ARBOR NETWORKS

MASTERLINE

10 Years of DDoS Attacks

in the data of Arbor Networks' Infrastructure Security Report and ATLAS

Marco Gioanola, Senior Consulting Engineer

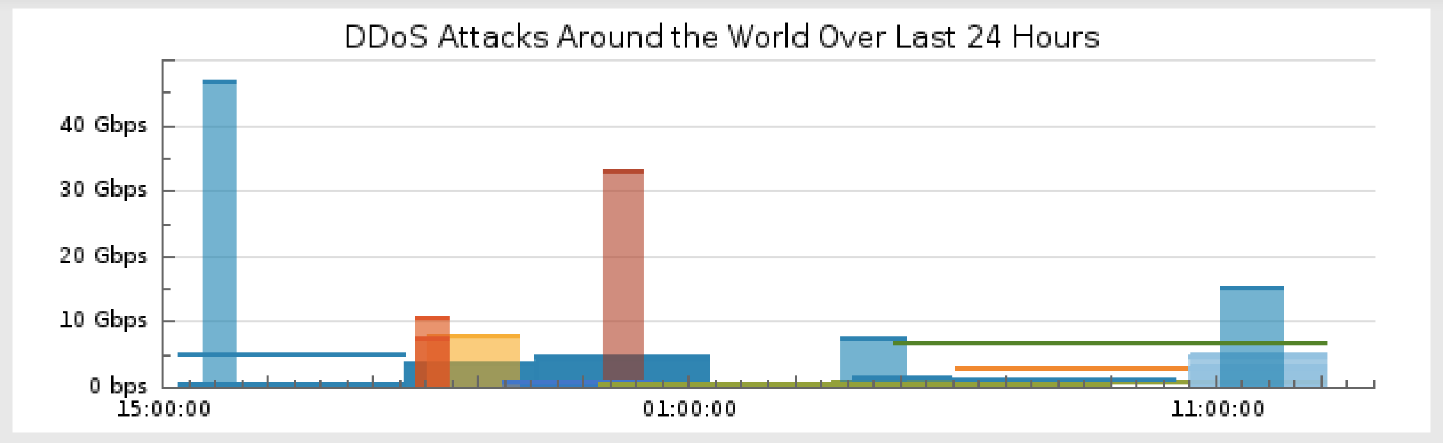
Ljubljana, April 1st 2015

The speaker

- DDoS mitigation projects since 2004
- Background in public key infrastructures
- Managed security services
- With Arbor Networks since 2006
  - the global leader in anti-DDoS market
  - Italy, Slovenia, Croatia, Balkans, Greece, Cyprus, Malta, Turkey, Arabic Gulf, Pakistan...
  - Subject Matter Expert for Arbor Cloud

The data

- **Worldwide Infrastructure Security Report**
  - Ten years of surveying the operational security community on threats, concerns, mitigation/detection strategies and technologies.
  - 287 respondents in 2014, 180 questions each. (Thank you!)
- **ATLAS**
  - Statistical data anonymously shared by Internet Service Provider customers
  - 400 ISPs partecipating
  - >120 Tbps of aggregate traffic monitored

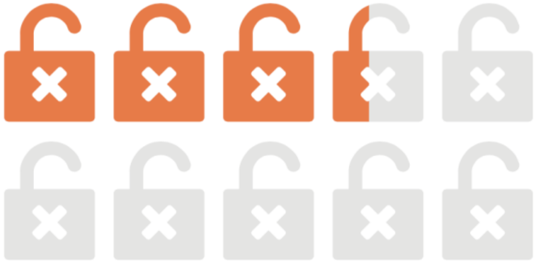


WISR 2014 Key Findings

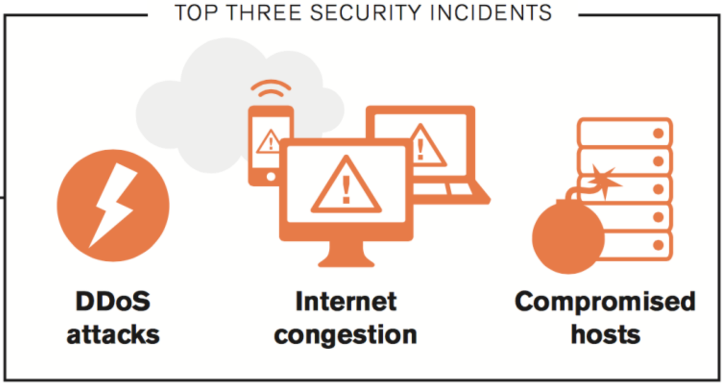
IPv6	• **Traffic growing strongly, but still not significant** • Nearly three-quarters of service providers now have some customers utilizing IPv6 services
Data Center	• Big increase in those seeing revenue loss due to DDoS • **Almost two thirds reported DDoS attacks, 33% see attacks exceed total Internet bandwidth** • Big rises in use of IDMS and ACLs
DNS	• **Worrying trend indicating a decrease in focus on DNS security** • Lower number of respondents see customer visible outages
Security Practices	• Most respondents have dedicated resources, but hiring / retaining still an issue • Concerning reductions in anti-spoofing and DDoS incident rehearsal
Mobile	• LTE being pervasively deployed • Fewer respondents see customer visible outage due to a security incident • Attacks targeting mobile infrastructure up, but down against Gi / SGi

ARBOR® NETWORKS

Enterprise Incident Response (WISR)



34% of respondents indicate an **increase in security incidents** this year

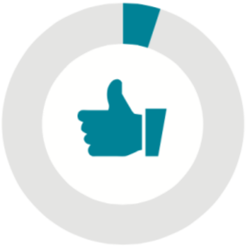


TOP THREE SECURITY INCIDENTS

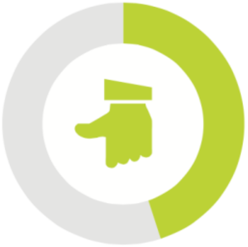
DDoS attacks

Internet congestion

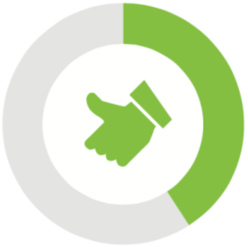
Compromised hosts



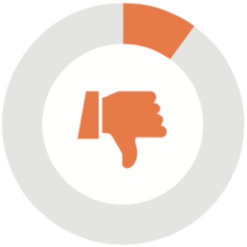
5% of respondents feel **fully prepared** to handle these incidents



45% of respondents feel **somewhat prepared** to handle these incidents

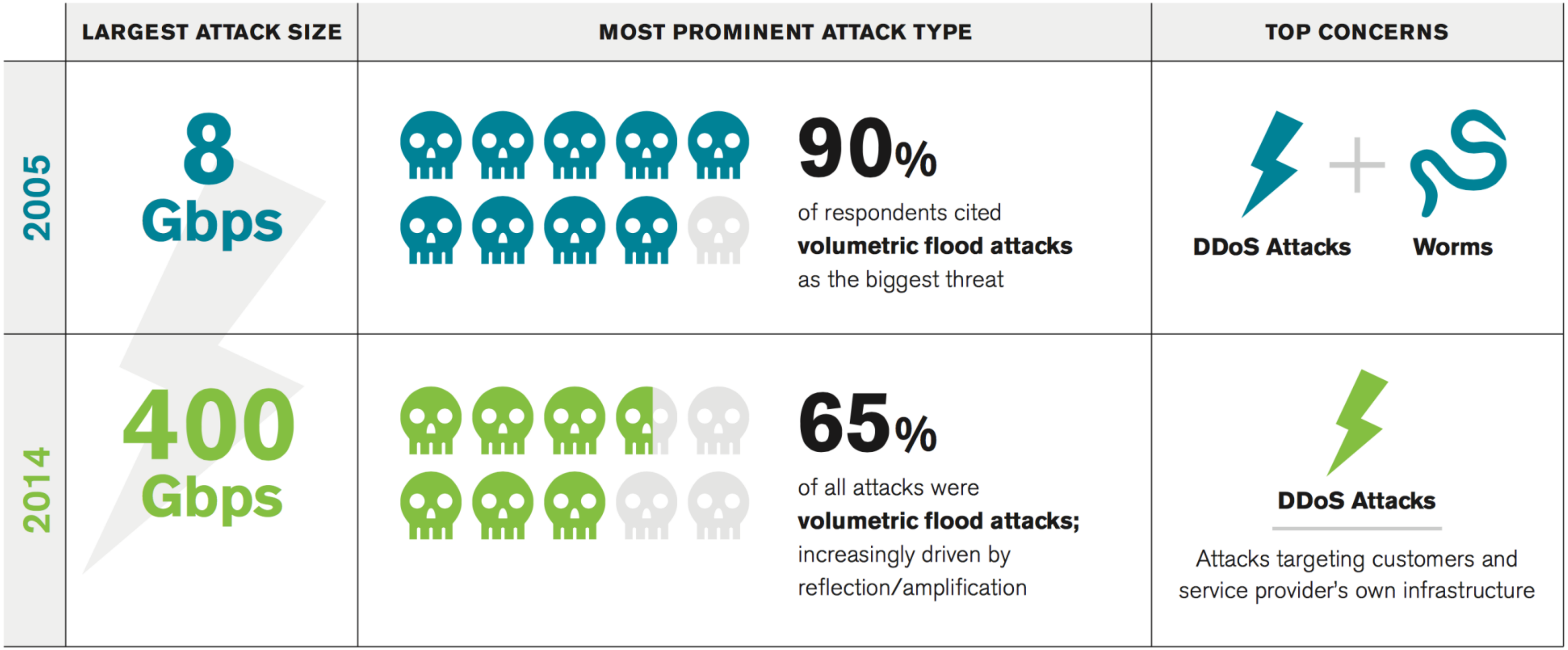


41% of respondents feel **reasonably prepared** to handle these incidents



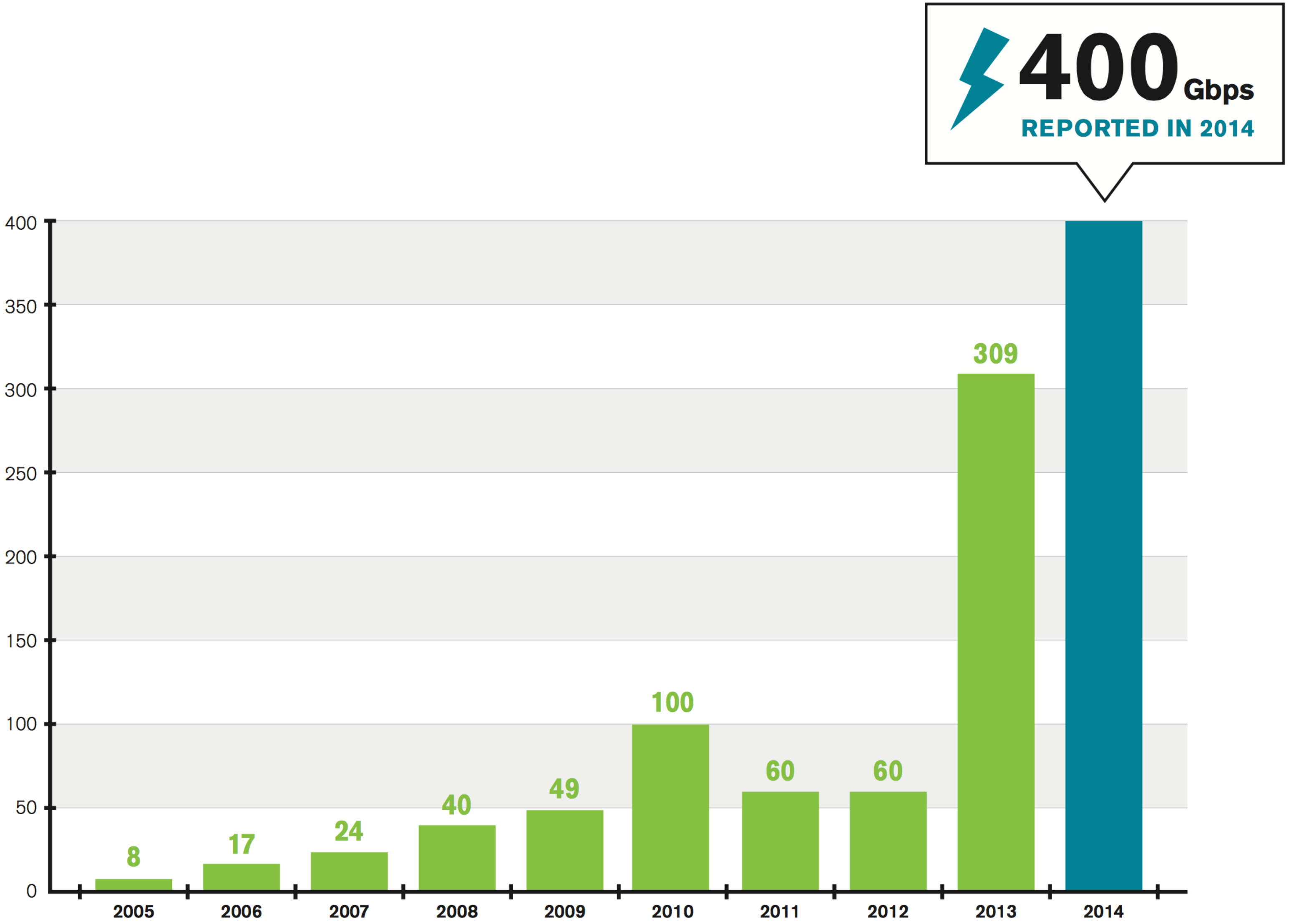
10% of respondents feel **completely unprepared** to handle these incidents

DDoS 2005 vs 2014 (WISR)

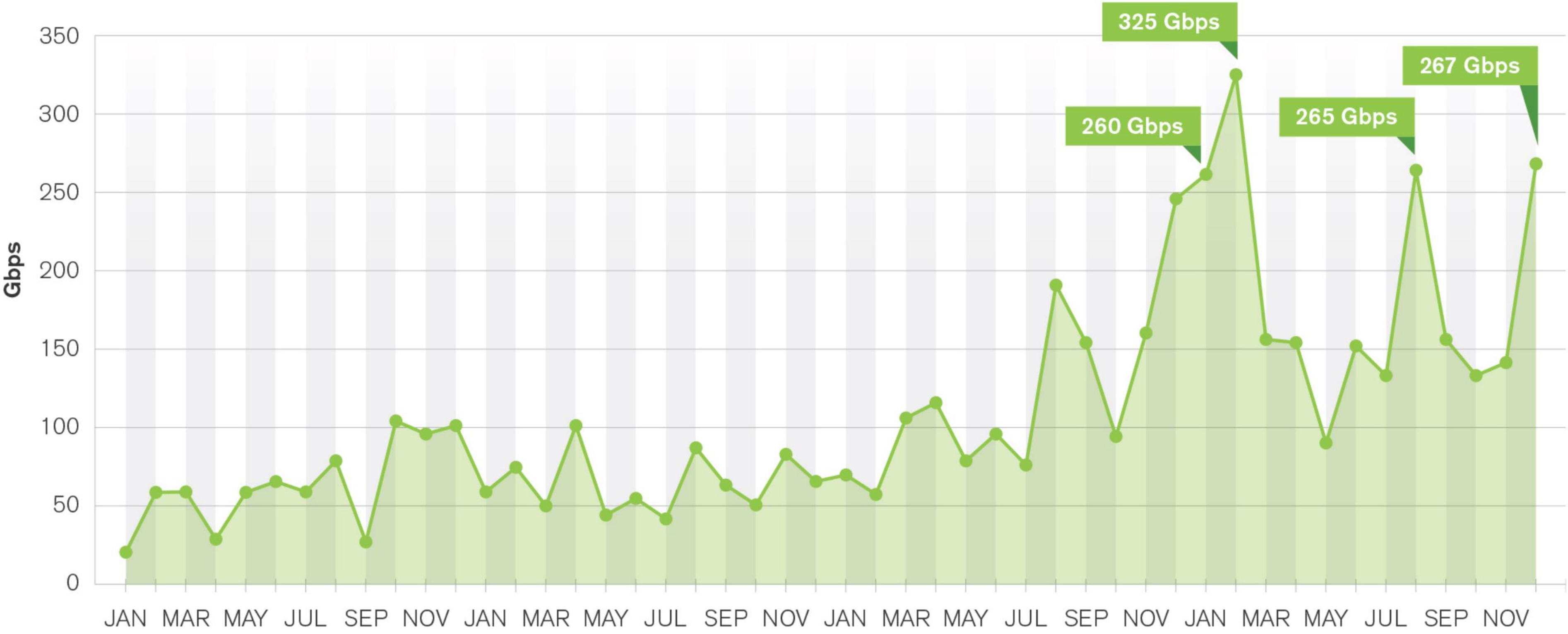


	LARGEST ATTACK SIZE	MOST PROMINENT ATTACK TYPE	TOP CONCERNS
2005	8 Gbps	90% of respondents cited **volumetric flood attacks** as the biggest threat	DDoS Attacks + Worms
2014	400 Gbps	65% of all attacks were **volumetric flood attacks;** increasingly driven by reflection/amplification	DDoS Attacks Attacks targeting customers and service provider's own infrastructure

Largest DDoS Attacks (WISR)

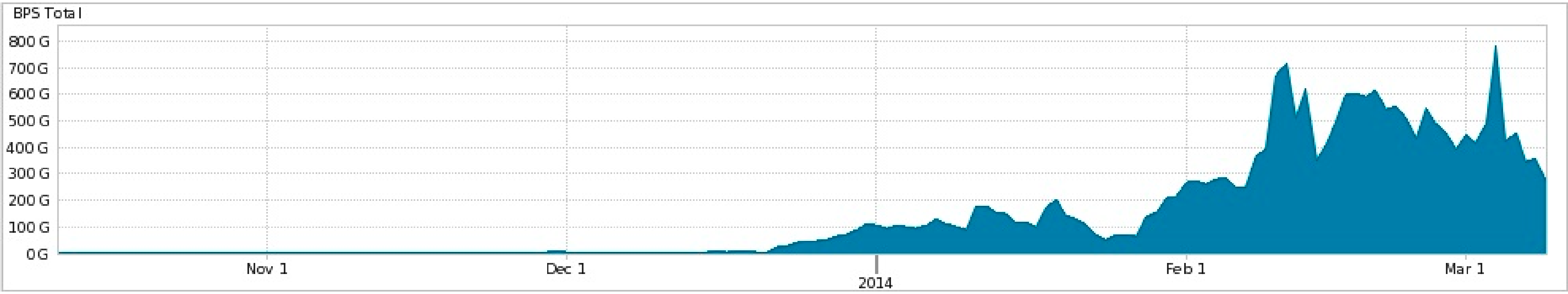


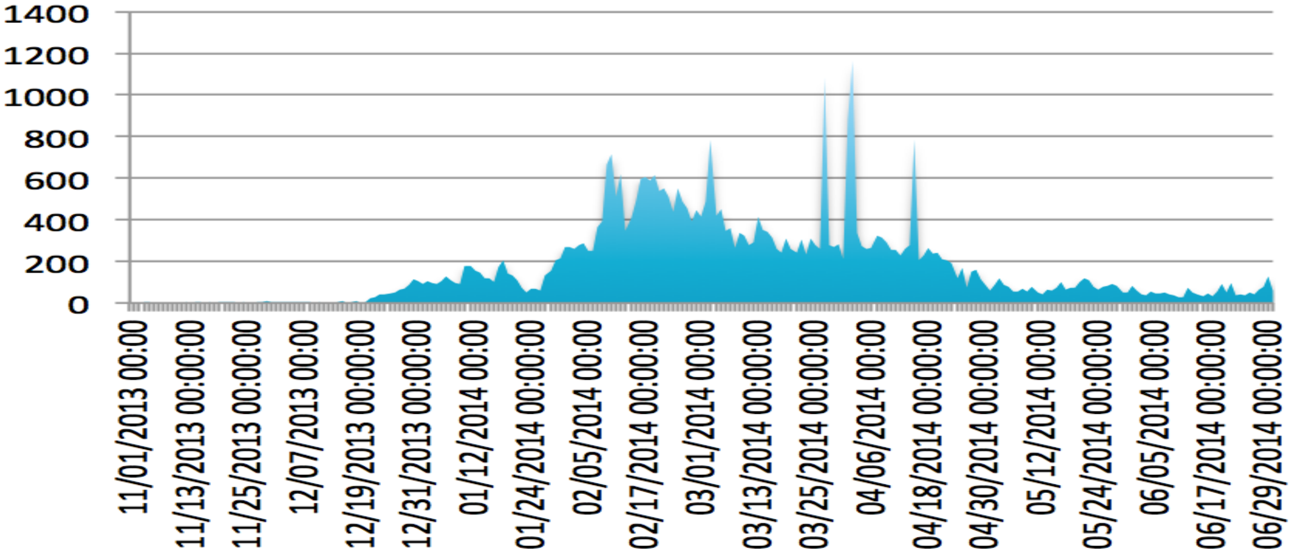
ATLAS Peak Attack Sizes 2011-2014



2014 as seen through ATLAS

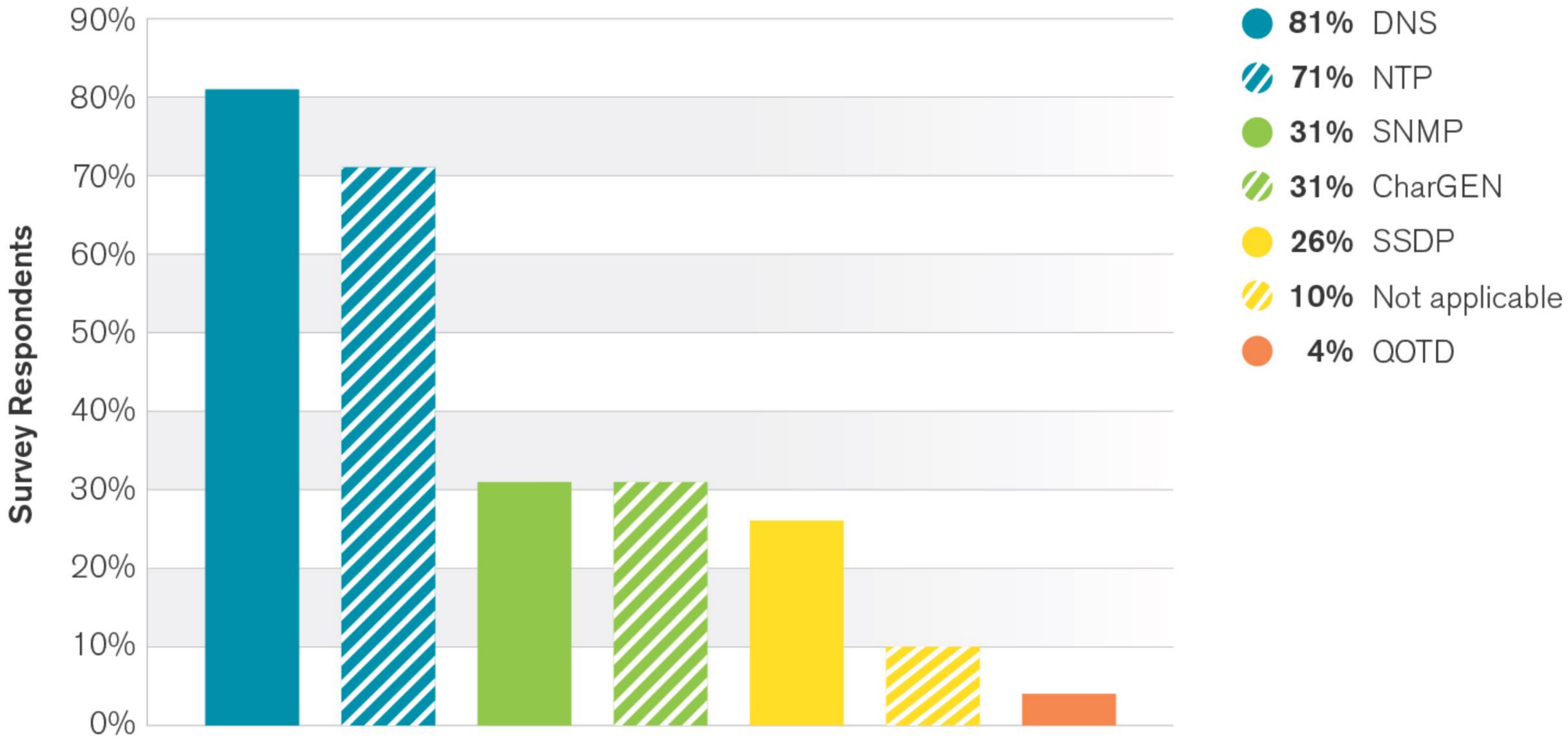
- “The year of reflection”
  – NTP monlist





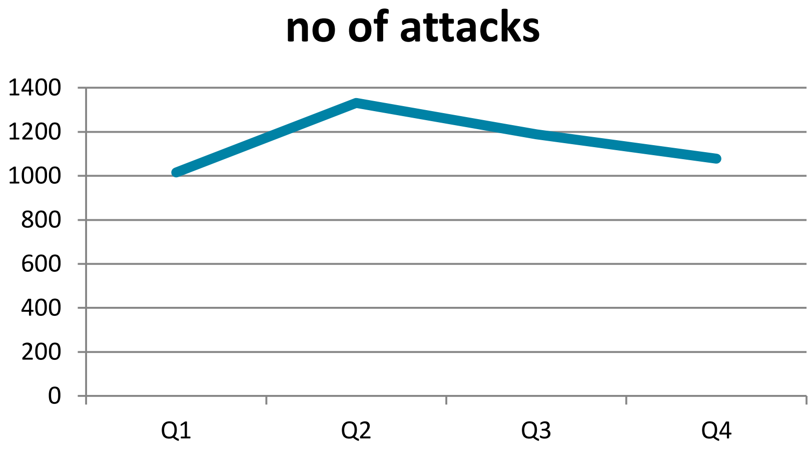
ARBOR NETWORKS

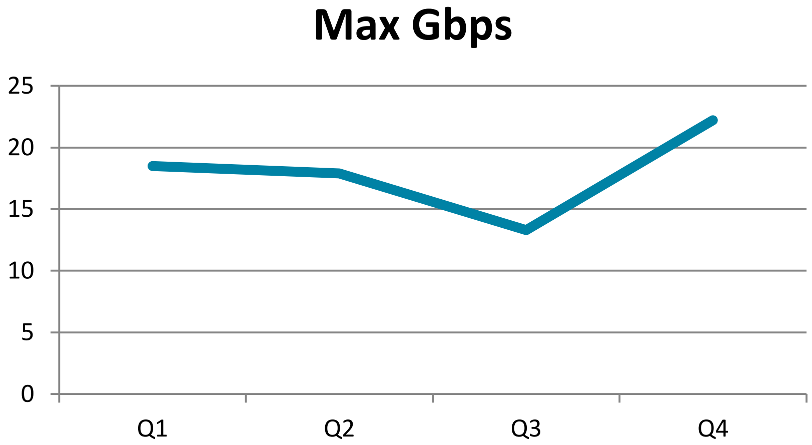
Protocols used for Reflection/Amplification (WISR)

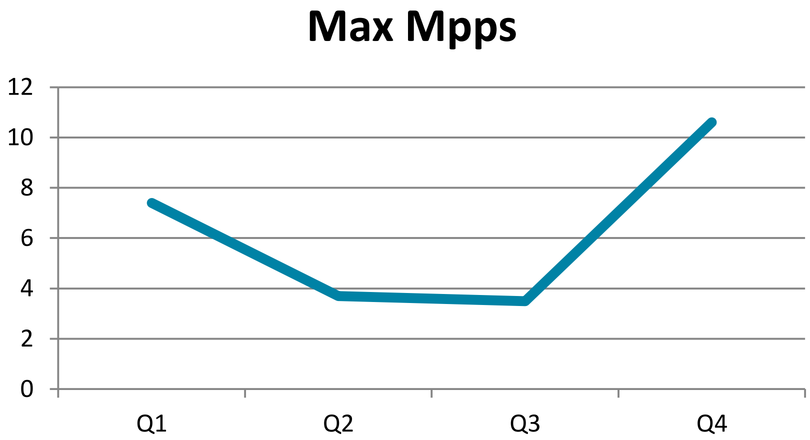


- Compromised / misconfigured CPEs still causing a lot of trouble. ISPs must act!

Slovenia, 2014 as seen through ATLAS

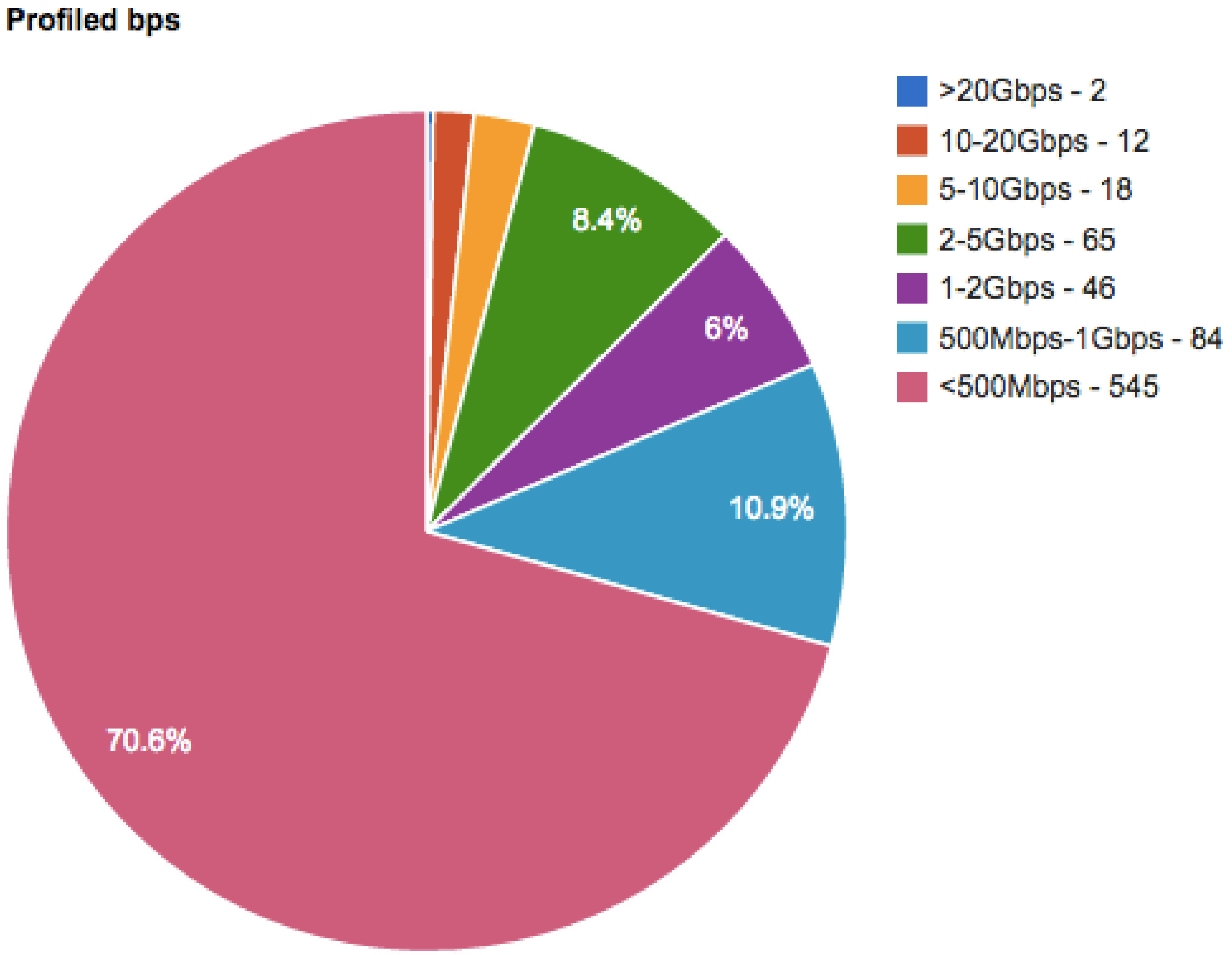






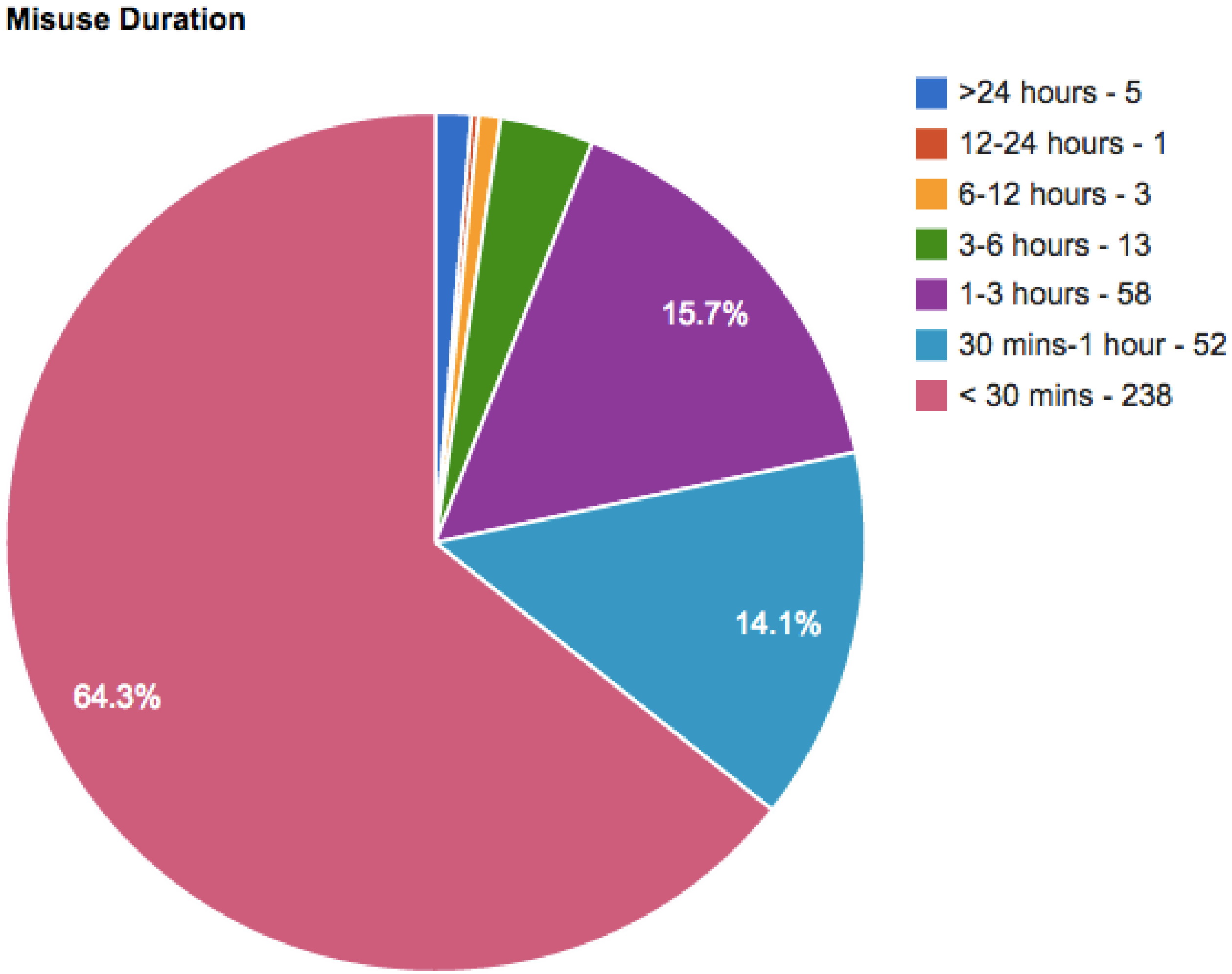
Slovenia, 2014 as seen through ATLAS

- bps size distribution example (Q4)



Slovenia, 2014 as seen through ATLAS

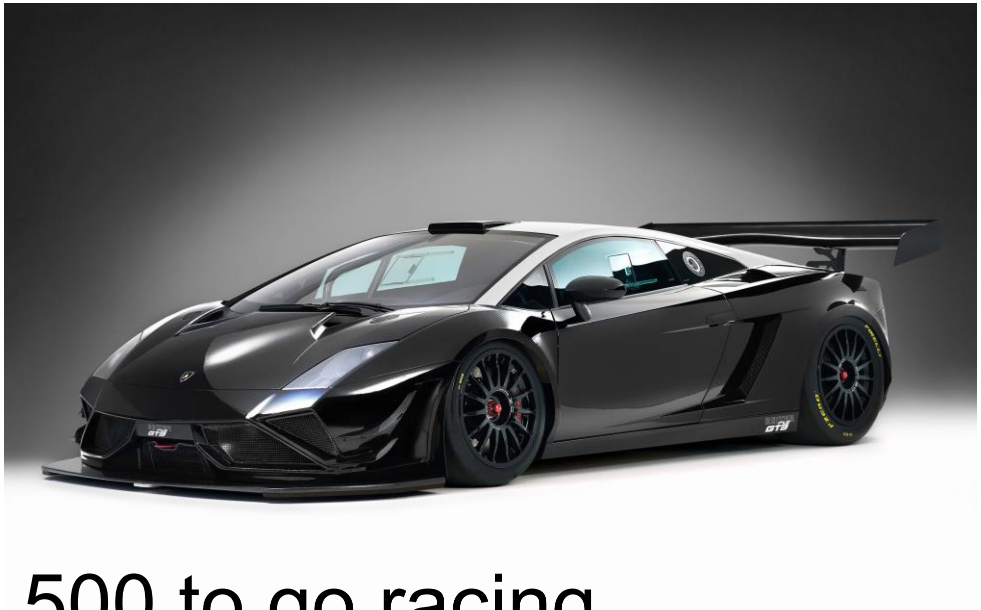
- duration distribution example (Q4)



DDoS mitigation DOs and DON'Ts

- DON'T:
  - think that you can solve it server-side
    - OS-level or application-level tweaking/optimization is necessary, but not enough. Not by a long shot.
  - think that you can throw bandwidth at it
  - think that you can solve it with:
    - firewalls of any shape or form or generation
    - IPS
    - DPI
    - Load balancers
    - These are all devices designed to do **other things**
    - They mostly perform stateful inspection, which is **BAD** in DDoS mitigation
    - Anti-DDoS features in non-dedicated devices will result in extreme **oversizing** and, eventually, failure anyway.

Spot the difference



- You don’t use a FIAT 500 to go racing
  - (you don’t use a firewall for anti-ddos)
- You don’t use a LAMBORGHINI to go to the supermarket
  - (you don’t use a ddos mitigation system as an IPS)

DDoS mitigation DOs and DON'Ts

- DO:
  - use Infrastructure Access Control Lists to **defend** from large, well-known reflection/amplification attacks
  - use BCP38 and BCP84 to **prevent** attacks
    - if we manage to stop spoofed traffic, we have solved half of the problem
  - secure your DNS/NTP/etc. servers
  - set up upstream blackholing (as a last resort)
  - use BGP Flow Specification
  - for most granular mitigation, use dedicated anti-DDoS systems

...and even if you’re using dedicated devices...

- DO:
  - place them in the right place (more on this later)
- DON’T:
  - think they are “magic”
  - use destination-based mitigation techniques
  - think rate-limiting is a DDoS mitigation technique

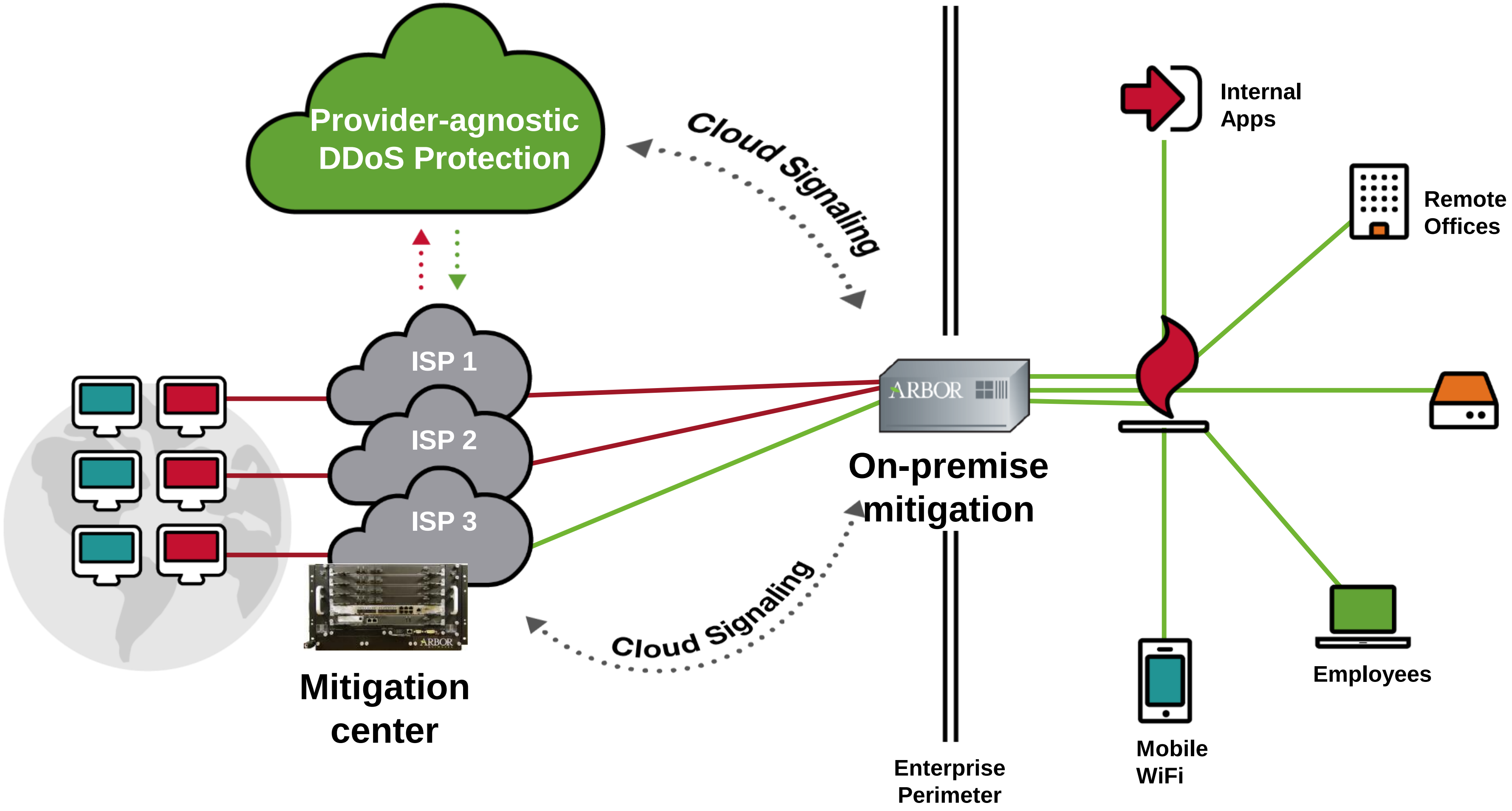
DDoS mitigation requires analysts skills

DDoS mitigation stops attackers (sources)

Let’s play the acronyms game

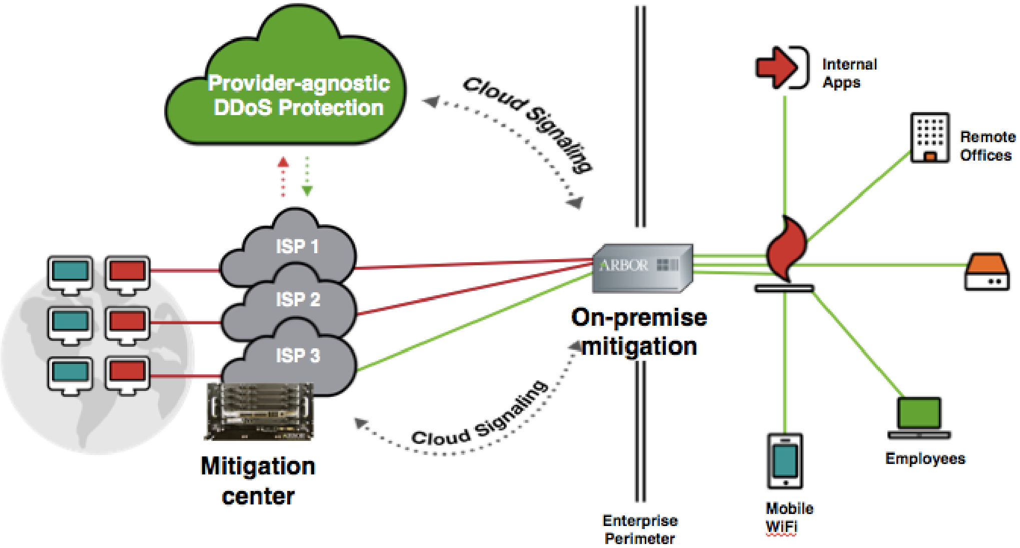
- CDN
  - Global Content Delivery Networks do provide DDoS mitigation services
    - usually for HTTP only; specific use case.
- SDN / NFV
  - Software Defined Networking / Network Functions Virtualization are, actually, currently, little more than buzzwords(*)
  - Use what we have now: BGP, FlowSpec.

Stopping attacks in the right place



Stopping attacks in the right place

- On-premise mitigation
  - inline (pros and cons)
  - always on
  - layer 7 visibility
  - limited capacity
- ISP services
  - on demand, /32 “offramp”
  - shared infrastructure
  - layer 3-4 detection
  - higher capacity
  - local support
- provider-agnostic services
  - on demand, BGP-based or DNS-based (pros and cons)
  - shared infrastructure
  - higher capacity
  - less granularity
  - remote support



Resources

- www.arbornetworks.com/report
- www.digitalattackmap.com
- www.youtube.com/user/ArborNetworks

mgioanola@arbor.net

Thank You

MASTERLINE

ARBOR® NETWORKS

ARBOR®
NETWORKS