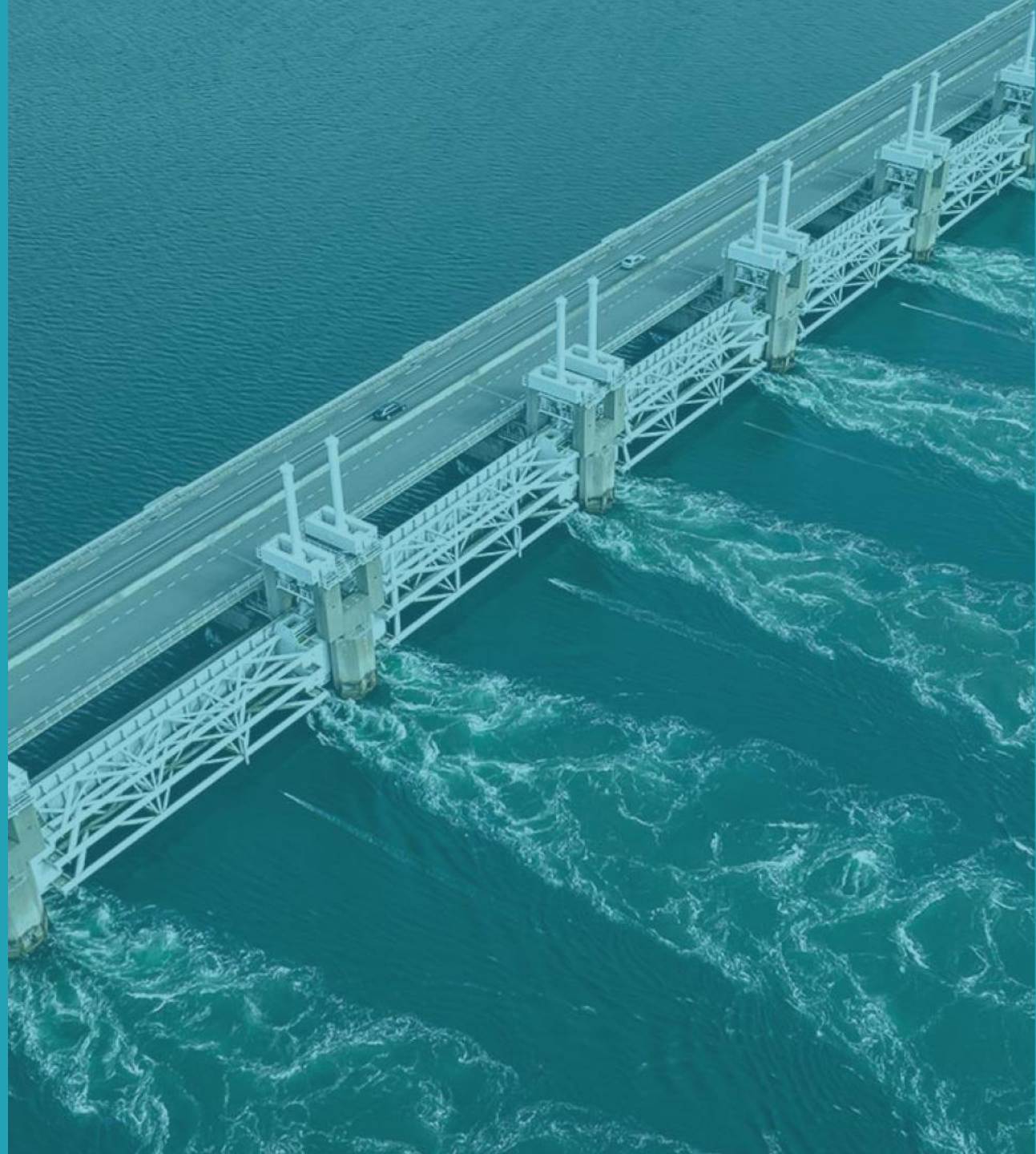
Nationale Beheersorganisatie Internetproviders

DDoS Landscape as you have never seen it before

NBIP • 11 June 2026

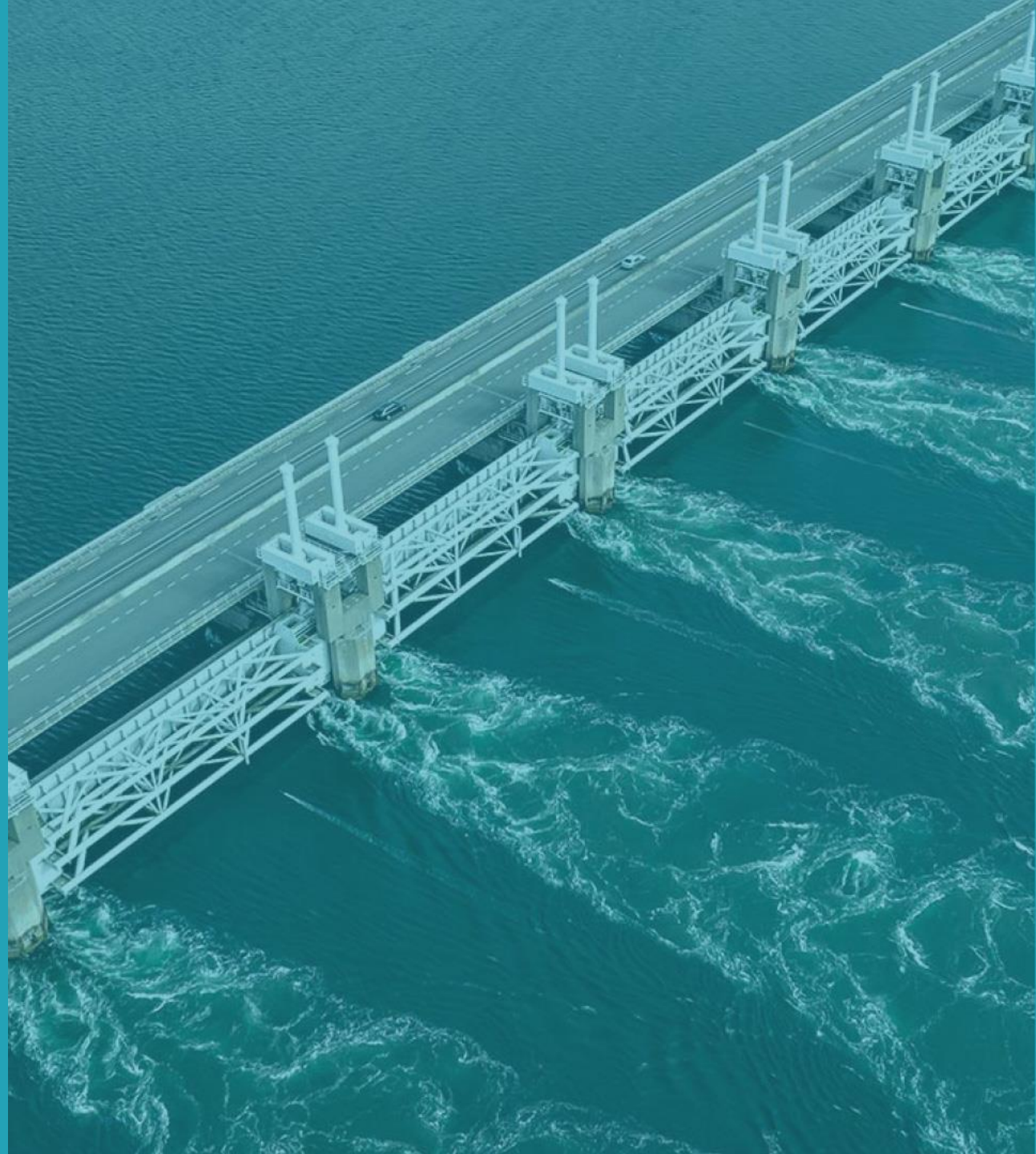
DDoS Data

Signal to Noise

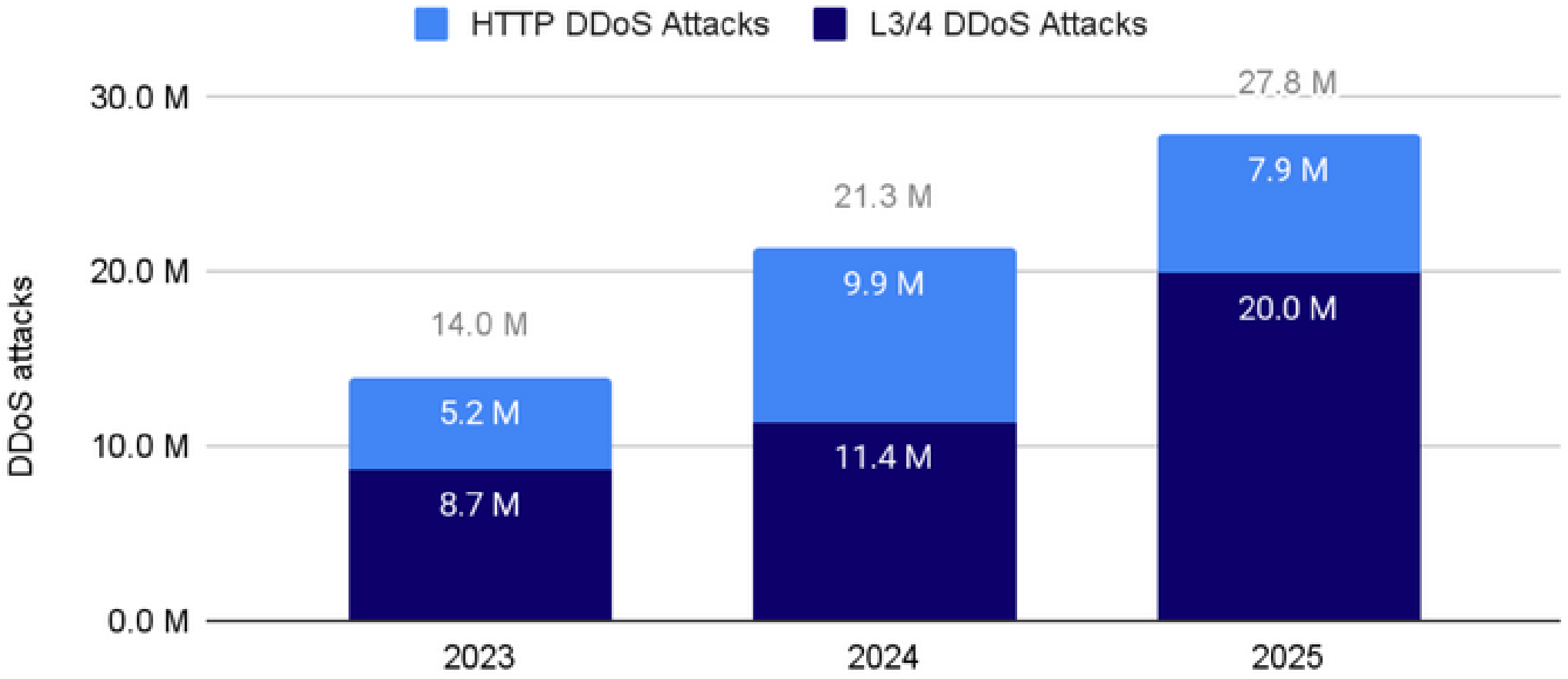


DDoS Data

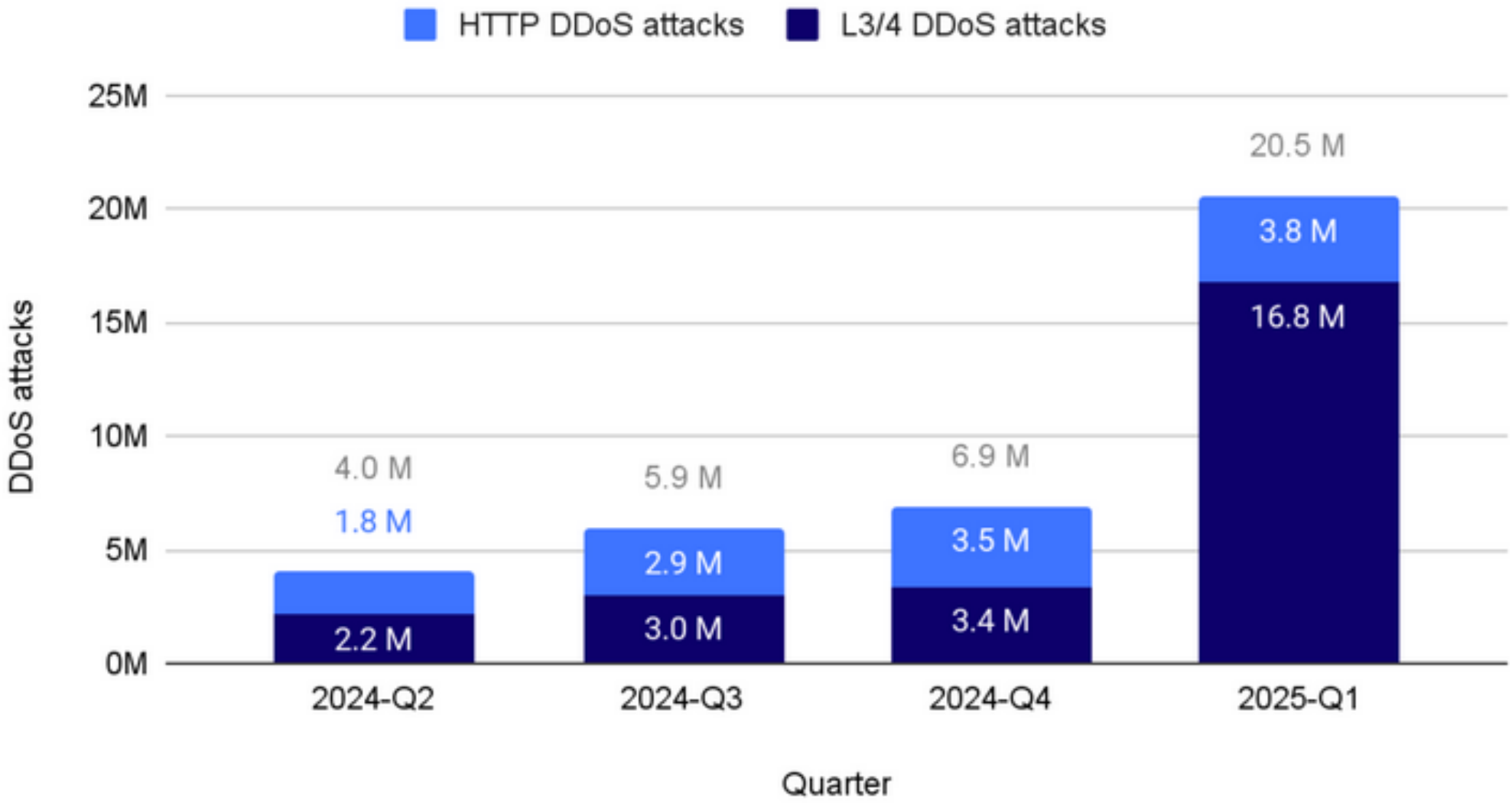
- **Trends 2025**



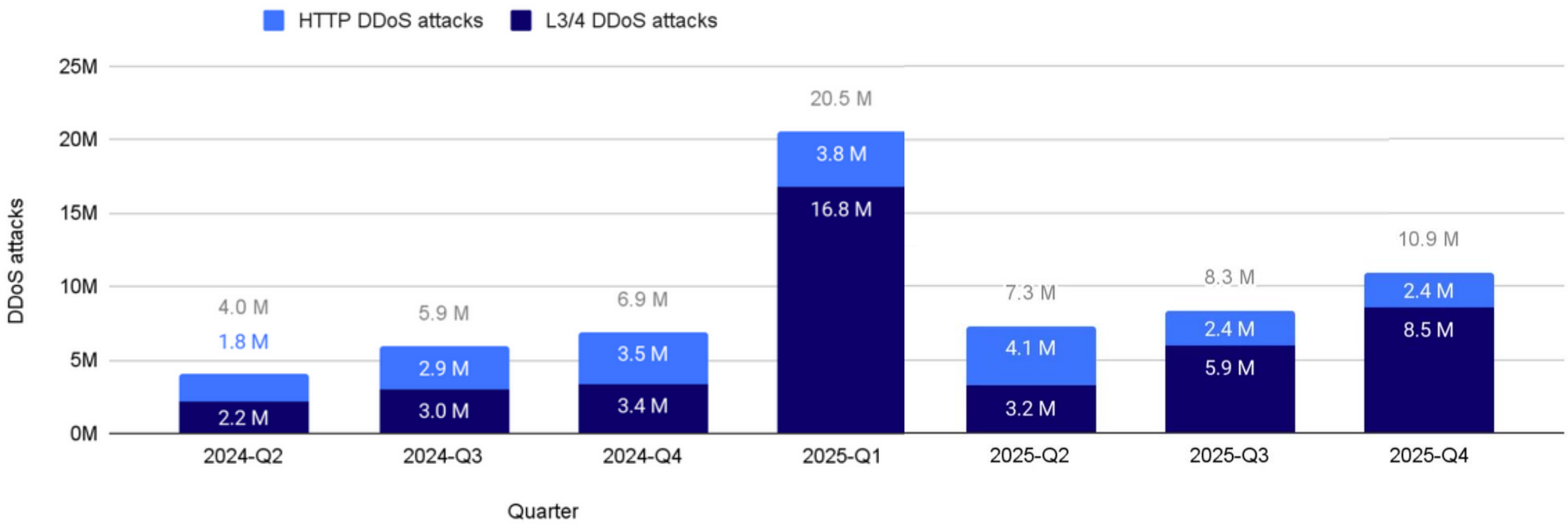
Largest DDoS Trend shift 2025



Largest DDoS Trend shift 2025

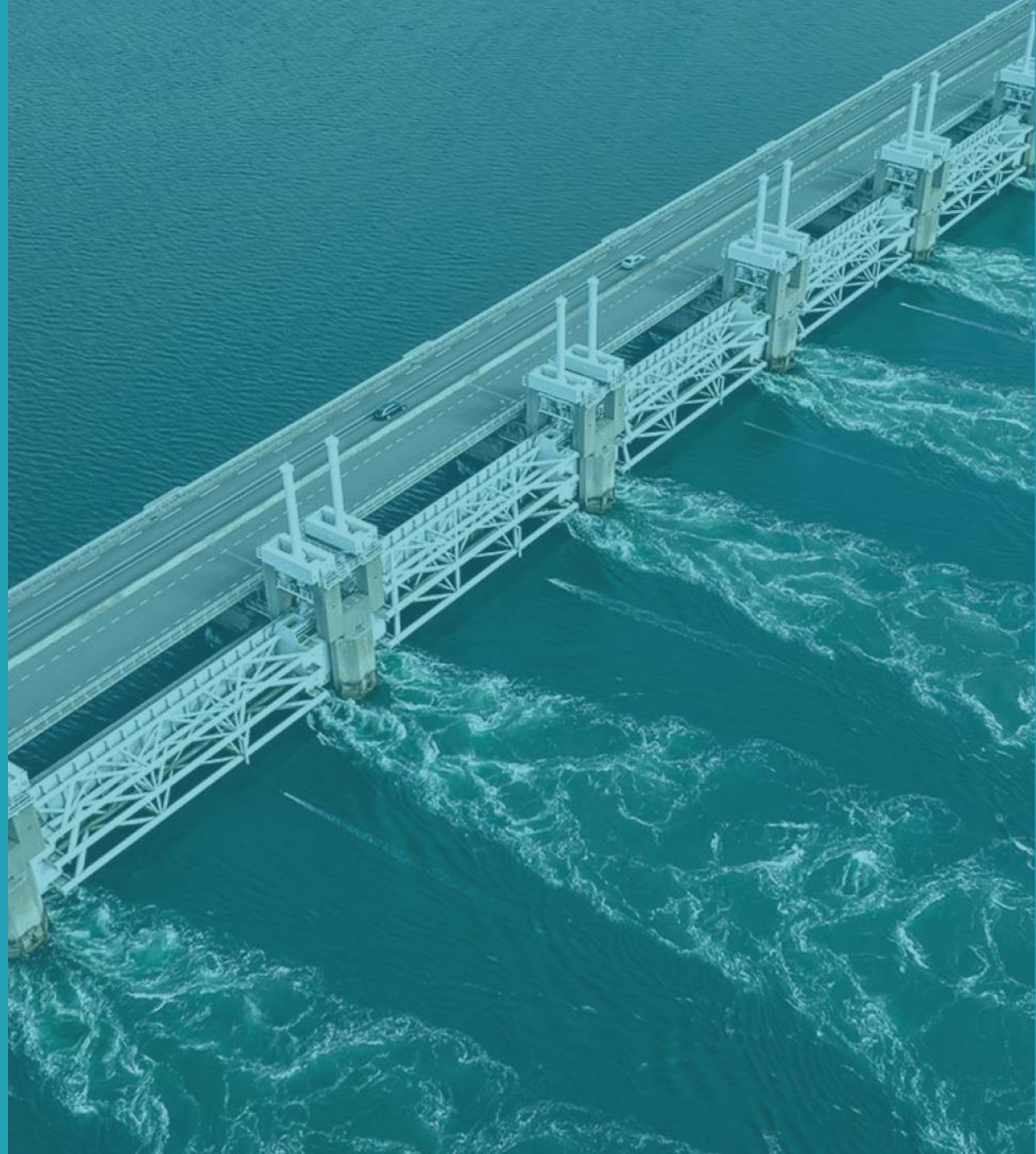


Largest DDoS Trend shift 2025

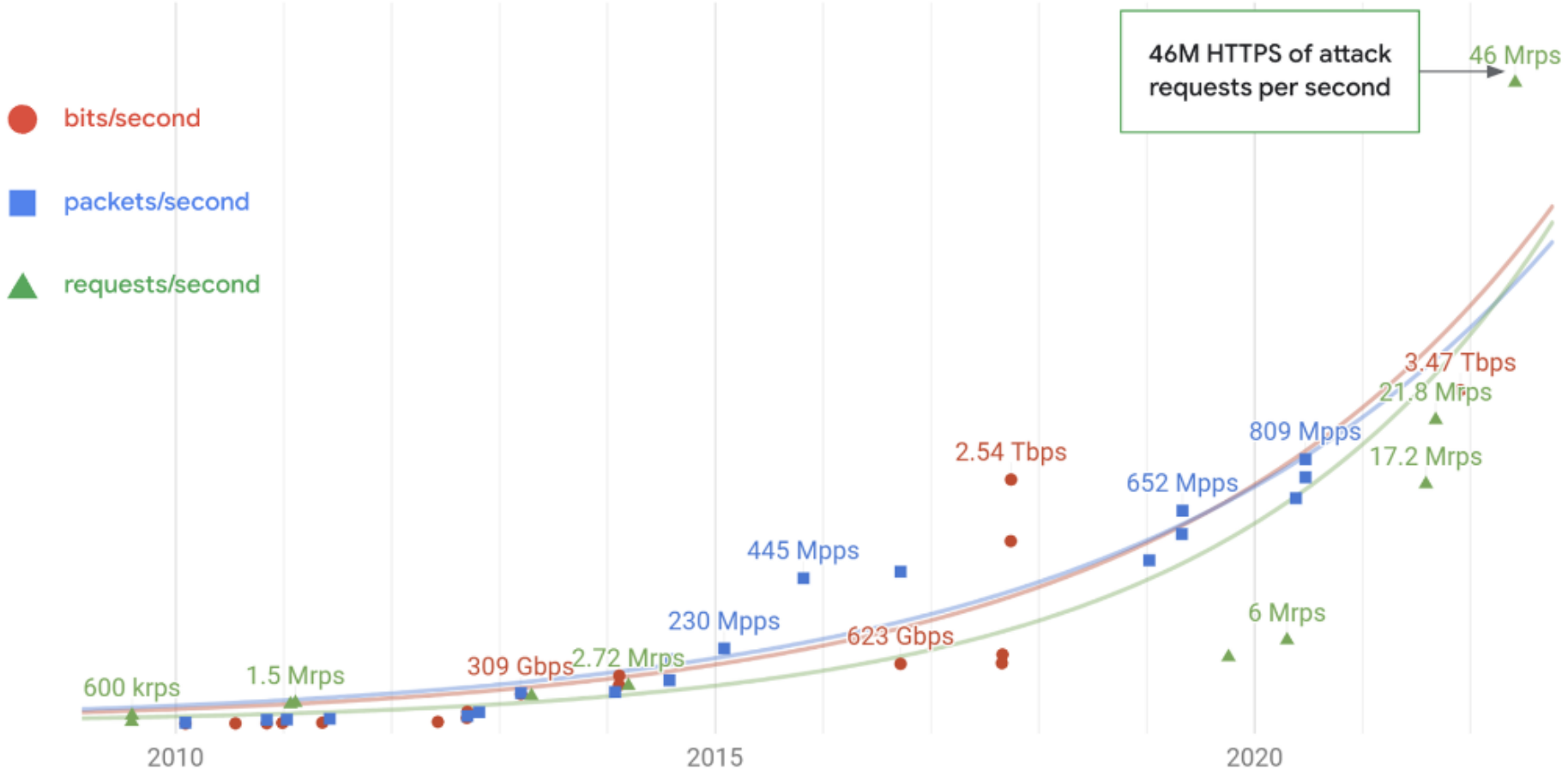


DDoS Data

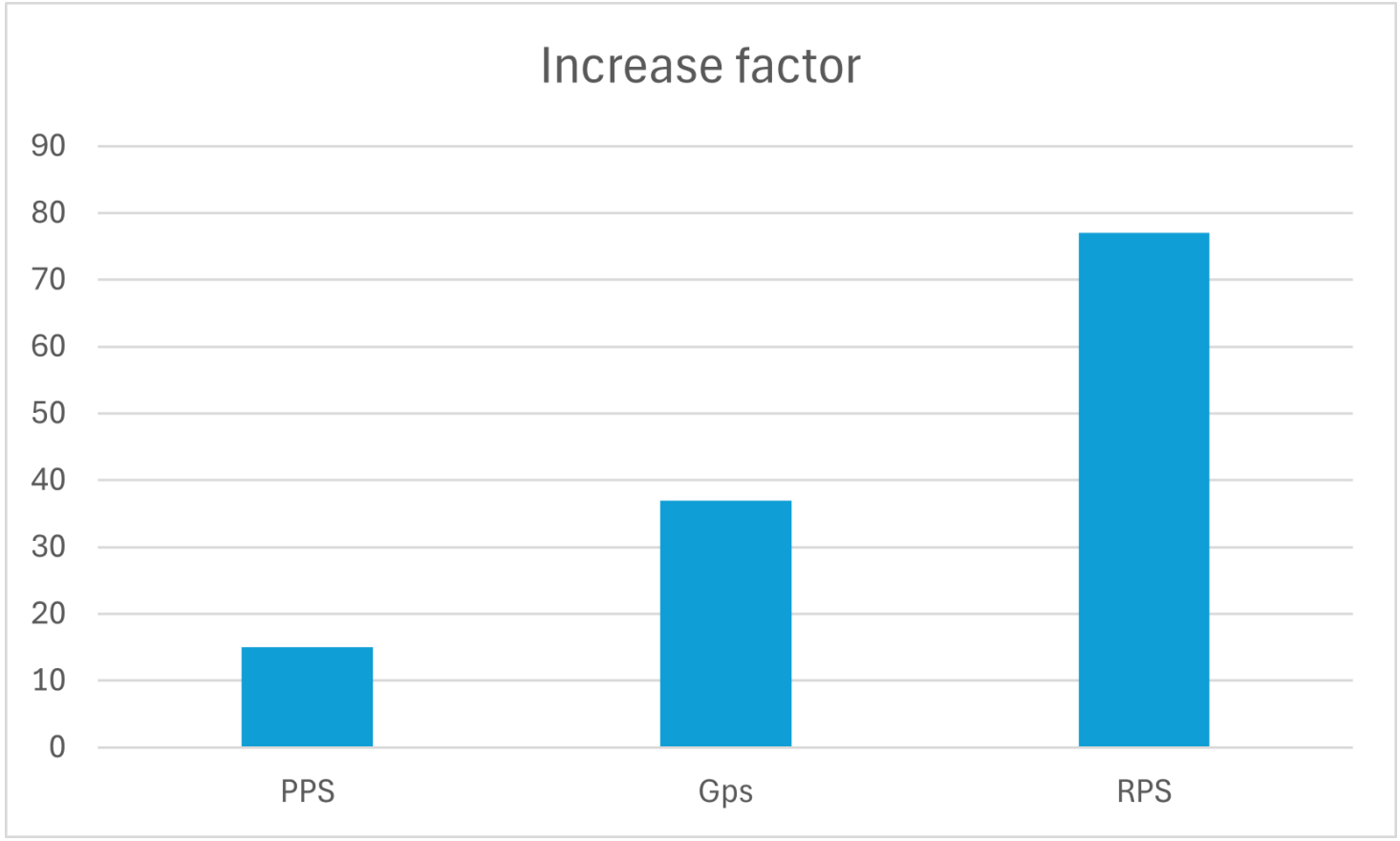
- Trends 2025
- Scary Metrics



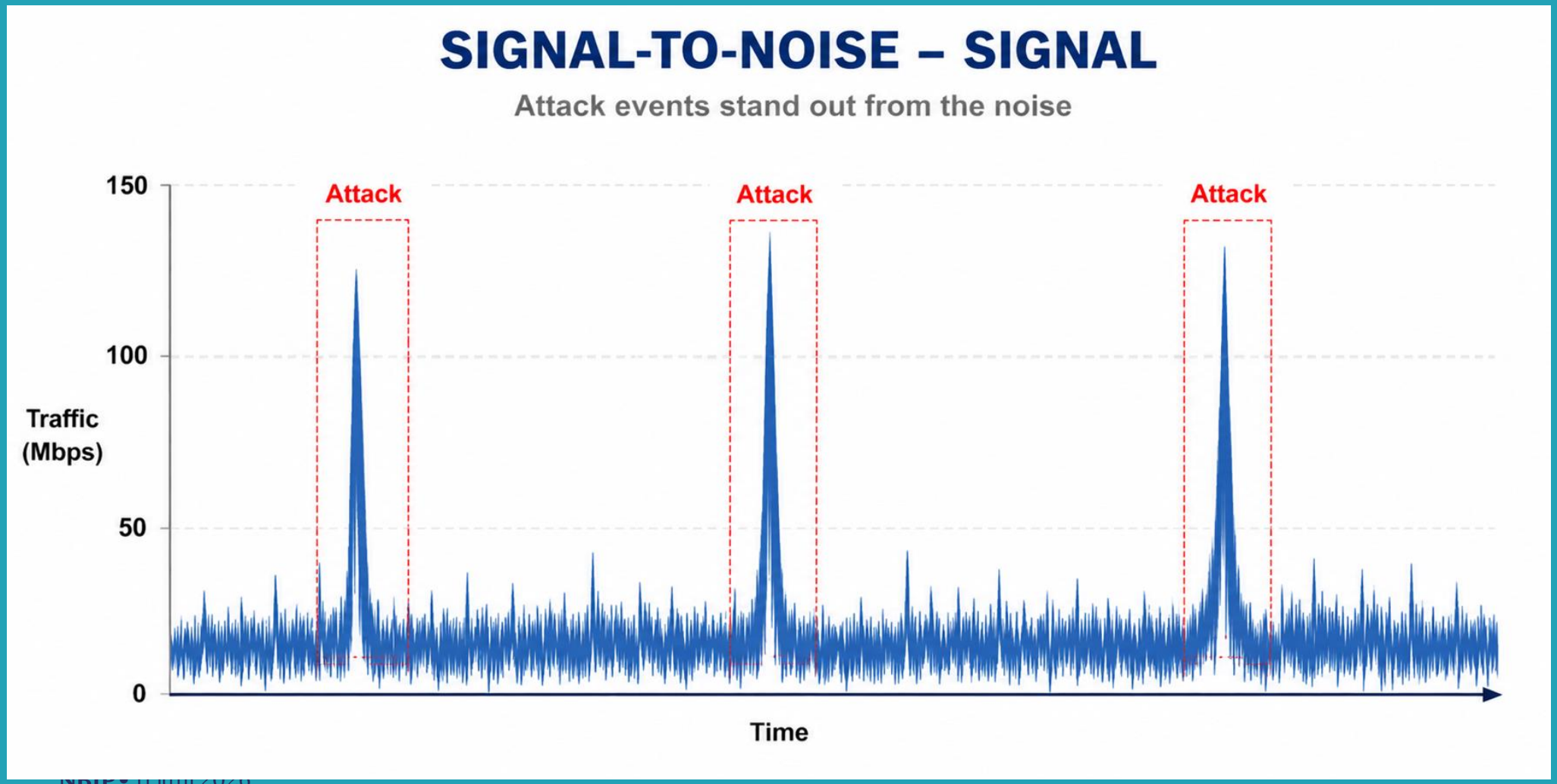
Scary Metrics



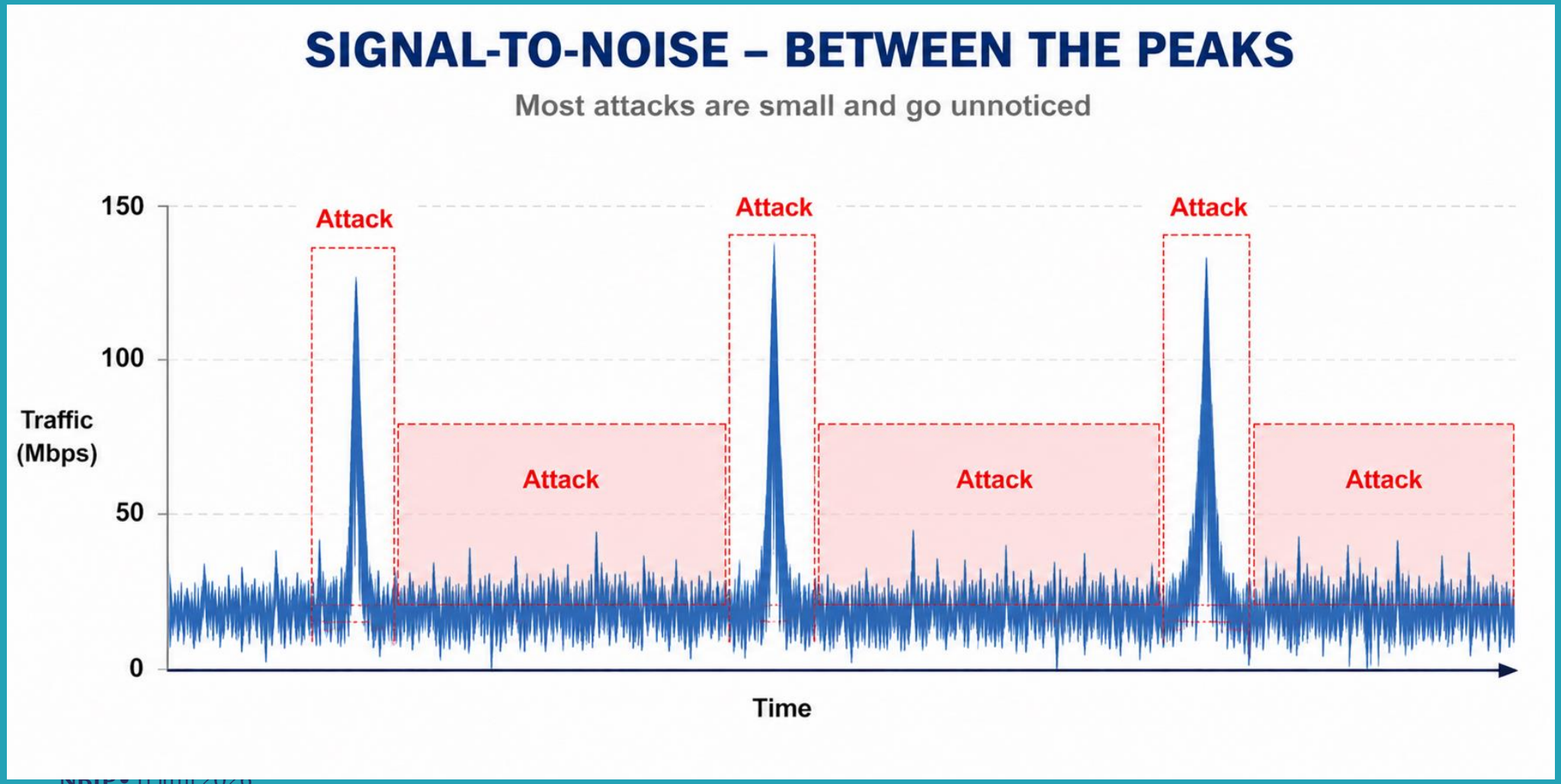
Scary Metrics



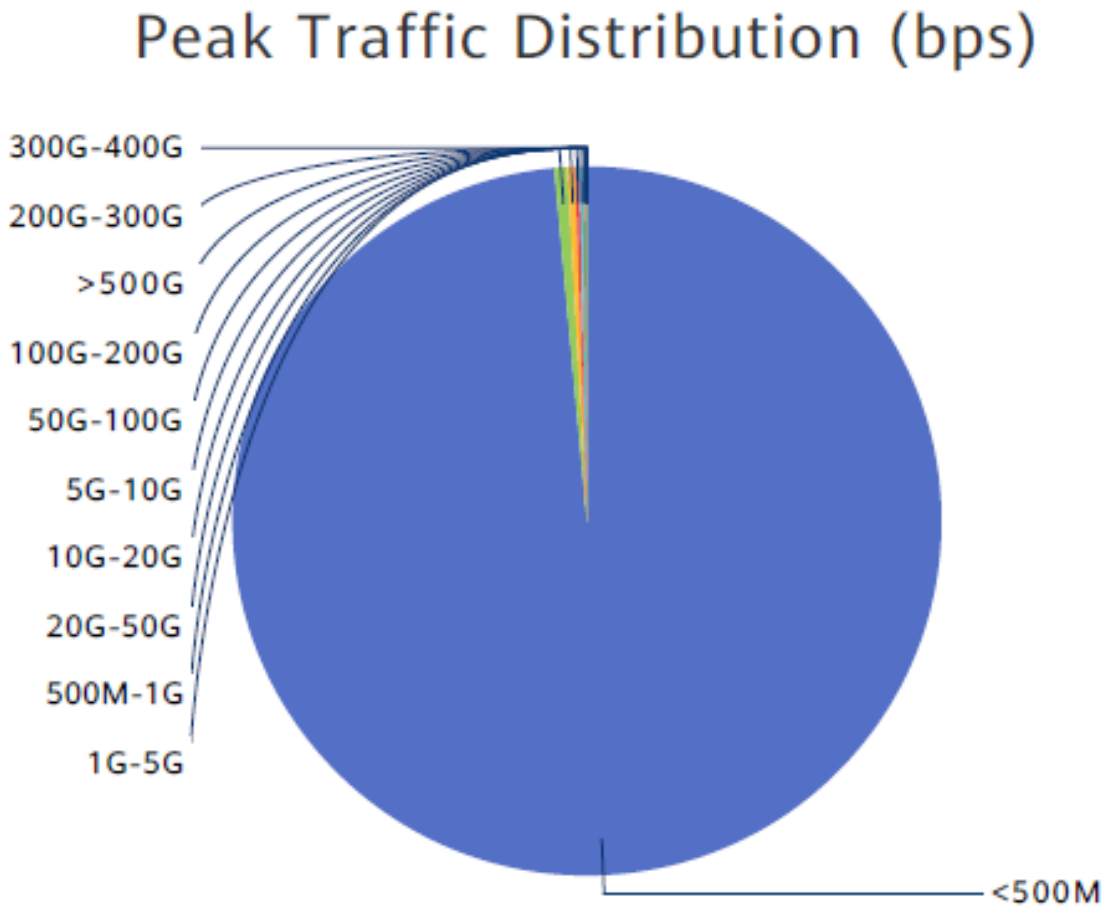
Signal


SIGNAL-TO-NOISE – SIGNAL
Attack events stand out from the noise
150
100
50
0
Traffic (Mbps)
Attack
Attack
Attack
Time

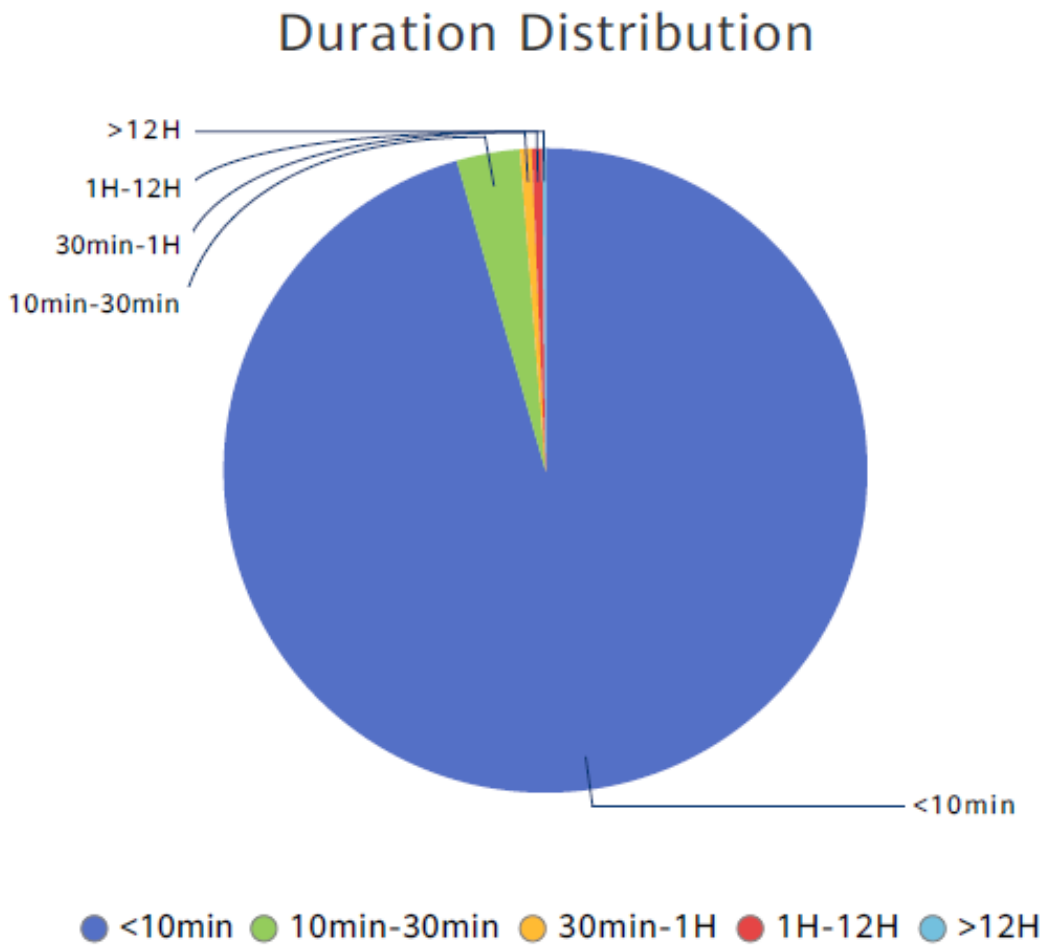
Noise


SIGNAL-TO-NOISE – BETWEEN THE PEAKS
Most attacks are small and go unnoticed
150
100
50
0
Traffic (Mbps)
Attack
Attack
Attack
Attack
Attack
Attack
Time

Attack Profiles



Attack Profiles

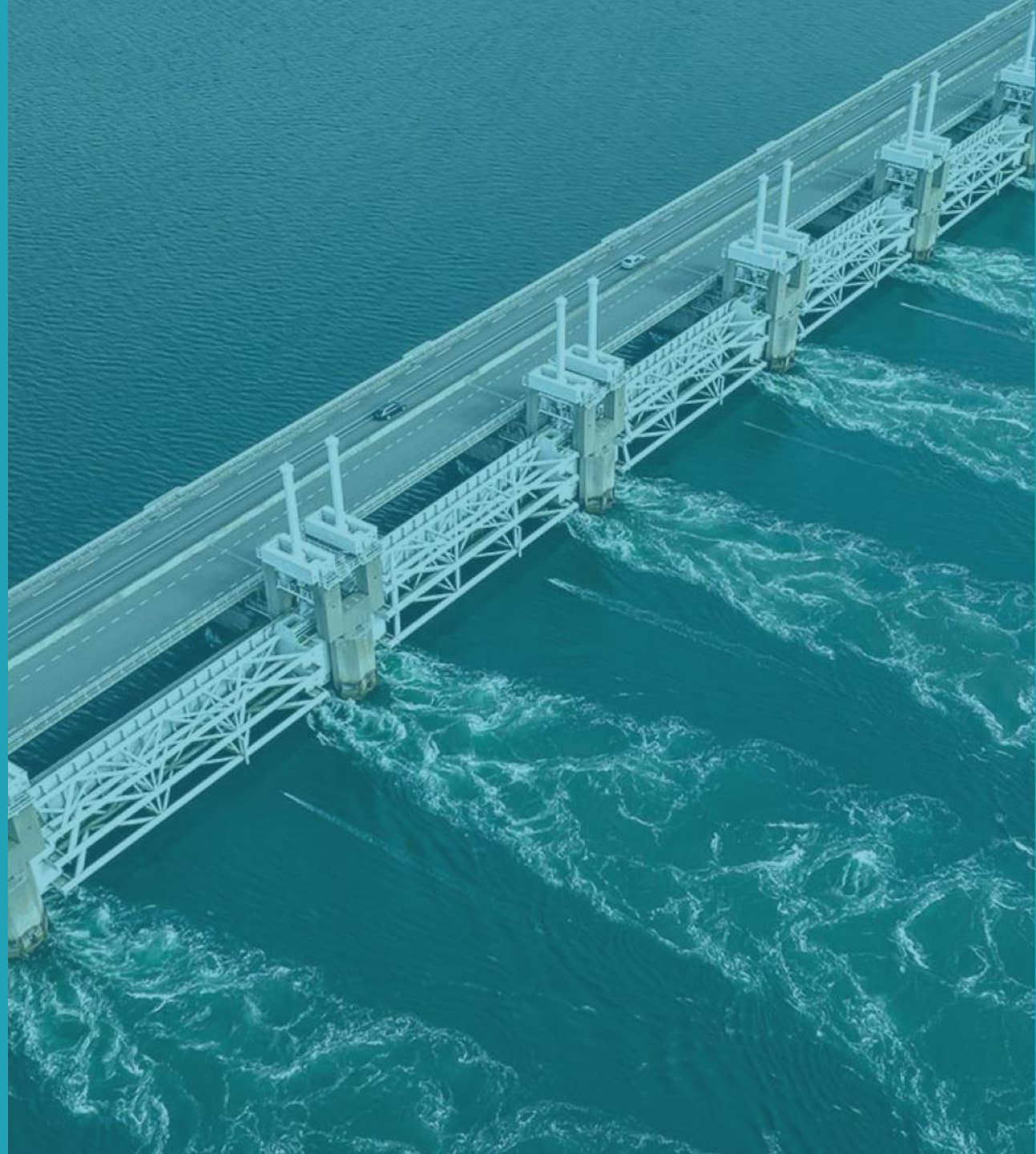


What will coming knocking at your door

Vector	8/10 attacks will be multi-vector
Split	7.5/10 attack vectors will be UDP based
Type	7/10 UDP based attacks include DNS Amp
Mbps	8.5/10 attacks will be <500 Mbps
PPS	8.5/10 attacks will be <100k PPS
Time	8.5/10 attacks will be <10 Min

DDoS Data

- Trends 2025
- Scary Metrics
- Protection



The acronym to live by

The 5 P’s - PPPPP

Proper

Preparation

Prevents

Prolonged

Pain

NOTE

- Pain is often not fully preventable
- Reduced performance should be considered
- Reduced accessibility should be considered
- Additional costing should be considered

How to prepare

Know your application

- Know your critical endpoints
- Know your peacetime traffic profile, intimately
- Know your applications architecture
- Know your application IP Space

Example

The bad

Requesting a Geoblock for a /23.

Spoiler alert – this broke other things

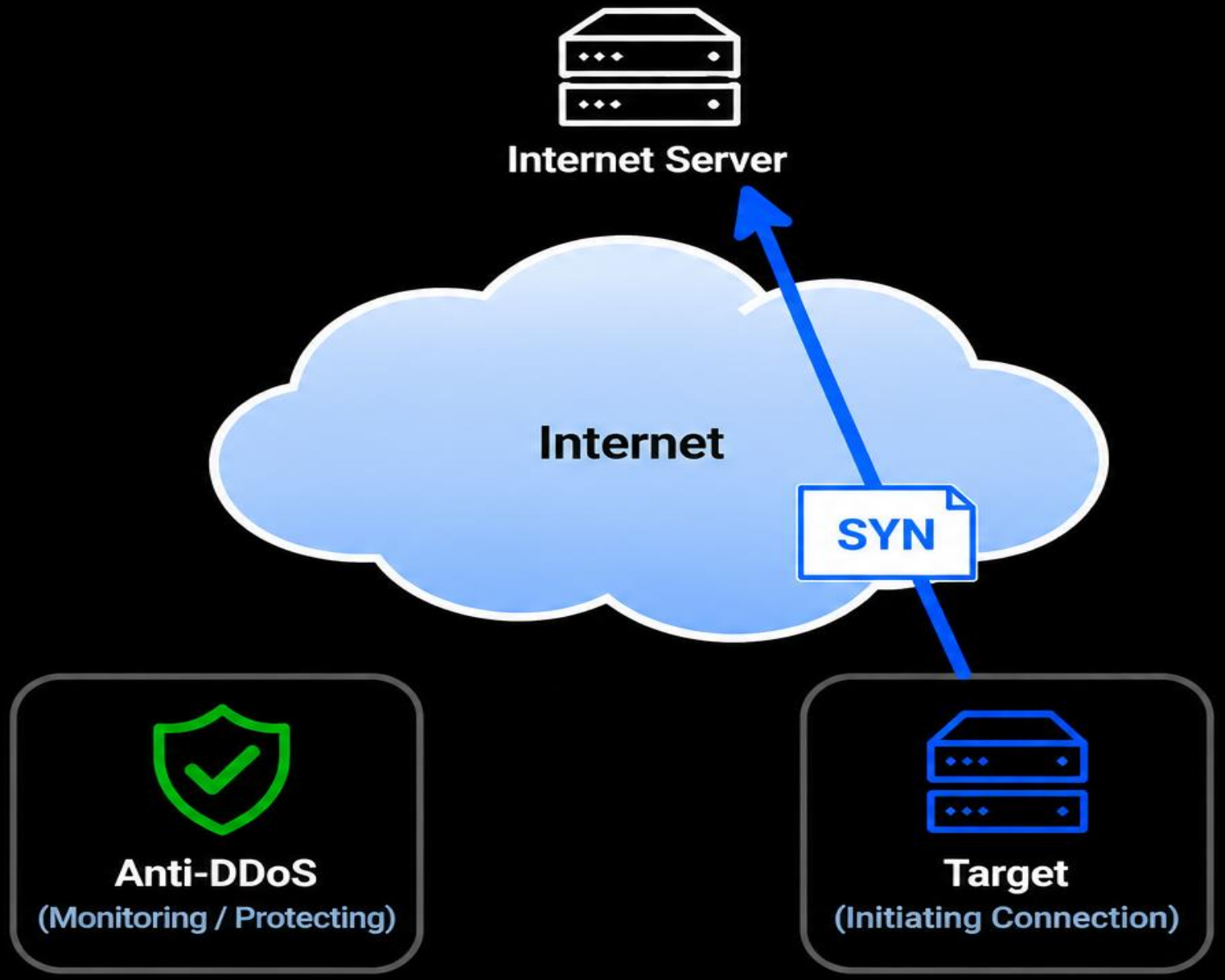
Example

The bad

- Which services use which endpoints
- Anycast traffic
- What about cloud services
- What about proxied requests
- What about outbound requests

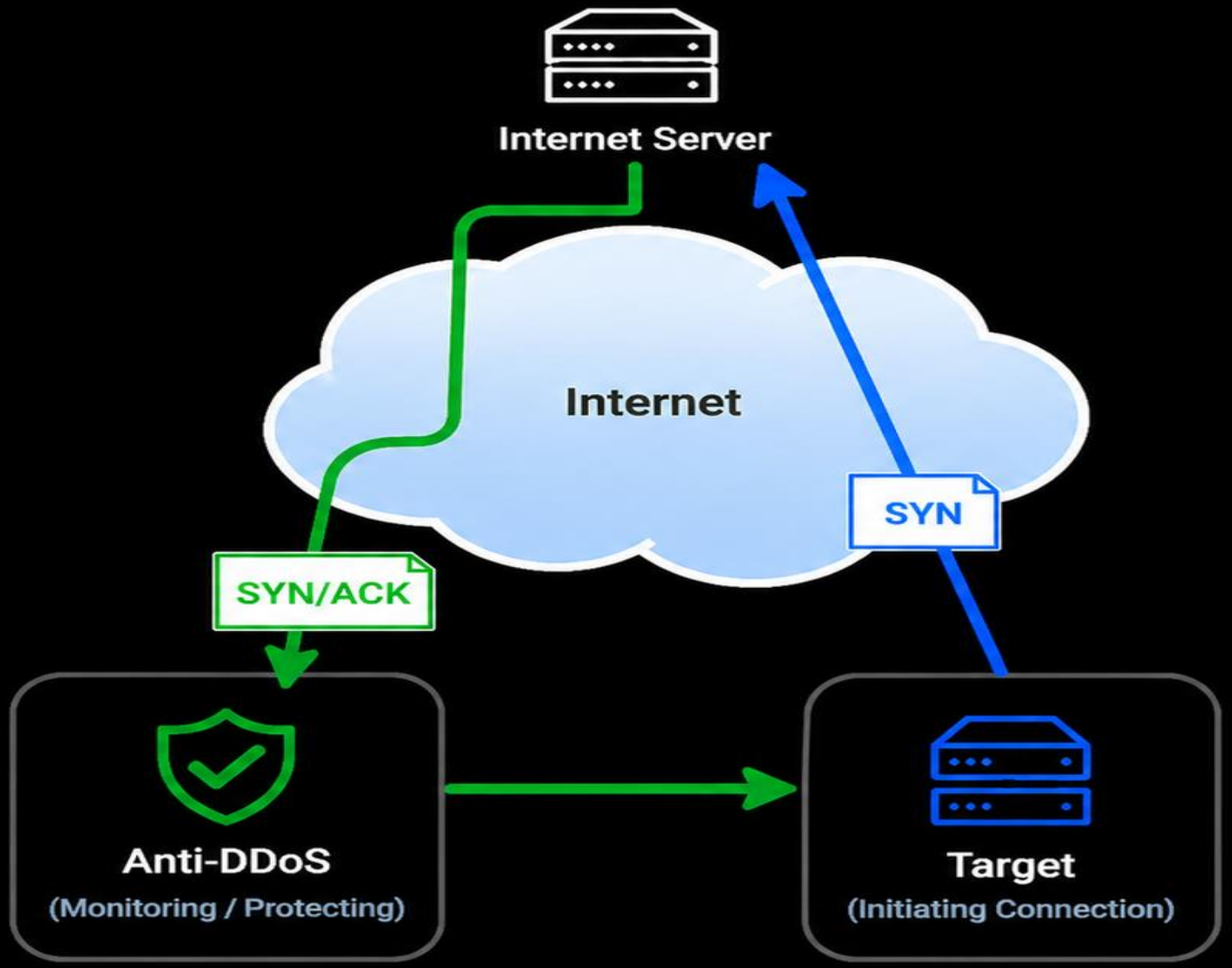
1 Normal TCP Session Initiation

Target initiates an outbound connection.



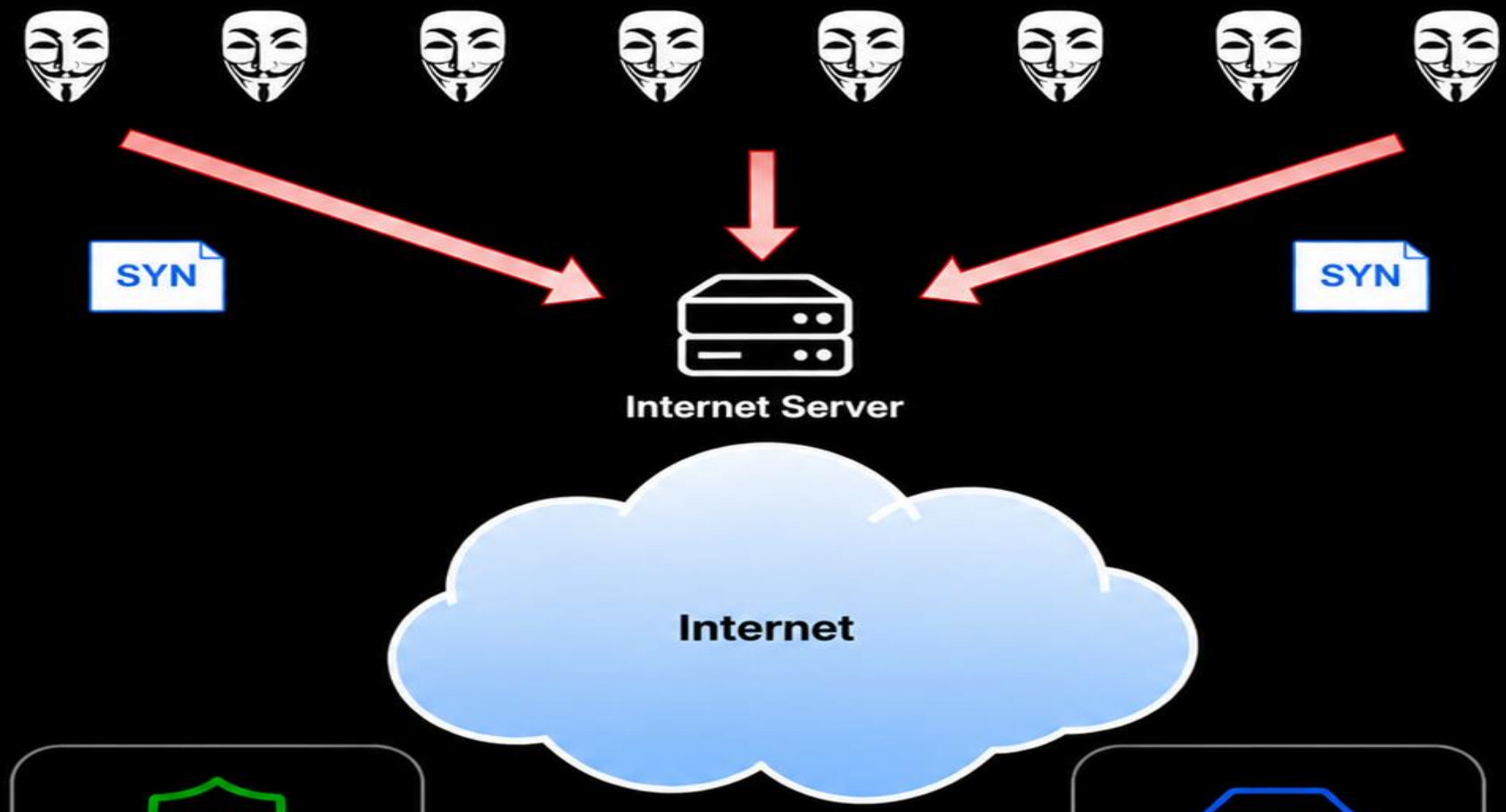
2 Normal TCP Handshake – Response

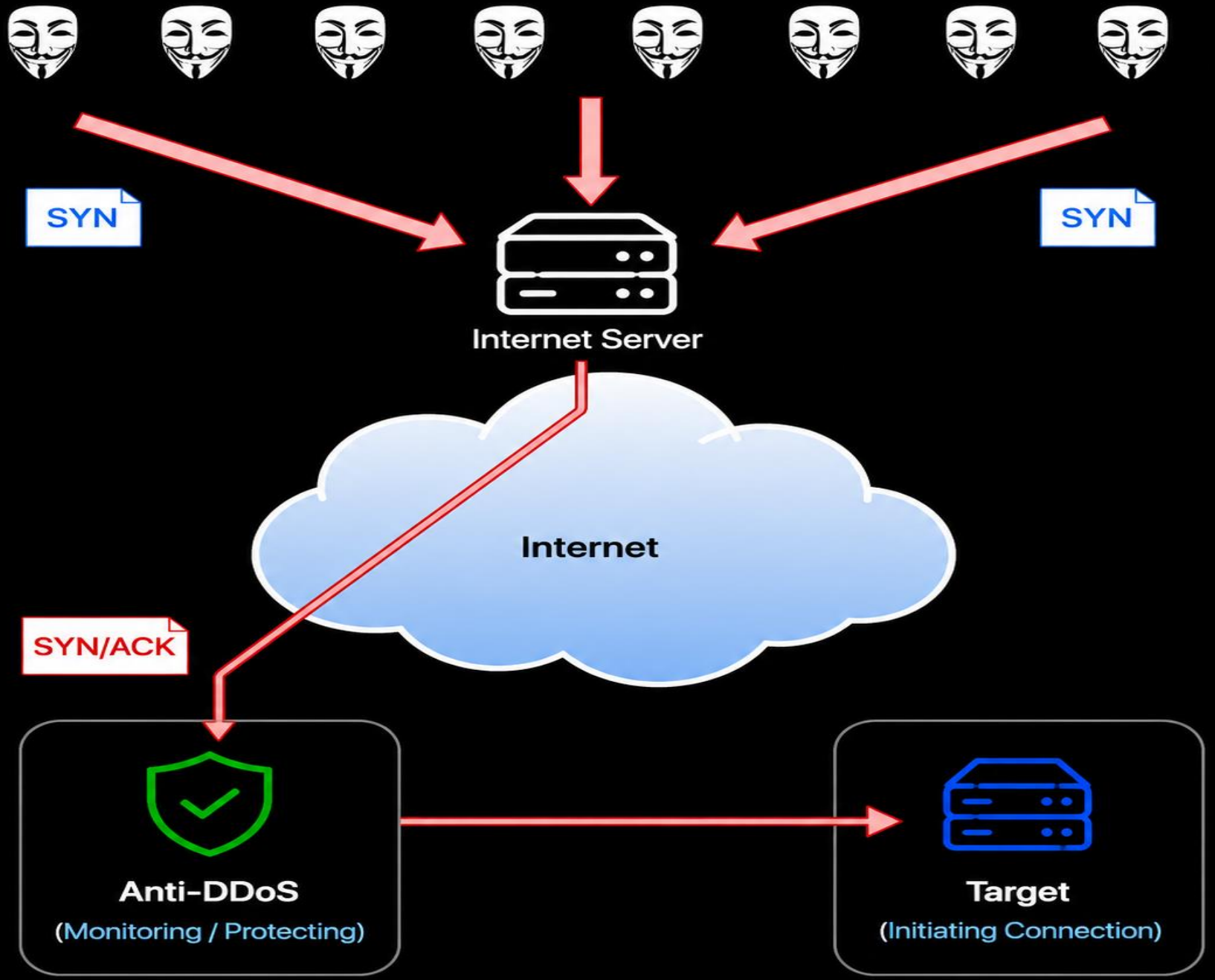
The server responds with SYN/ACK via the Anti-DDoS.



3 TCP Reflection Attack – Amplification

Attackers spoof the target's IP and send SYN packets.

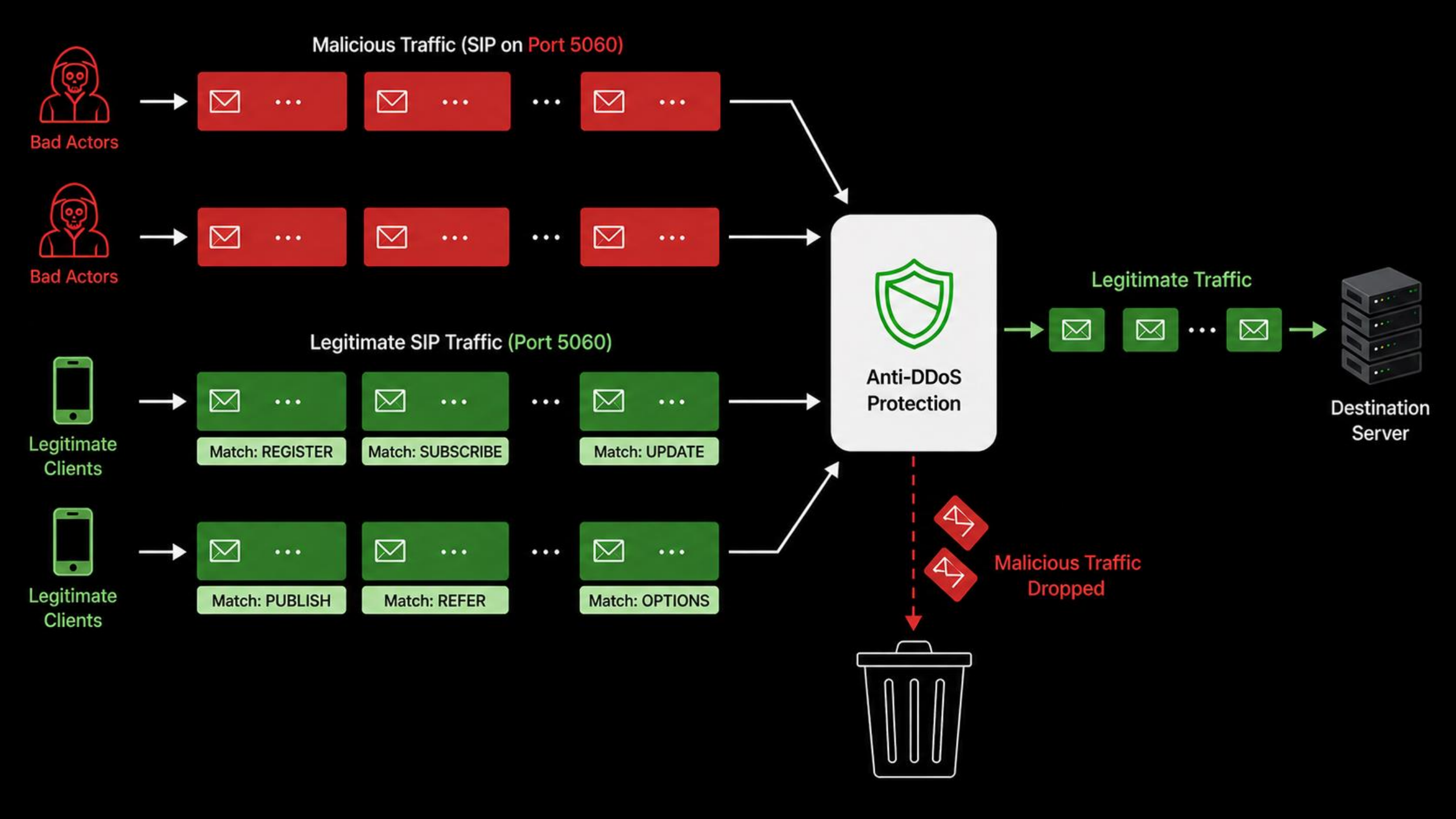



SYN
SYN
Internet Server
Internet
SYN/ACK
Anti-DDoS
(Monitoring / Protecting)
Target
(Initiating Connection)

Example

The good

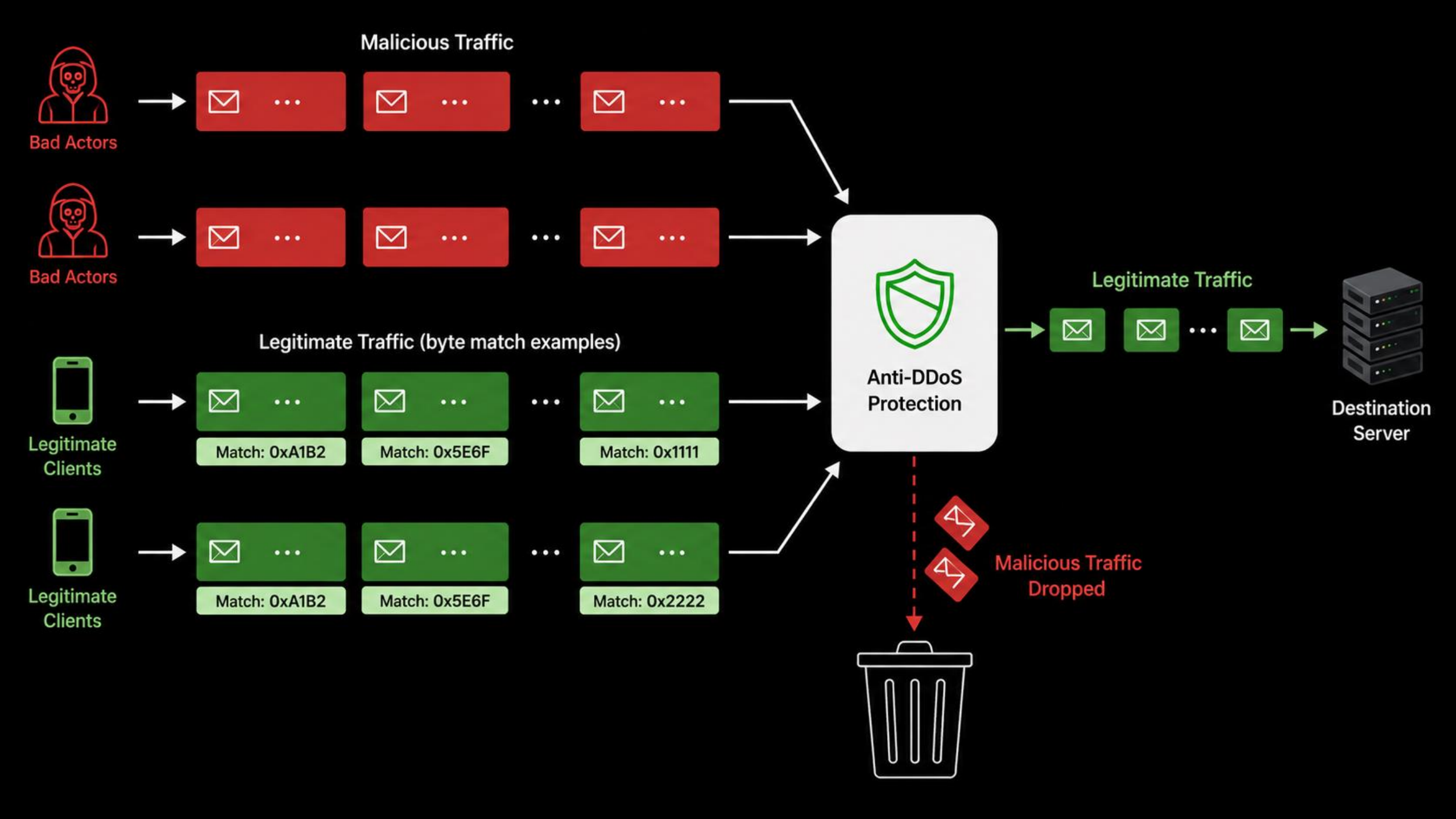
- Exact traffic profile and ratio’s
- Service endpoint IPs
- Packet sizes (based on codecs)
- Fragmented packet sizes
- Instant feedback on policy deployments
- Outbound connections


Malicious Traffic (SIP on Port 5060)
Bad Actors
Bad Actors
Legitimate SIP Traffic (Port 5060)
Legitimate Clients
Match: REGISTER
Match: SUBSCRIBE
Match: UPDATE
Legitimate Clients
Match: PUBLISH
Match: REFER
Match: OPTIONS
Anti-DDoS Protection
Legitimate Traffic
Destination Server
Malicious Traffic Dropped

Example

The great

- UDP Application
- Customer owns the client application
- Provides byte matches in advance

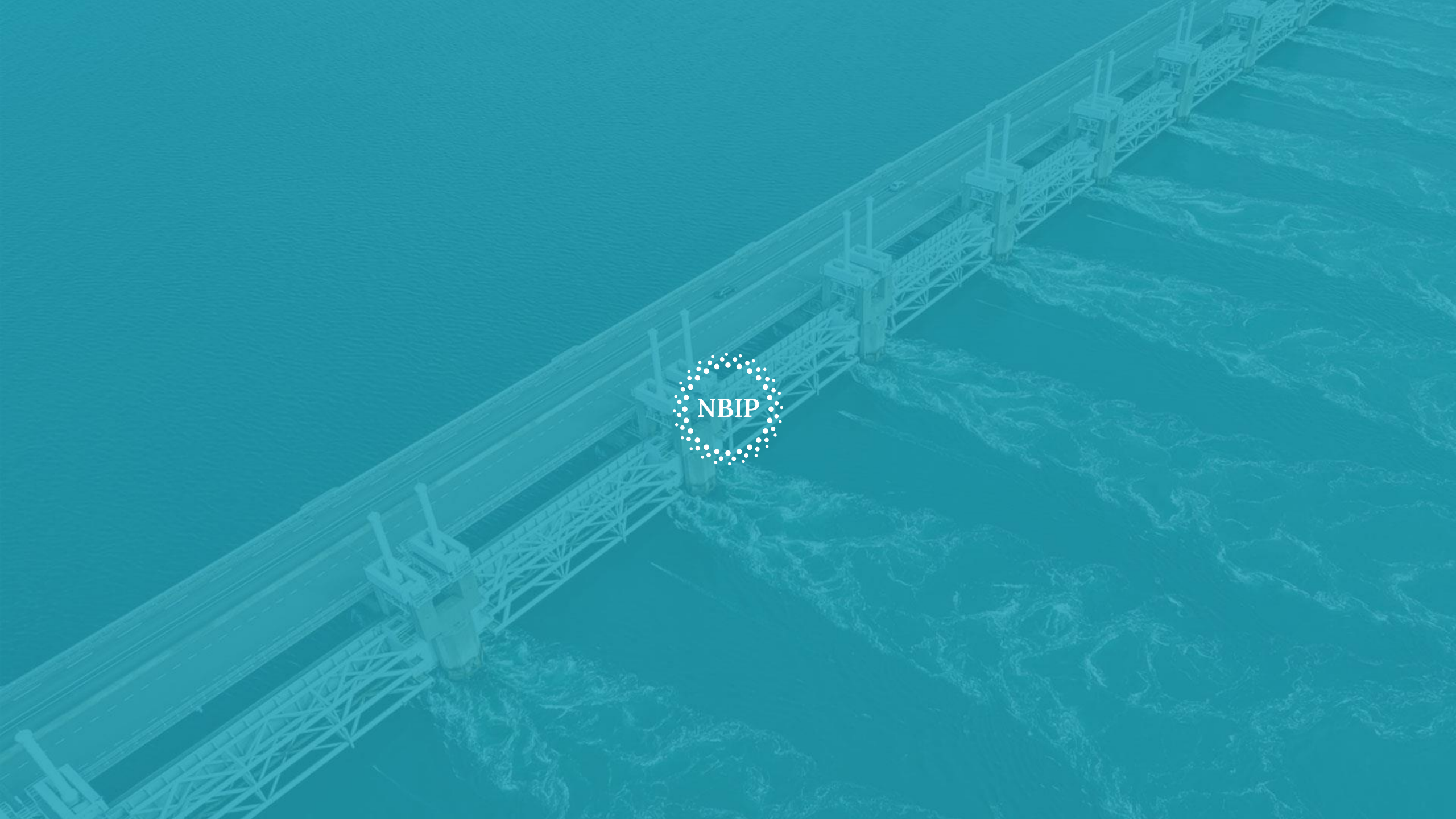

Malicious Traffic
Bad Actors
Bad Actors
Legitimate Traffic (byte match examples)
Legitimate Clients
Match: 0xA1B2
Match: 0x5E6F
Match: 0x1111
Legitimate Clients
Match: 0xA1B2
Match: 0x5E6F
Match: 0x2222
Anti-DDoS Protection
Legitimate Traffic
Destination Server
Malicious Traffic Dropped

How to prepare

Break glass incase of emergency

- DNS Flexibility (TTL strategy)
- Prepared and maintained “last-resort” workflow
- Pre-documented policies and workflows (WAF/Anti-DDoS/etc)
- Define the win

Questions?


NBIP