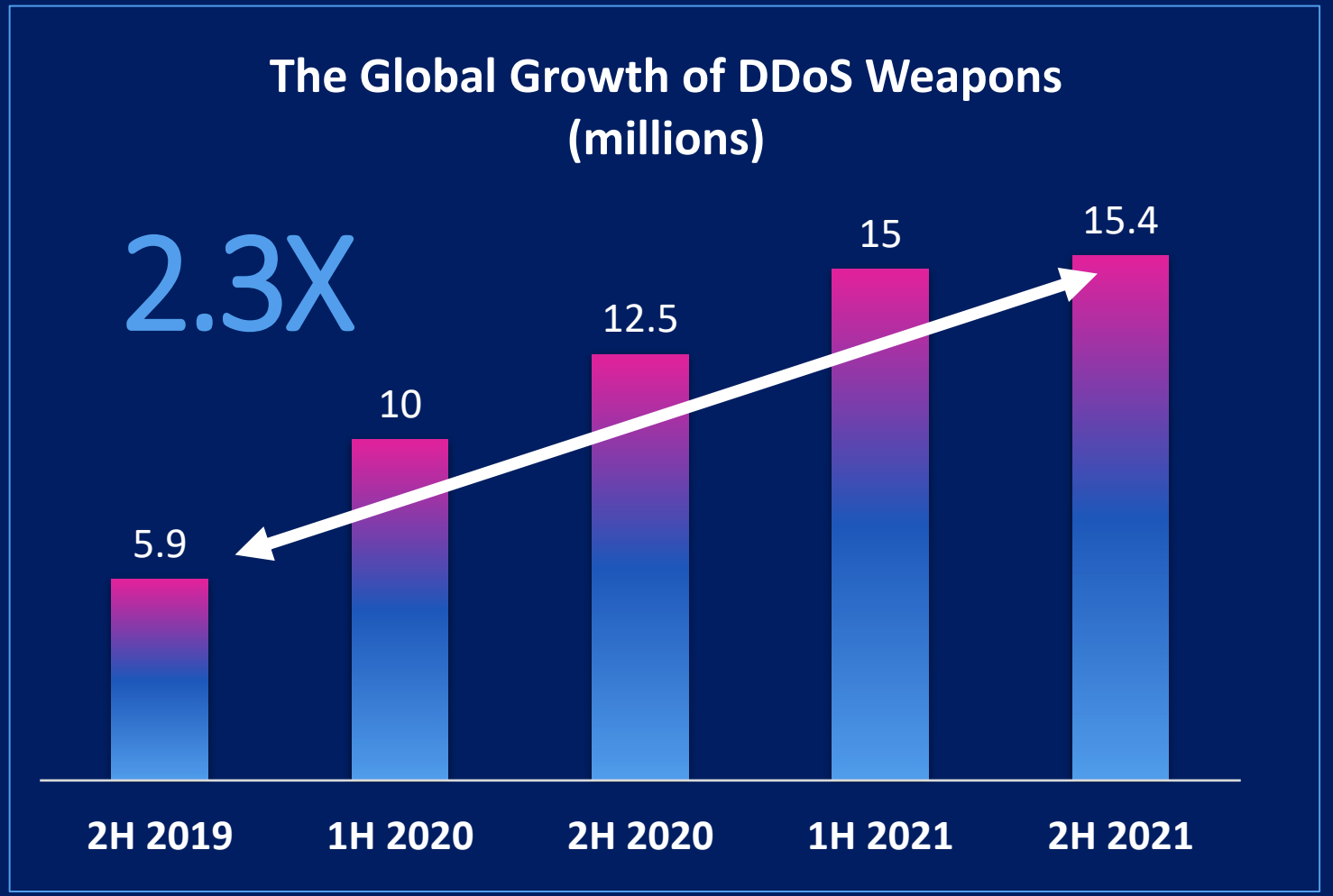
…Using Millions of Available Weapons Globally

Unique DDoS Weapons Tracked by A10 Networks

Approximately

15.4 Million

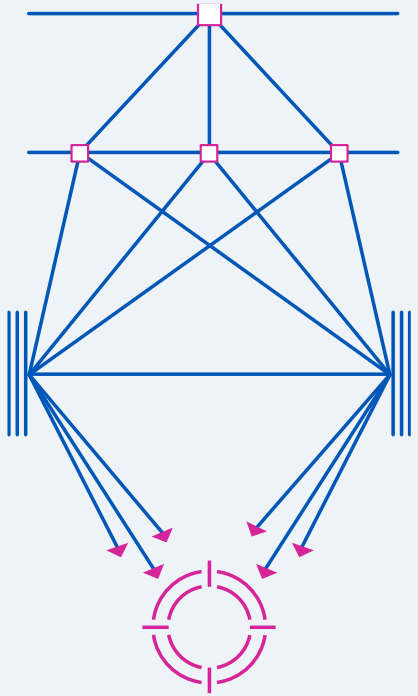
2H 2021



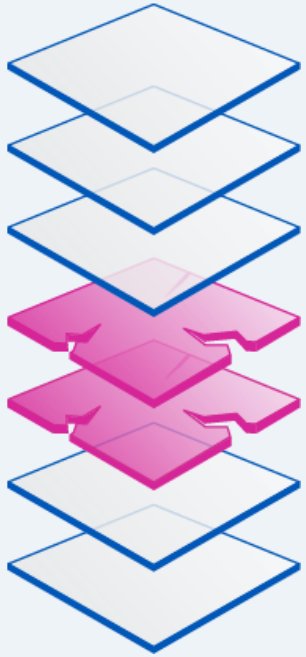
Source: *2022 A10 Networks DDoS Threat Report*

Three Main Types of DDoS Attacks

Volumetric Attacks



Network Protocol



Application Attacks

DDoS Attacks Can Be Launched Anytime, Anywhere, by Anyone

Reflected Amplification Attack

The ongoing conflict in Ukraine - an example of state-sponsored cyber warfare using DDoS

2M
Requests

2M Apple Remote Desktop (ARD) requests

34x
Amplification

30,622 ARD weapons
10% could generate 3.2TB
50% could generate 16TB

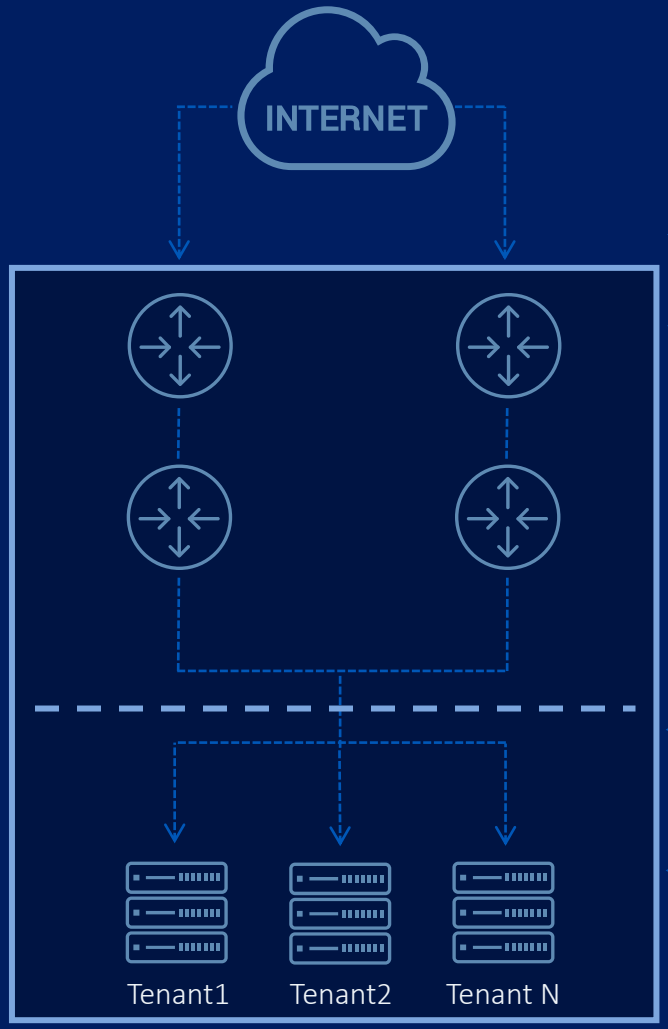
In Ukraine, DDoS attacks were used by Russia to complement the physical confrontation on the ground

Data Center Provider DDoS Challenges

- Business Challenges
  - Today's threats require constant vigilance
  - Must combat sophisticated volumetric attacks *AND* meet tenants' protection demands
  - Limited resources to manage increased traffic and threats
  - DDoS attacks threaten business success
- Operational Challenges
  - Complicated, manual operations
  - Slow response to attacks
  - Mitigation scalability
  - Shortage of trained DDoS security staff

DDoS Protection Strategies

Multi-vector DDoS Attack Sketch



Data Center Backbone

Tenants Site

Volumetric

- DNS amplification
- NTP amplification
- UDP Flood

Network Layer

- Fragmentation
- SYN floods
- SSL renegotiation

Application Layer

- Slowloris
- HTTP floods
- DNS NXDOMAIN attack

Defense Techniques

Network Edge/Backbone

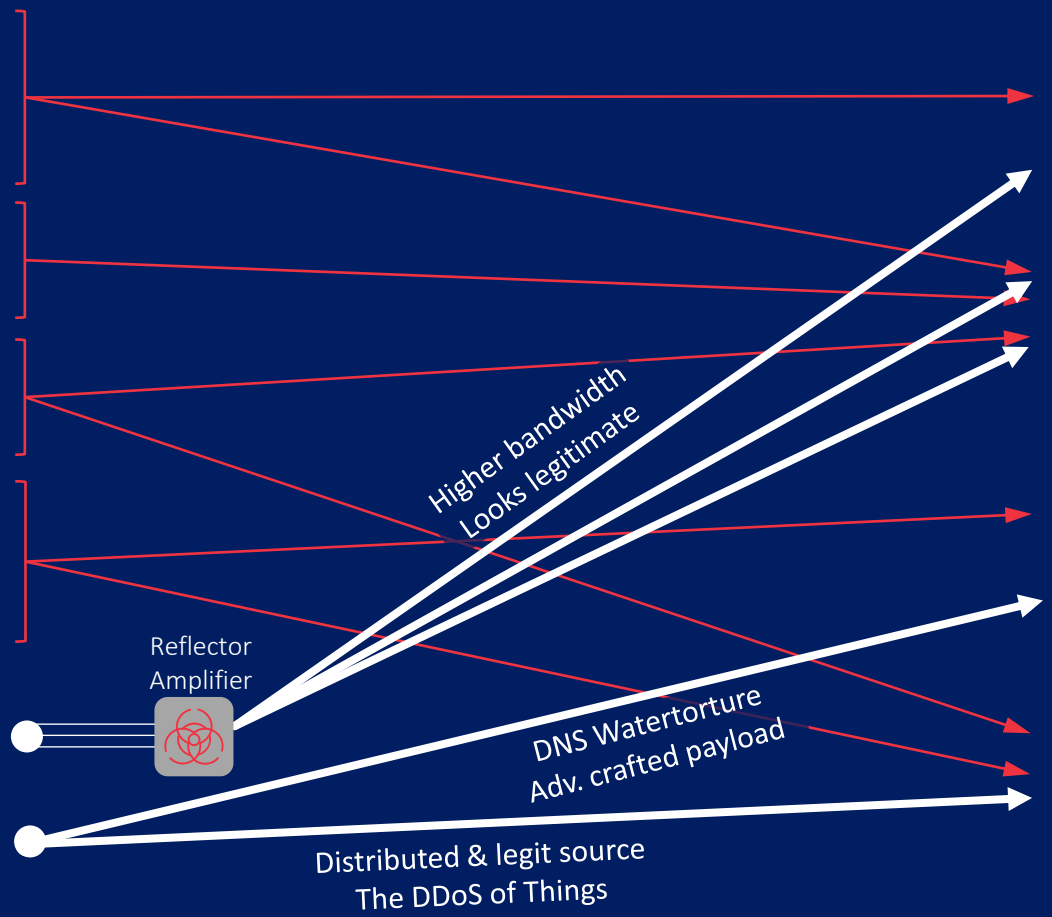
- xFlow sampling-based detection
- Protection for high number of volumetric attacks and high PPS

Tenant Site

- Inline deployment inspecting all packets (always-on)
- Protection for volumetric, network & application attacks

DDoS Attack Types and Vectors

Attacks Types
IP Anomaly
Protocol Anomaly
L3/L4 Volumetric
L4 Protocol
L4 Resource
SSL Protocol
SSL Resource
L7 Protocol
L7 Resource
L7 Flood
Reflected Attack
Botnets-based Attack



Victim Areas

Network/System Infrastructure

- Bandwidth
- CPU
- Memory
- Connections/ sockets

Network Layer - UDP

Network Layer - TCP

Application Layer - UDP

- DNS
- QUIC
- SIP
- Gaming

Application Layer - TCP

- HTTP
- HTTPS
- SIP
- FTP
- Gaming

DDoS Attack Mitigation Techniques

Potential impact on legit users	**Commonly used countermeasures**	*Technical complexity*
High	Blackholing / RTBH	
	Destination rate limit/ traffic shaping	
	IP reputation/Geo-based blacklist	
	IPS signature-based filter	
	Per-SRC rate limit/ traffic shaping	
	L4-7 behavioral policy violation with rate limit	
	L4-7 behavioral policy violation with SRC blacklist	
	Automatic attack pattern recognition	
	Application malformed request check	
	Advance L7 challenge authentication	
	Source L4-based authentication	
	Protocol misuse & anomaly check	
	Block/rate limit amplification attacks	
Low	Packet anomaly check	

DDoS Mitigation Strategy

- *Precise tracking & anomaly detection*
- *Auto-updating threat intelligent list*
- *Comprehensive L4-7 countermeasures*
- *Automatic attack pattern recognition against zero-day attack*

How to apply these countermeasures?

Poll Question

- What is the biggest challenge you're experiencing with your current DDoS detection and mitigation solution?

1. Can't scale/growing pains
2. Can't adapt to evolving network technology
3. Difficulty in maintaining service availability
4. Sluggish performance speed
5. Inadequate detection of attacks

A10 DDoS Defense with Thunder Threat Protection System (TPS)®

A10 DDoS Defense Solution Overview

Thunder TPS

- High performance and scalable platform for mitigation and detection
- Available in
  - hardware appliance powered by Intel® Xeon® CPU and FPGA
  - Virtual appliance
  - Public Cloud (Azure)

aGalaxy

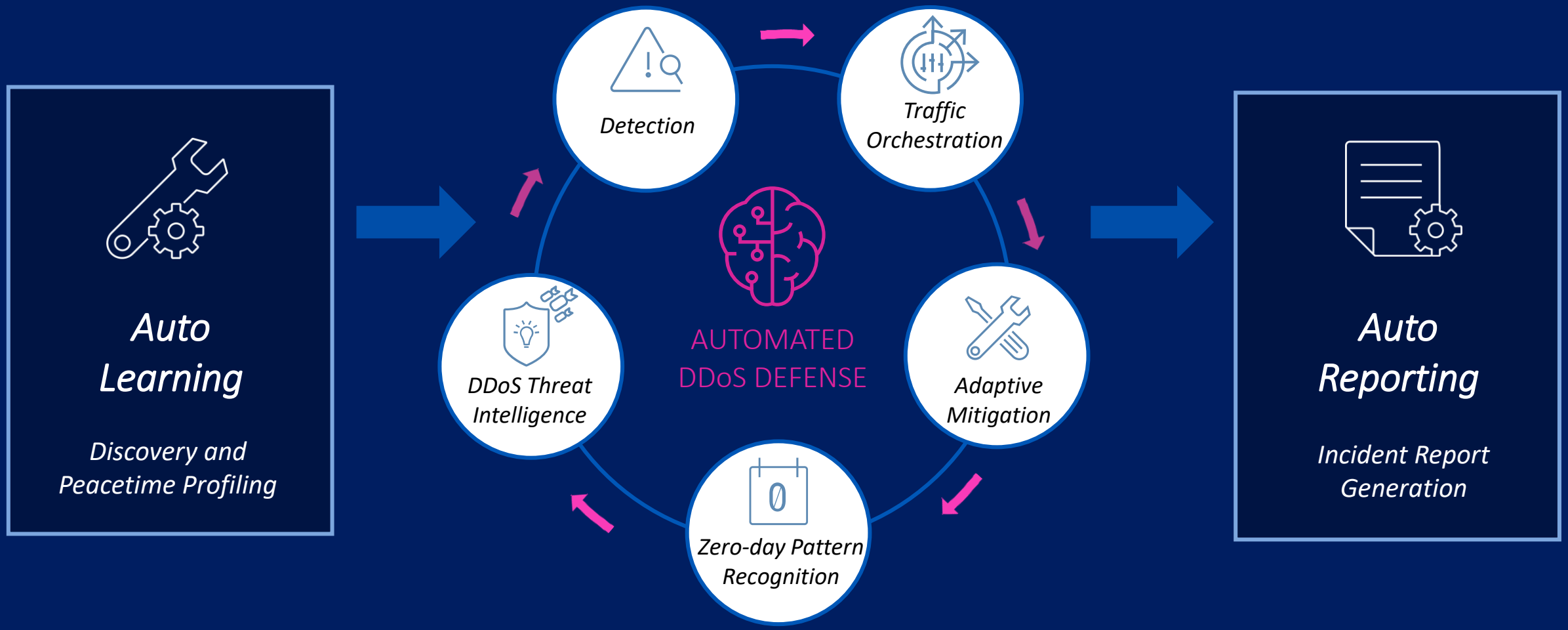
- Centralized management console and reporting
- Intelligent automaton as a DDoS defense orchestrator
- Subscriber portal for multi-tenancy
- Virtual appliance

Services

- 24x7 DDoS Incident Response Support (DSIRT) incl. wartime support
- DDoS threat and weapon Intelligence

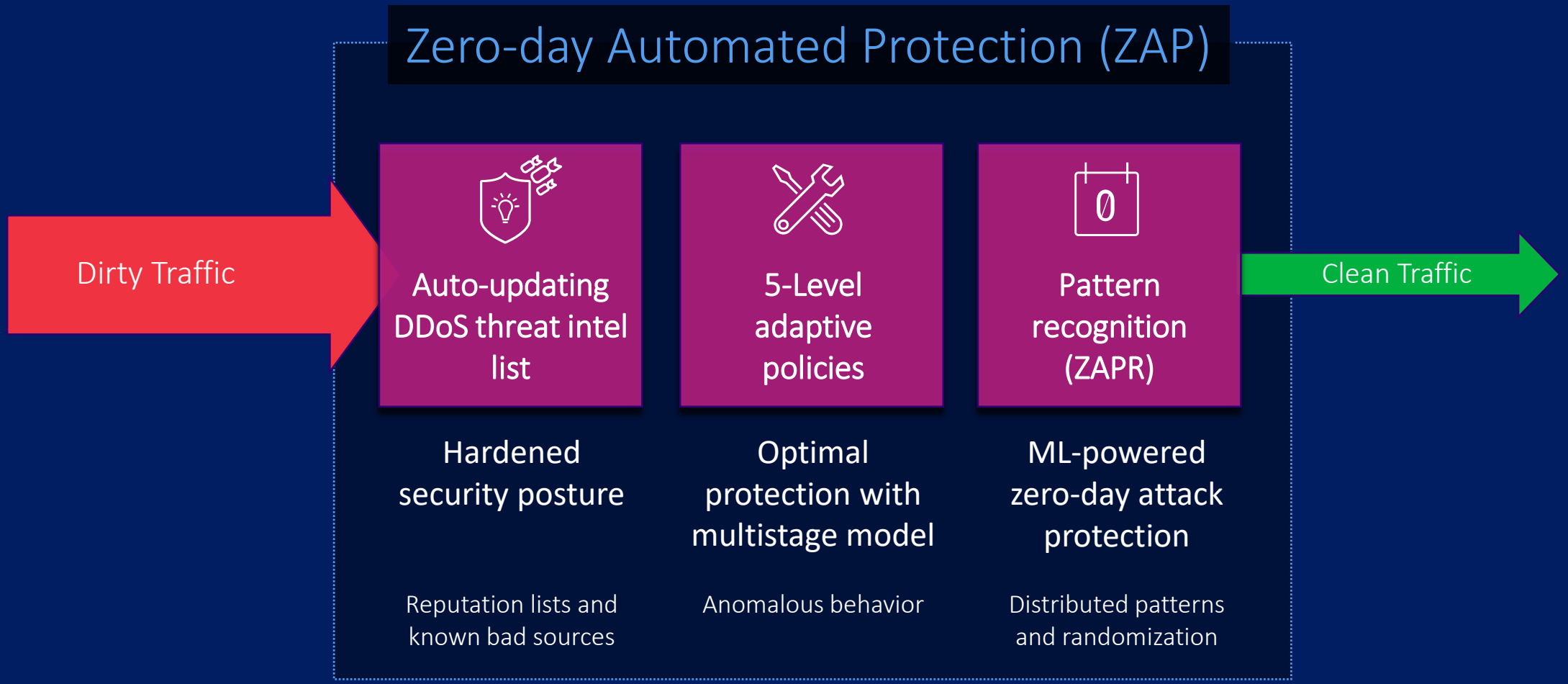
Automated DDoS Defense

Intelligent Automation Across Full Protection Cycle



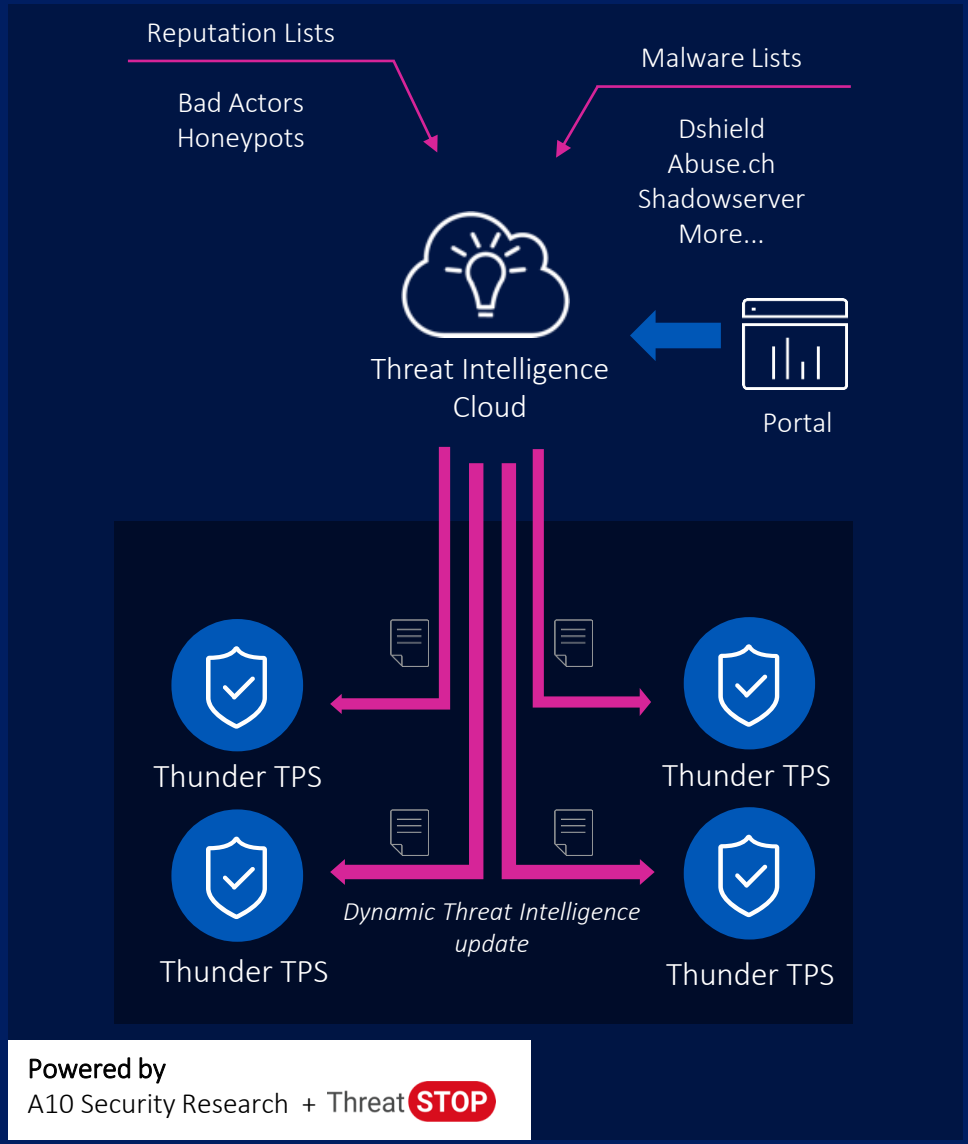
Before | **During the Attack** | **After**

In-depth Defense With Multi-modal Mitigation



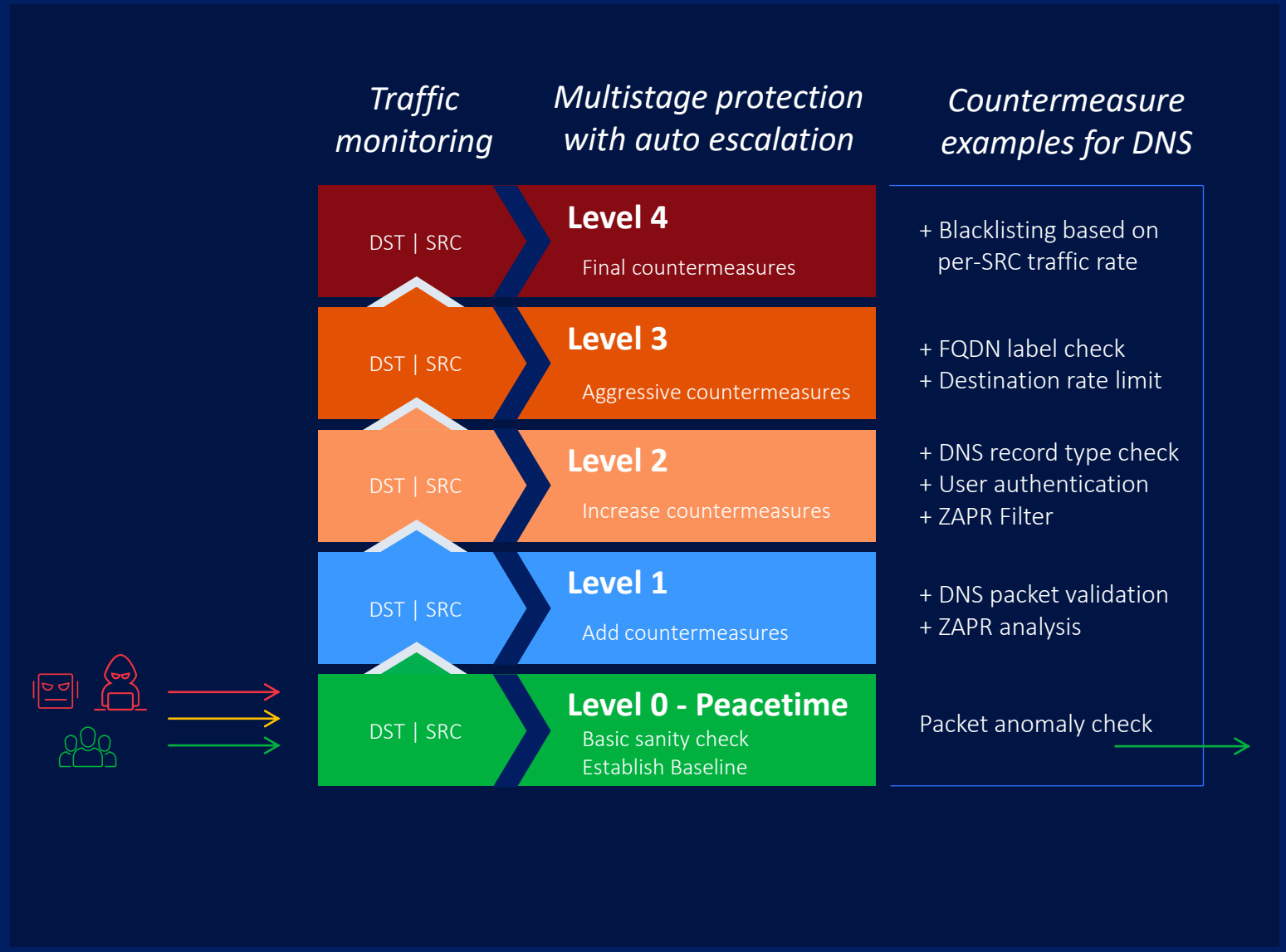
Actionable DDoS Threat Intelligence

- Block known threats proactively using high quality DDoS threat lists
- Millions of collective list for DDoS threat
  - 60+ public, private, proprietary sources
  - Expand protection against botnets, C&C communications, reflection attacks
  - Automatic periodic update
- Practicable list capacity (up to 96M) on Thunder TPS

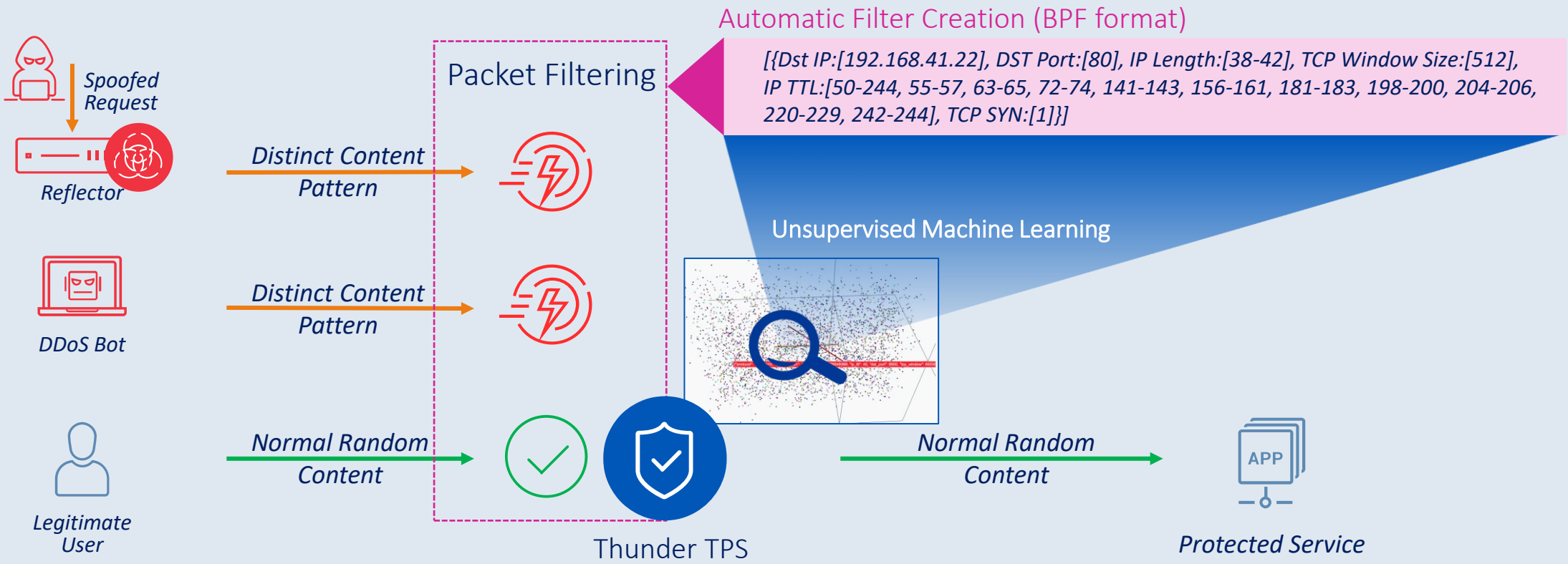


5-Level Adaptive Protection for Precision

- Auto level escalation depending on the degree & persistence of anomaly
- Operators have the option to manually intervene at any stage of an attack
- Minimize false positive & false negative

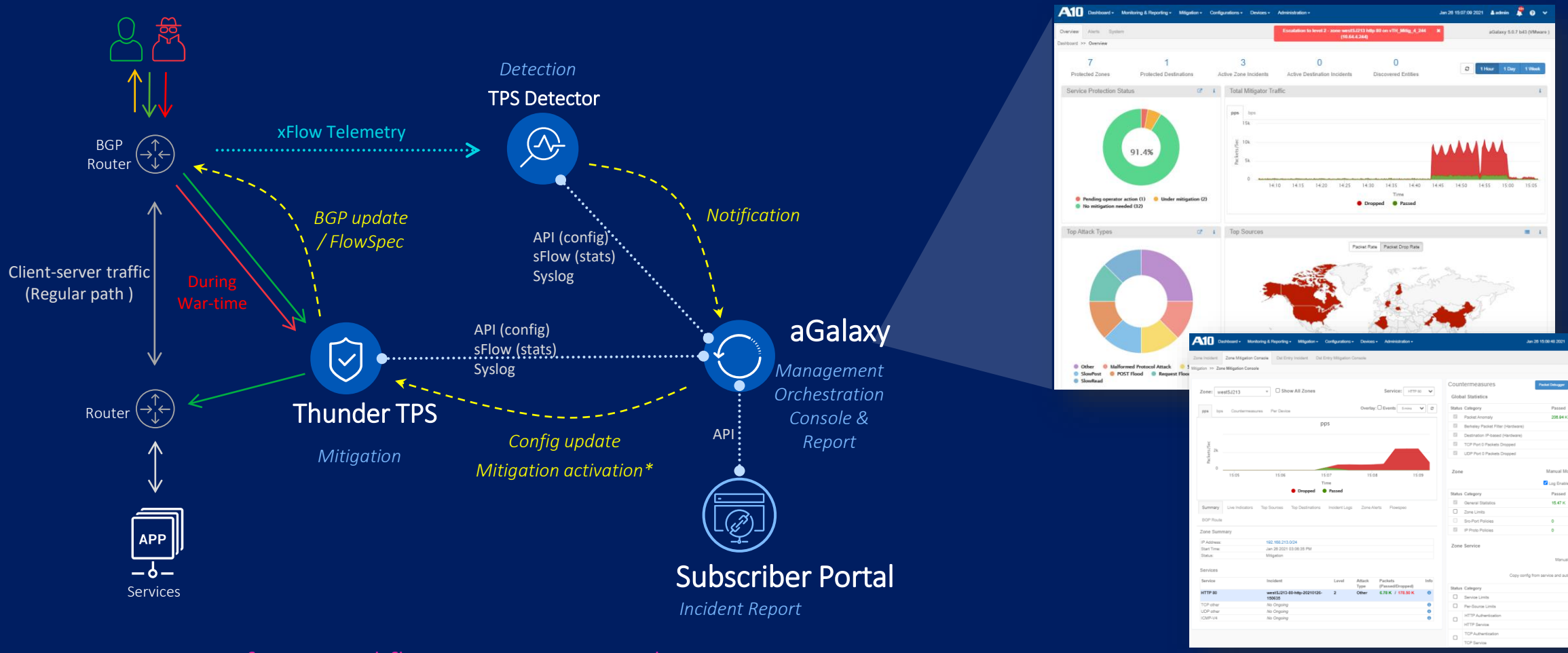


Zero-day Attack Pattern Recognition (ZAPR)



Intelligent & realtime mitigation against Zero-day DDoS attack

aGalaxy - Automation & Management



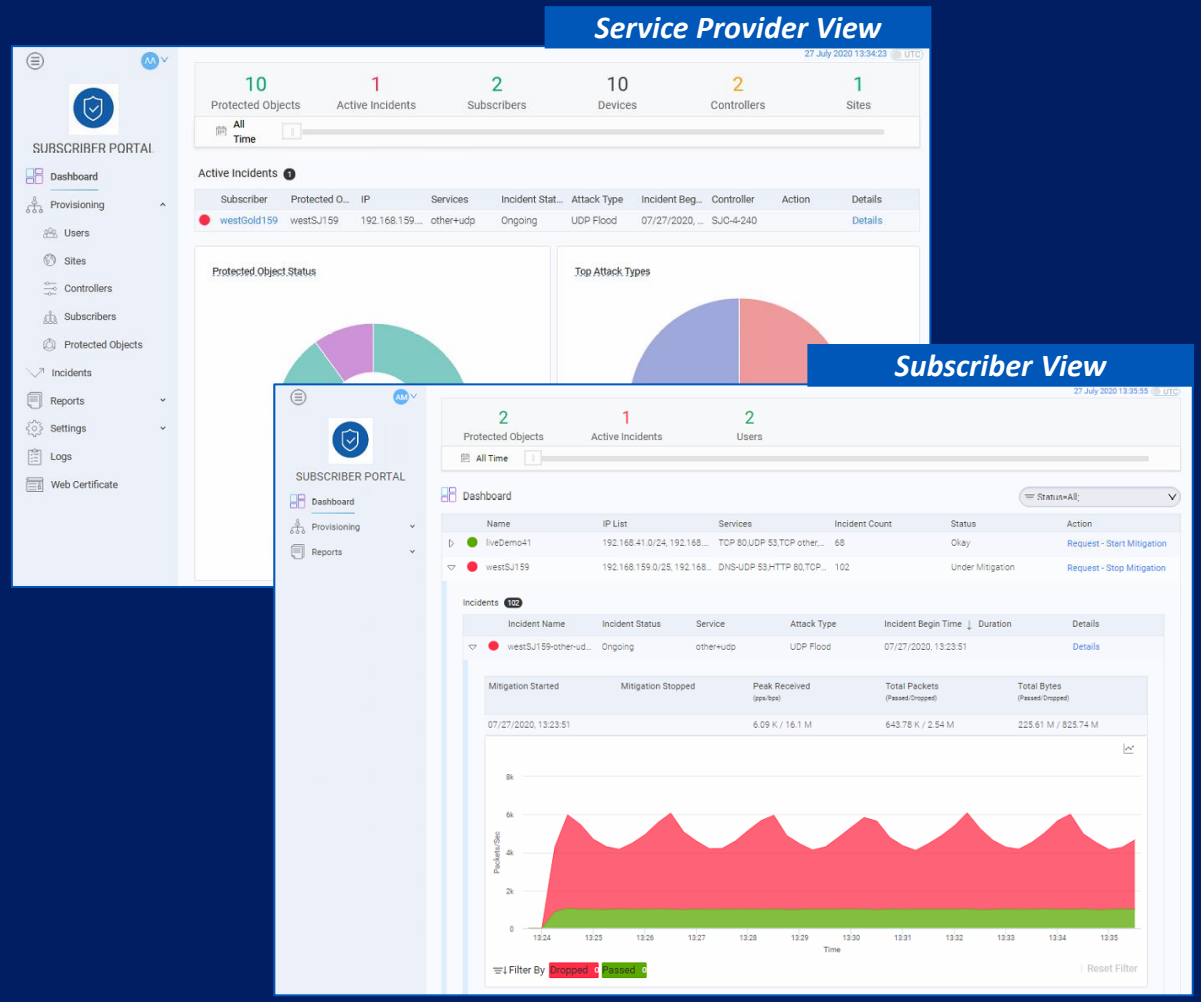
DDoS Defense workflow in Reactive Deployment

* Mitigation can be activated automatically or manually

Case Study Examples
DDoS Protection Services

DDoS Protection Service

- Off-the-shelf subscriber portal for DDoS Protection-as-a-Service MSSPs
- Provides a simplified user experience and additional security
  - Admin portal for aGalaxy integration
  - Supports multiple aGalaxy deployments, providing consolidated service visibility to subscribers
  - Multi-tenant with granular incident view and on-demand reporting for subscribers
- Tailored views for Service Providers and Subscribers



Data Center DDoS Scrubbing Service

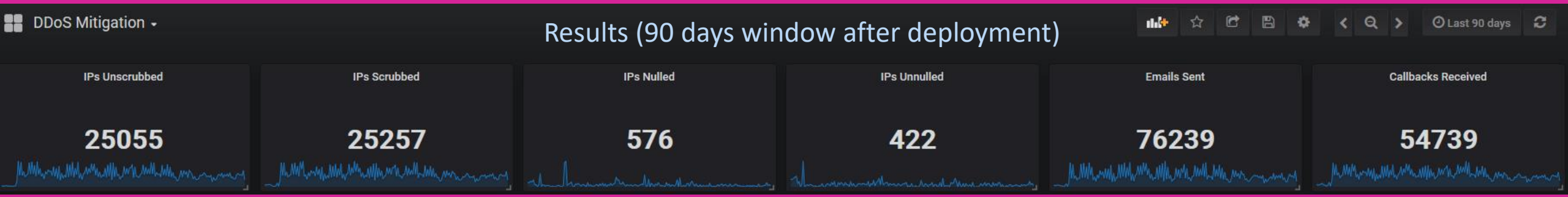
Results After Deployment

Attacks Mitigated

Reduction in Support Tickets

Increased NPS

> The ability to automate and scale the delivery of differentiated services could have a major impact on the quality and economics of DDoS scrubbing services. A10's innovations are significant advancements.
>
> leaseweb — Bart van der Sloot, Managing Director of Leaseweb Network



Summary

Choose The Best DDoS Defense

What Makes A DDoS Protection Solution Better Than The Other?

Precision

Avoid costly collateral damage

Automation

Make personnel limitations more effective and efficient

Scalability

Optimize short term and protect long-term investments

Affordability

Performance by design to offer solutions that make economic sense

Three Steps to Stronger Security

01

Evaluate and Upgrade DDoS Defenses
Include multi-vector as well as volumetric defense

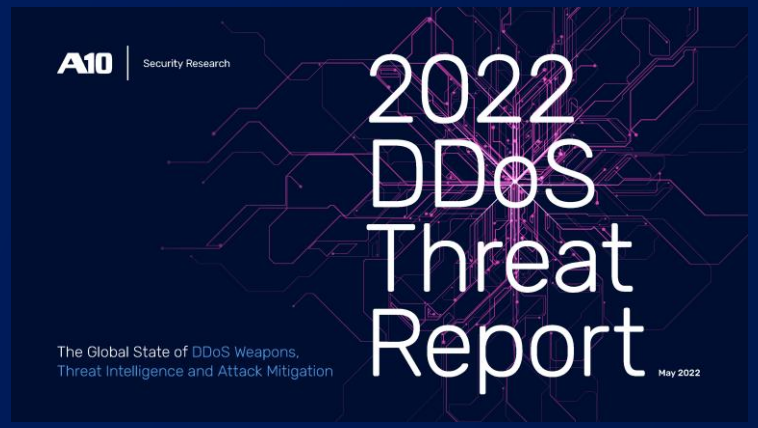
02

Protect Tenants – Consider DDoS protection services

03

Collaborate with Industry- build threat intelligence

Visit us at: www.A10networks.com



Download Today:
2022 A10 Networks
DDoS Threat Report

A10

Always Secure. Always Available.

Terry Young
tyoung@a10networks.com

Taka Mitsuhata
tmitsuhata@a10networks.com