Protecting your network from DDoS attacks

Graeme Antrobus
EMEA Sales Engineer
NTT DATA | Global IP Network
graeme.antrobus@global.ntt

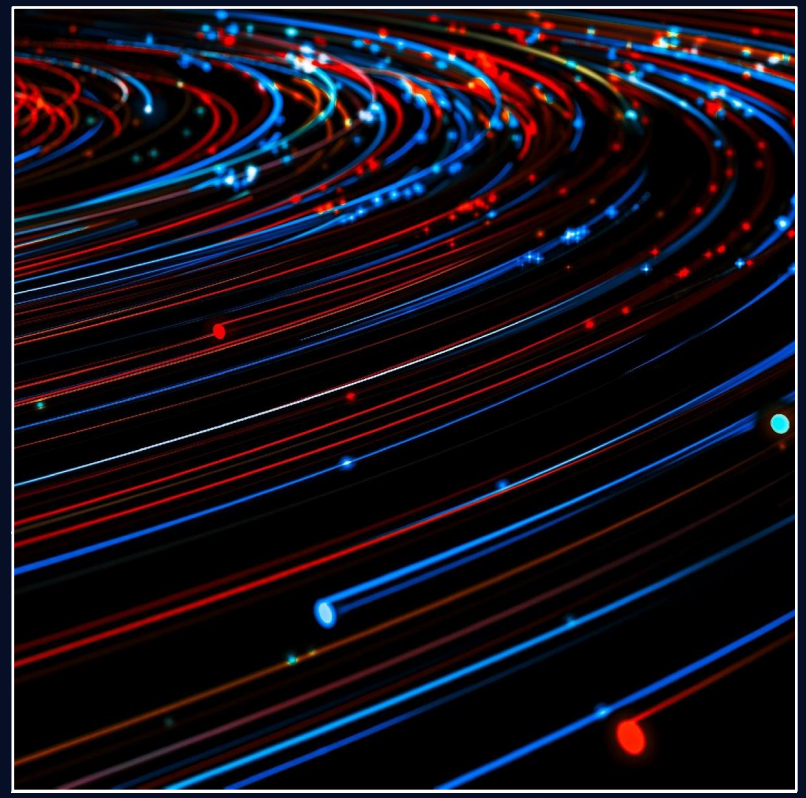
March 2025

Agenda

I. Part 1: The Threatscape
II. Part 2: Mitigation Strategy
III. Part 3: The Solution

Part 1

The Threatscape



The Threatscape

Radware's Cyber Threat Report: Web DDoS attacks surge 550% in 2024

Geopolitics, a growing threat surface, and AI tech drive bigger, longer, and more intense attacks.

Feb. 26, 2025

CrowdStrike: Cyber threats skyrocket as attackers think like businesses

Nadine Hawkins February 27, 2025 08:01 AM

The World's Most Popular Flight Tracker is Fighting An Ongoing DDoS Cyber Attack

BY MATEUSZ MASZCZYNSKI
5TH MARCH 2025

Web DDoS attacks see major surge as AI allows more powerful attacks

News By Sead Fadilpašić published 2 days ago

Layer 7 Web DDoS attacks increased five-fold in the span of a year

European Cyber Report 2025: 137% more DDoS attacks than last year - what companies need to know

NEWS PROVIDED BY
Link11 GmbH →
05 Mar, 2025, 12:33 GMT

SHARE THIS ARTICLE

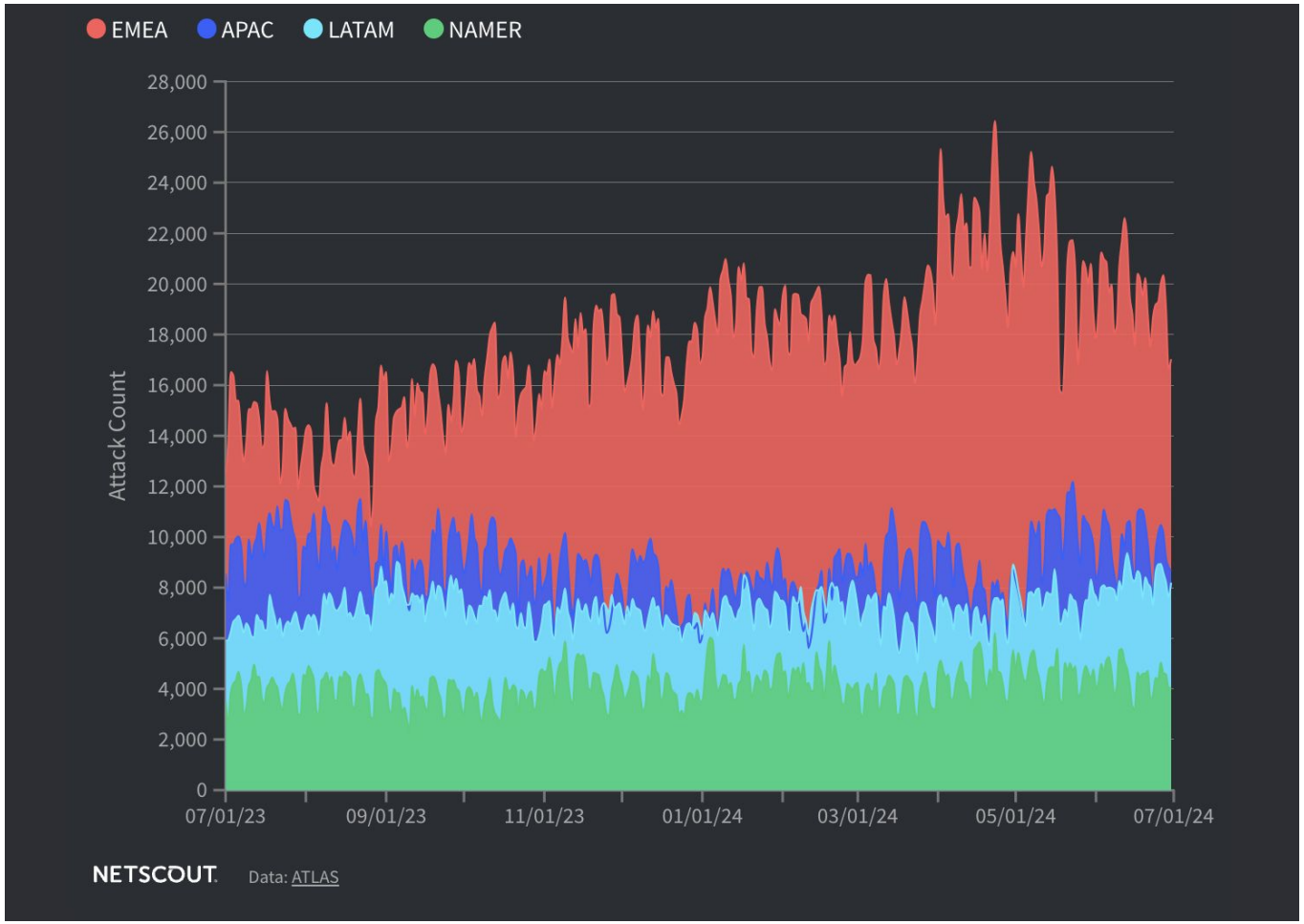
Eleven11bot Captures 86,000 IoT Devices for DDoS Attacks

by Jeffrey Burt on March 5, 2025

NTT DATA

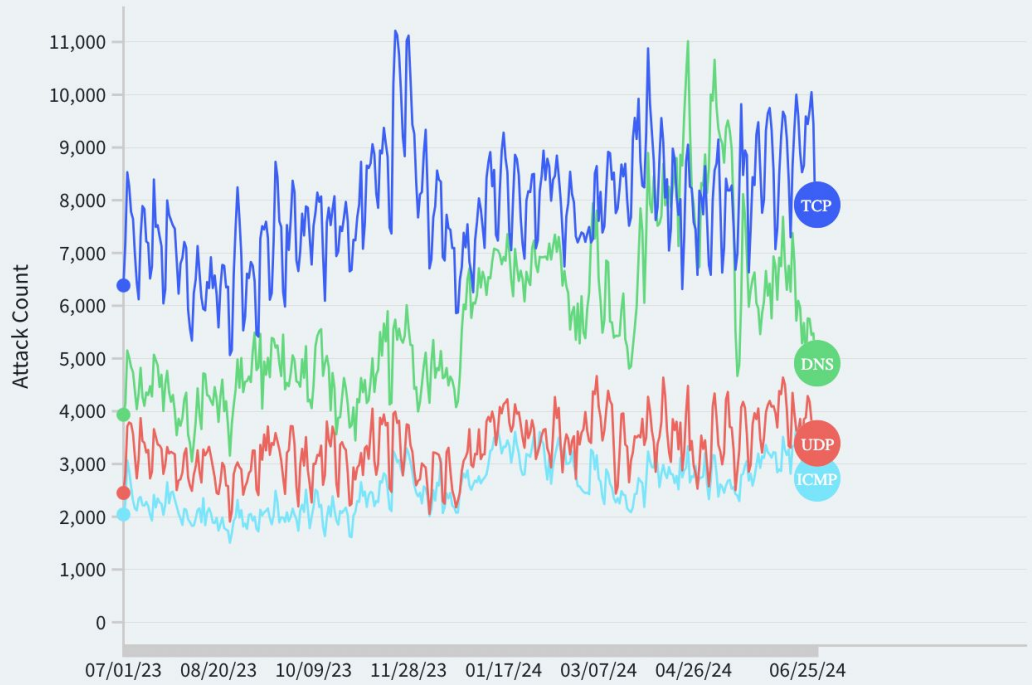
Daily Regional Attack Count (2023–2024)

Greatest volume of attacks are in EMEA



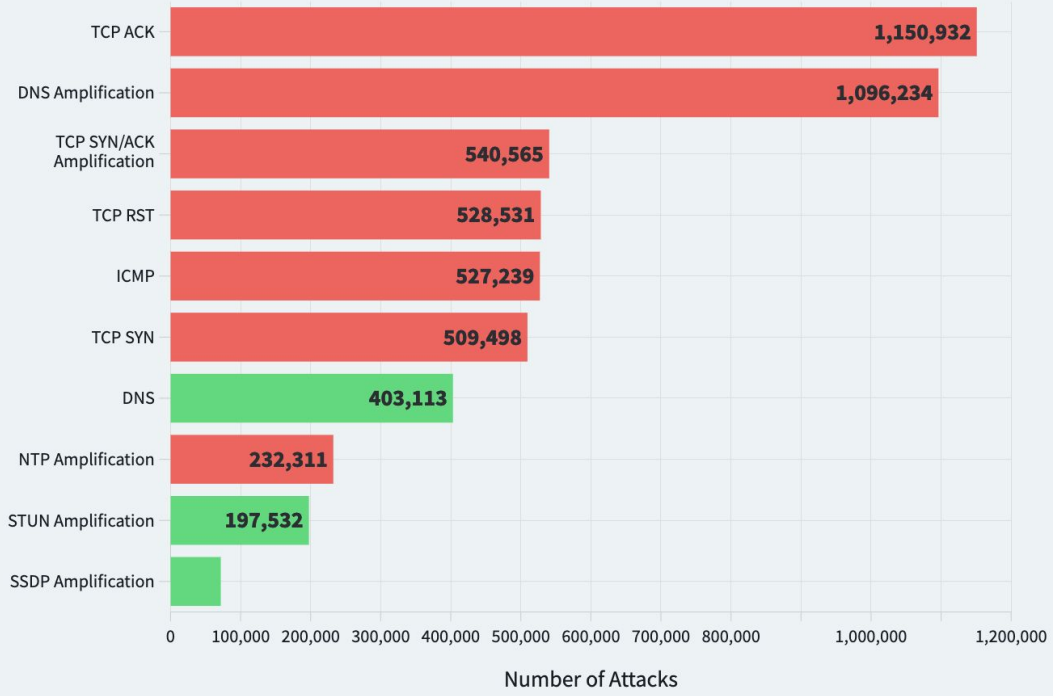
Top 10 EMEA DDoS Attack Vectors (2023 - 2024)

TCP most common attack vector



NETSCOUT. Data: ATLAS

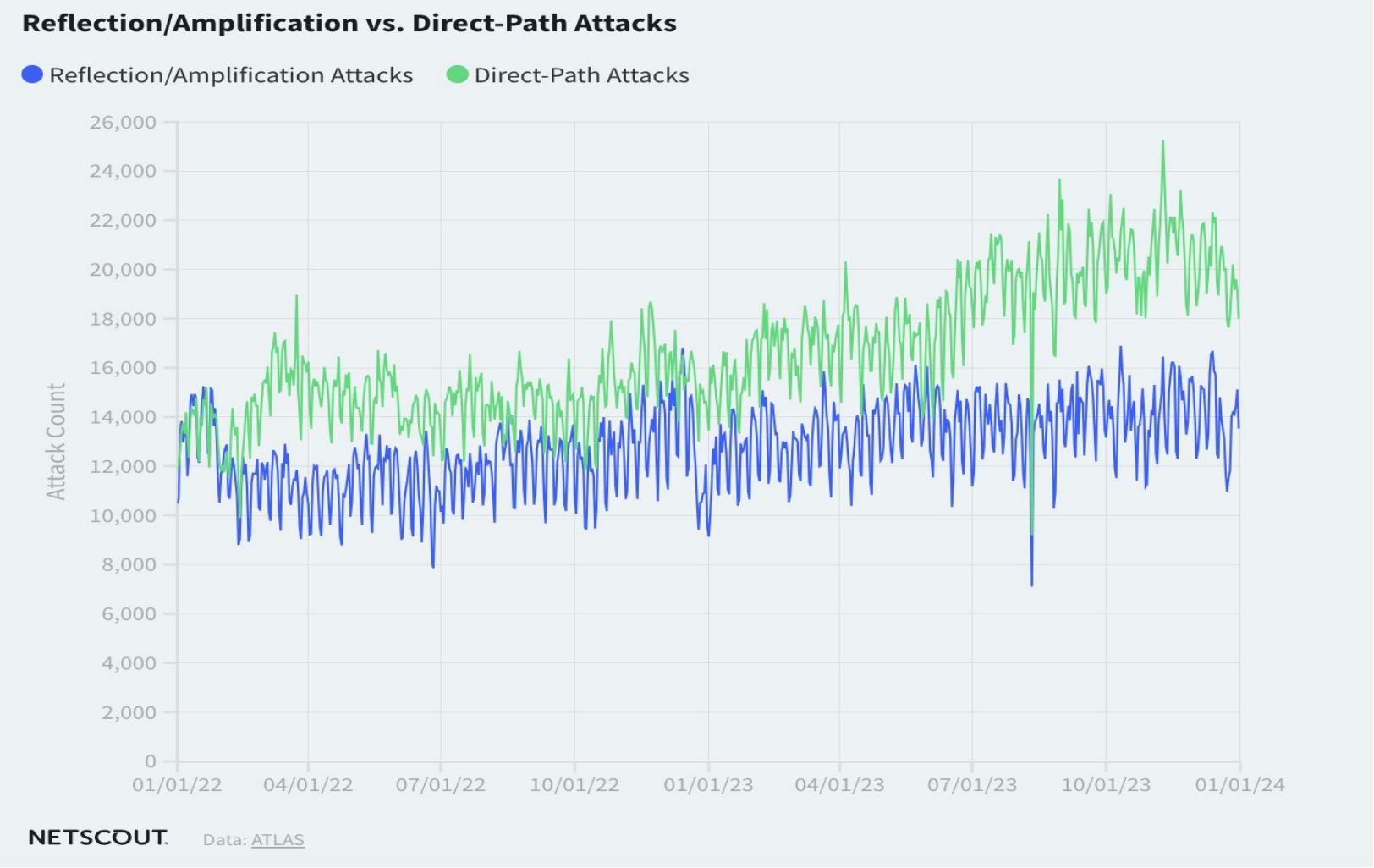
Note: It should be noted that many attacks are multi-vector and will include both TCP and UDP or some other combination. The above graphic is intended to show proportionality of distinct vectors used in attacks.



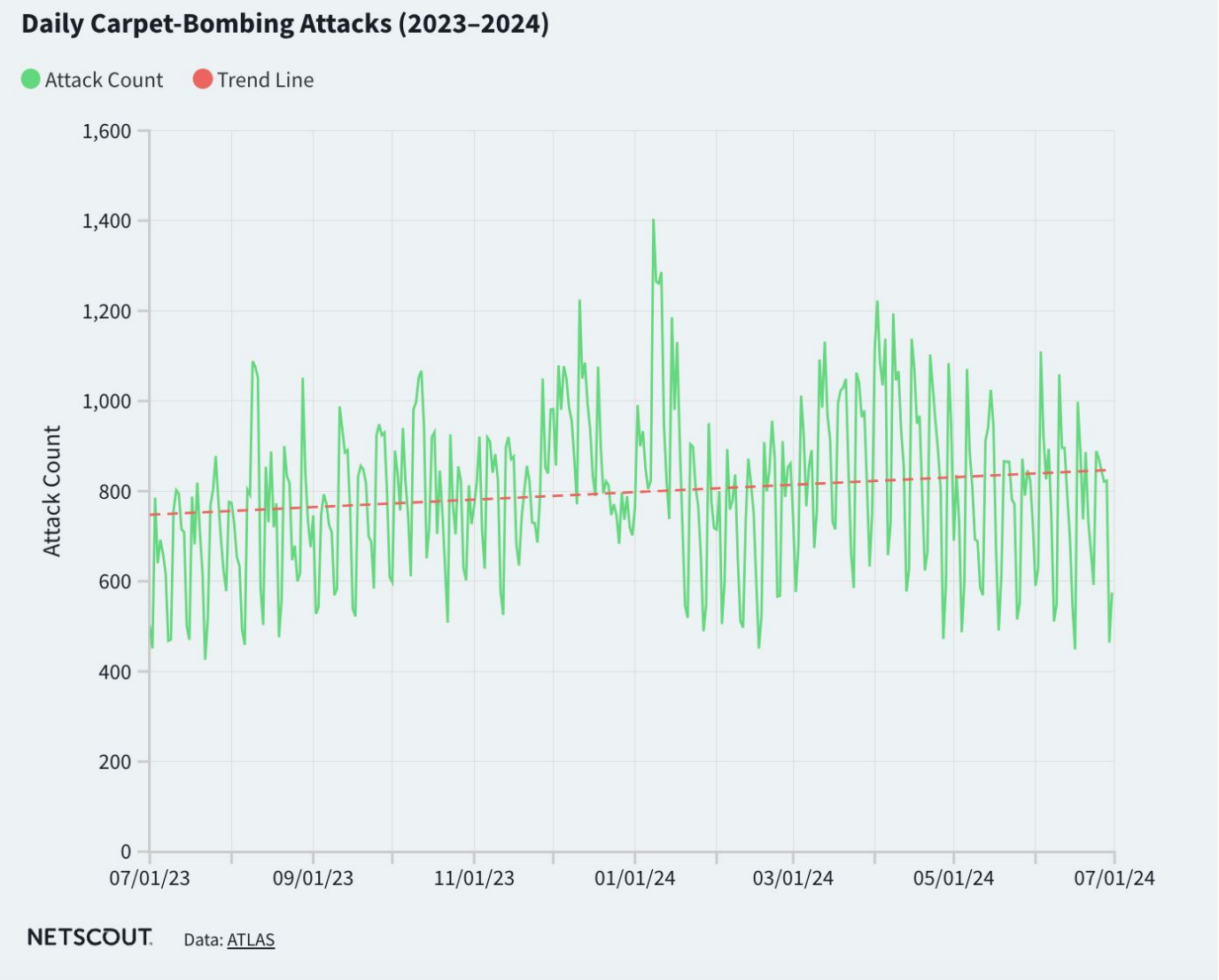
NETSCOUT. Data: ATLAS

Note: This is a sampling of our dataset.

DDoS Attack Methods – Amplification Attacks vs Direct-Path Attacks

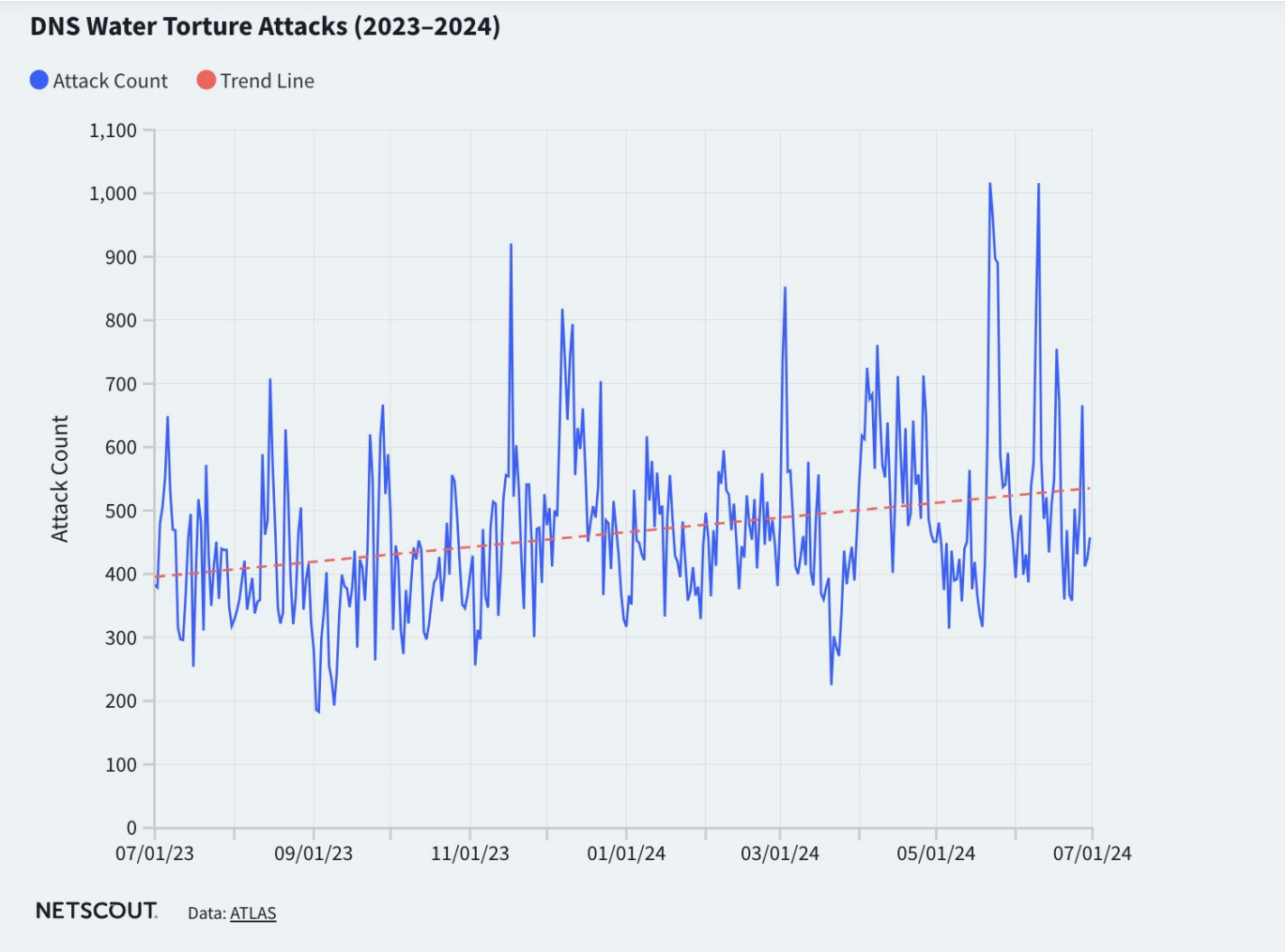


Carpet Bombing Attacks – NetScout & NTT DATA



NTT DATA Global IP Network
2023 vs 2024
25.2% Increase

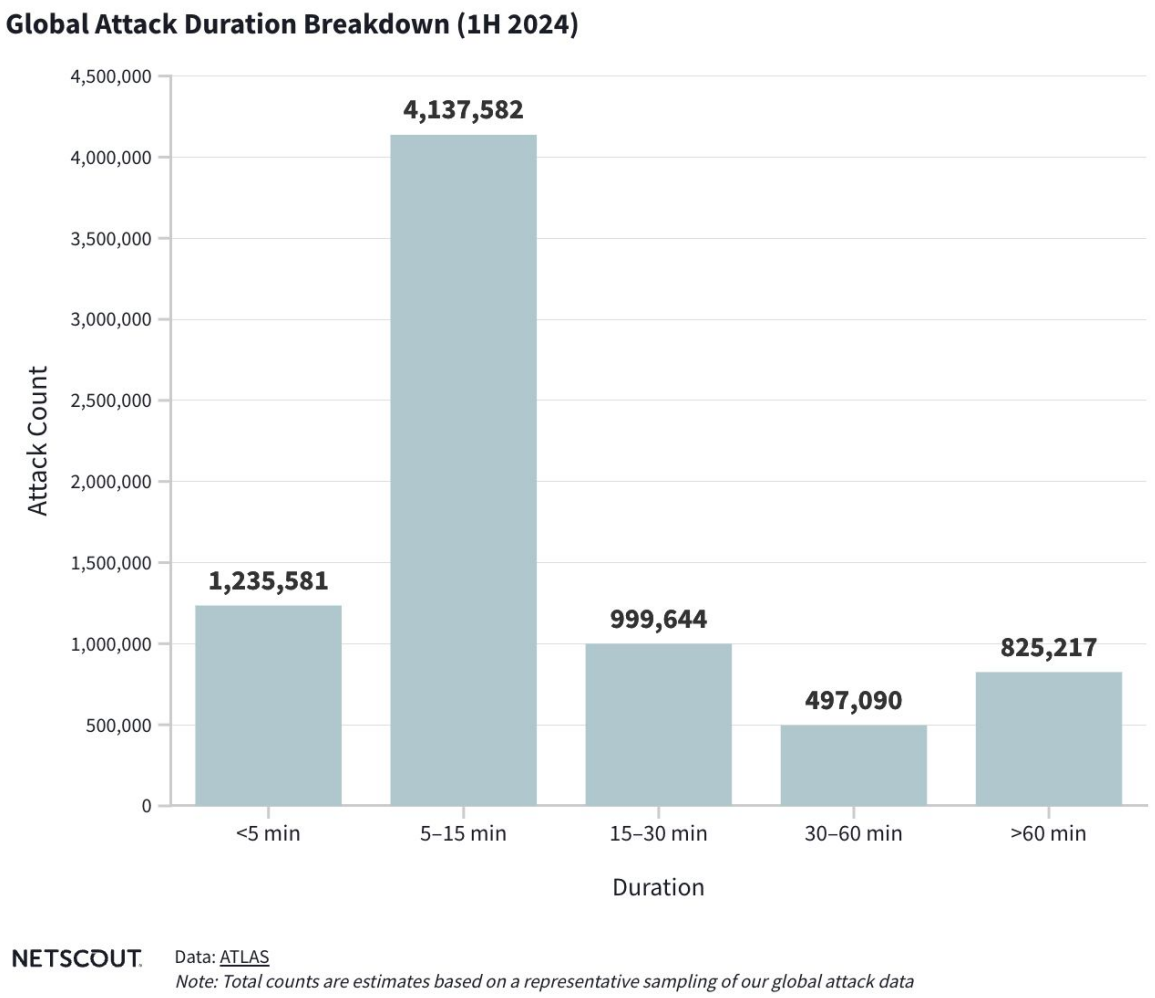
DDoS Attack Methods – DNS Water Torture Attacks



NTT DATA Global IP Network
2023 vs 2024
19% Increase

DDoS Attack Duration

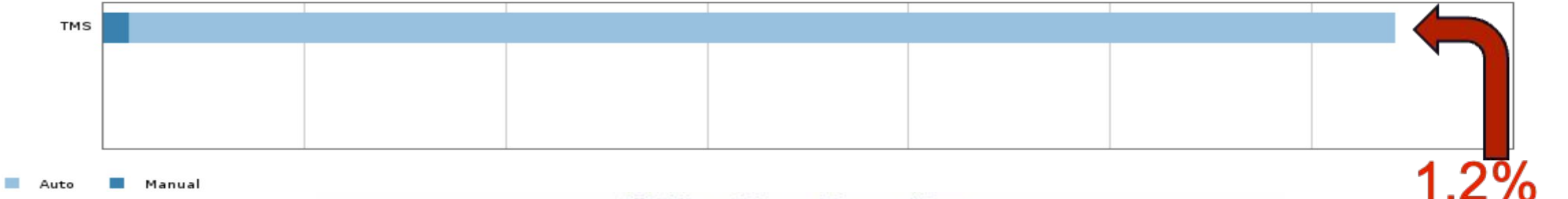
Majority of attacks are quicker than human intervention – use automation.

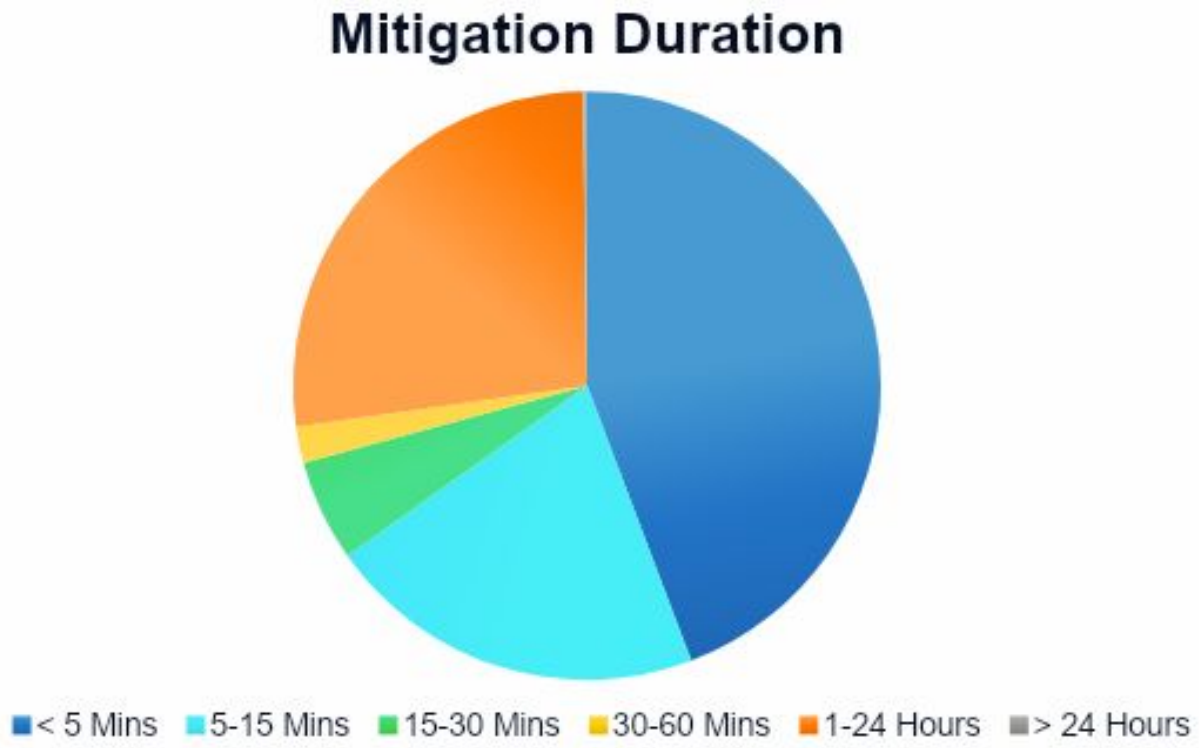


DURATION BY PERCENTAGE	
<5 min	16%
5–15 min	54%
15–30 min	13%
30–60 min	6%
>60 min	11%

DDoS Attack – Mitigations & Durations (2023-2024)

Mitigations Auto vs Manual





Part 2

Mitigation Strategy

Tools for DDoS Mitigation – Remotely Triggered Black Hole

Remotely Triggered Black Hole (RTBH)

- Capability: Blocks ALL traffic to a destination IP address, bad AND good 
- Requires changes in route announcement configuration
  - A multi-homed network has to setup this capability with all upstream providers to be effective
  - ... or withdraw the aggregate / announce a more specific via a single upstream

Can be deployed rapidly once setup

- NTT Selective Black Hole can reduce impact with regional and country control
- Best suited for maintaining availability of rest of network while attacked destination IP becomes unreachable

Tools for DDoS Mitigation – Access Control Lists

Access Control Lists (ACL)

- Capability: Block SOME traffic to or from specific destination or source IP addresses
- Requires one-off setup in advance with the provider
  - ACLs may also need maintenance in coordination with the provider as services and attacks evolve
- Can be deployed rapidly
- ACL sizes and complexity are finite, limits types of TCP and UDP attacks that can be filtered
- Depending on the specified ACL, may still affect good AND bad traffic
- Best suited for reducing attack surface – limit traffic you don't intend to receive and reduce efficacy of some categories of attacks

Tools for DDoS Mitigation – Intelligent Mitigation

Intelligent Mitigation (IM)

- Capability: Scrubs traffic, removing unwanted but keeping wanted flows
- Requires one-off setup in advance with the provider
  - Works best with a bit of context, which services are provided (or never provided) on which IP ranges?
- Automated mitigation option allows for rapid response
  - As quickly as 30 seconds to detect and begin mitigating per NTT DATA Global IP Network testing
- Manual mitigation option allows customers to test, pre-emptively mitigate
- Highly effective for many services and attacks types
  - May not be suitable for some encrypted traffic
- Best suited for maintaining availability of services while under attack

Deploying the Toolkit

Consider Combining the Tools for Impact

- Use NTT DATA's Selective RTBH to restrict reach to geographically feasible traffic origins
  - E.g. a European firm with a European customer base may black hole traffic originating outside Europe

- Use ACLs to reduce attack surface
  - Filter traffic from the Internet that's irrelevant to your application
  - Filter common attack vectors, internal services
  - Allow external DNS, NTP, …

- Use a mitigation solution like our DDoS Protection Services (DPS)
  - Allows mitigating highly distributed attacks and attacks occurring across multiple vectors
  - Helps keep services under attack accessible

Your Team is Your Greatest Asset

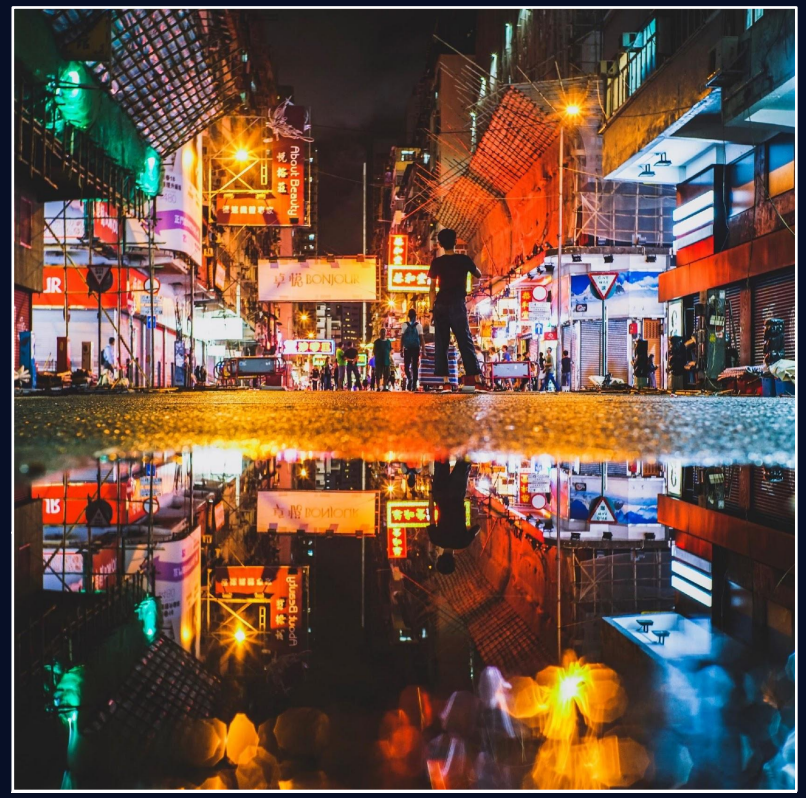
Develop a team and a process for responding to DDoS and security incidents

- Have checklists and playbooks
  - Ensure they're accessible even when your own network is under attack
  - Have key phone numbers, URLs, and e-mail addresses listed
  - If you self-host e-mail, have at least one off-network account
  - If you self-provide internet access, ensure you have:
    - Out-of-band (OOB) management access to your resources which does not share fate
    - Secondary Internet connectivity for key team members
- Train and test your team regularly
  - Ask your provider to conduct war games with your team
  - Repeat regularly to identify anything that may have changed ahead of time

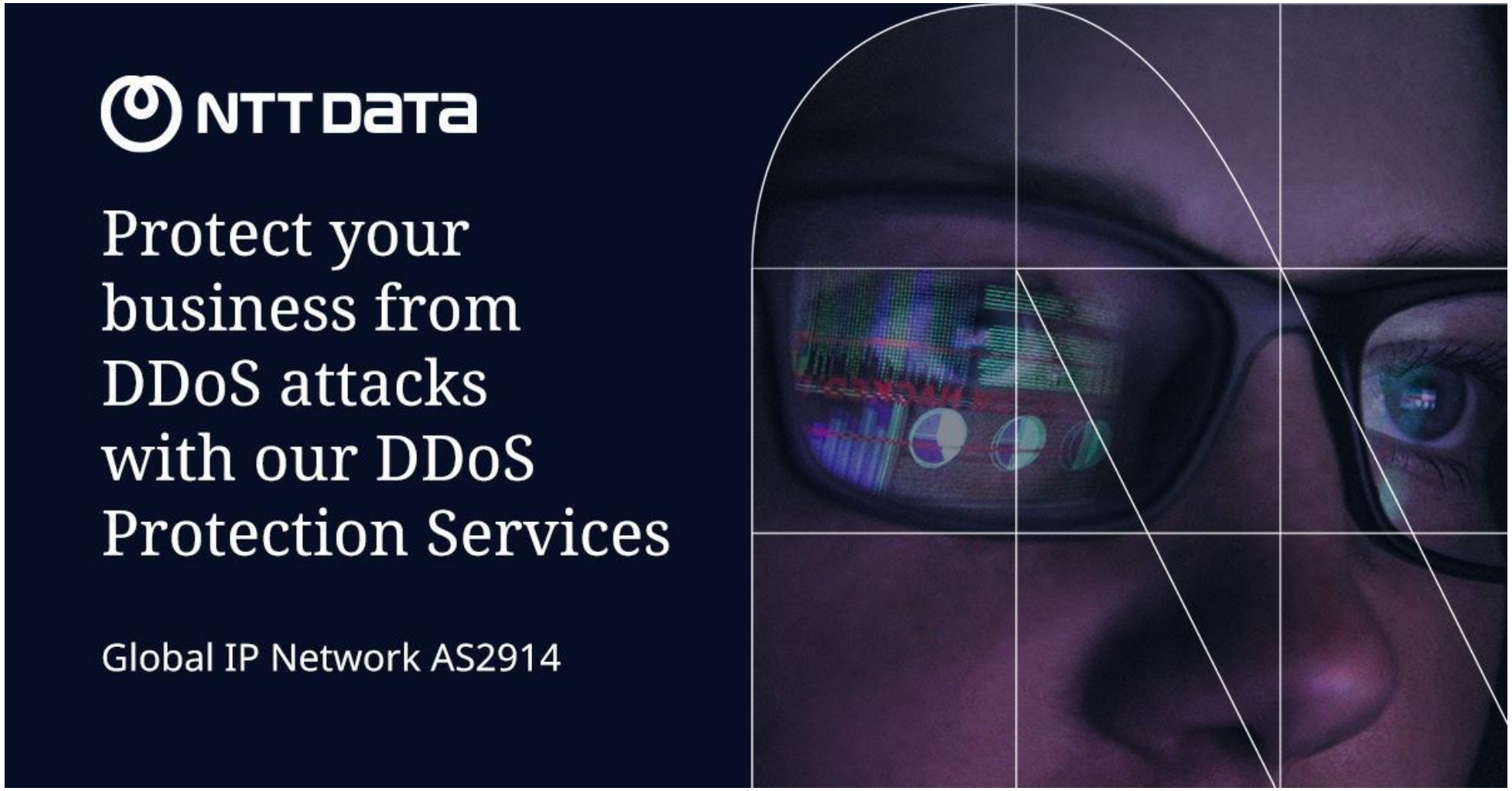
It's not much fun resetting expired passwords under duress!

Part 3

The Solution



The Solution



Solutions by NTT DATA - Blackhole and Selective Blackhole

Global Real Time Blackhole Service

- Drops traffic to destination IP across the entire NTT DATA Global IP Network backbone
- Available to all IP transit customers after initial set-up at no cost

Selective Real Time Blackhole Service

- Allows fine-tuning of blackhole announcements
  - Drops traffic only inside/outside of announcement region/country

❖ **Available to all IP transit customers after initial deployment at no extra cost**

NTT DATA Global IP Network Solutions - DDoS Protection Services

Basic Protection → Fully Automated

DPS Control
Permanent ACL

DPS Core

Permanent ACL

Customer Requested Mitigation

DPS Detect

Permanent ACL

Customer Requested Mitigation

Customer Initiated Mitigation

DDoS Detection

DPS Max

Permanent ACL

Customer Requested Mitigation

Customer Initiated Mitigation

DDoS Detection

Auto-Mitigation

DPS SP

Permanent ACL

Customer Requested Mitigation

Customer Initiated Mitigation

DDoS Detection

Auto-Mitigation

Protection and Reporting for End-Users

Flexible DDoS Protection Solutions for Every Customer

NTT DATA Global IP Network Solutions - DDoS Mitigation Platform

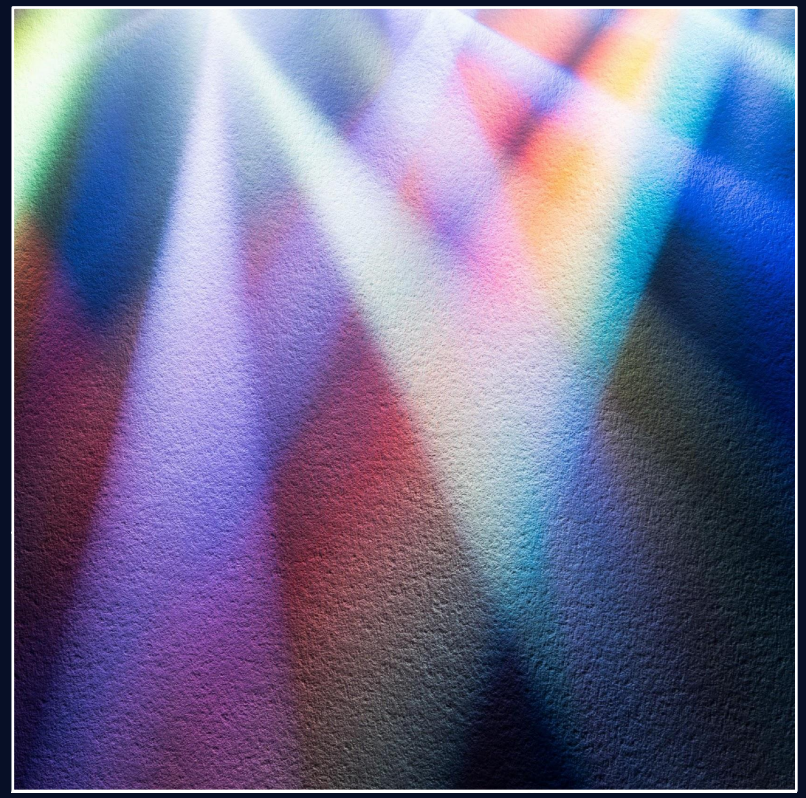
NetScout solution

- Arbor Sightline for DDoS detection
- TMS HD1000 Appliances for scrubbing

<u>Thirteen</u> strategically located mitigation platform locations on <u>five</u> continents

- Attacks can be mitigated closer to the attack origin
- Mitigation Platform locations:
  - **Asia:** Hong Kong, Singapore, and Tokyo
  - **Oceania** : Sydney
  - **Europe:** Amsterdam, Frankfurt, and London
  - **North America:** Ashburn, New York, Miami, Los Angeles, and San Jose
  - **South America:** São Paulo

Thank you!



Graeme Antrobus
Sales Engineer
NTT DATA | Global IP Network
graeme.antrobus@global.ntt

@GinNTTnet #globalipnetwork #AS2914

Follow us on

LinkedIn and X

NTT DATA

NTT DATA