

Key Internet backbone security trends

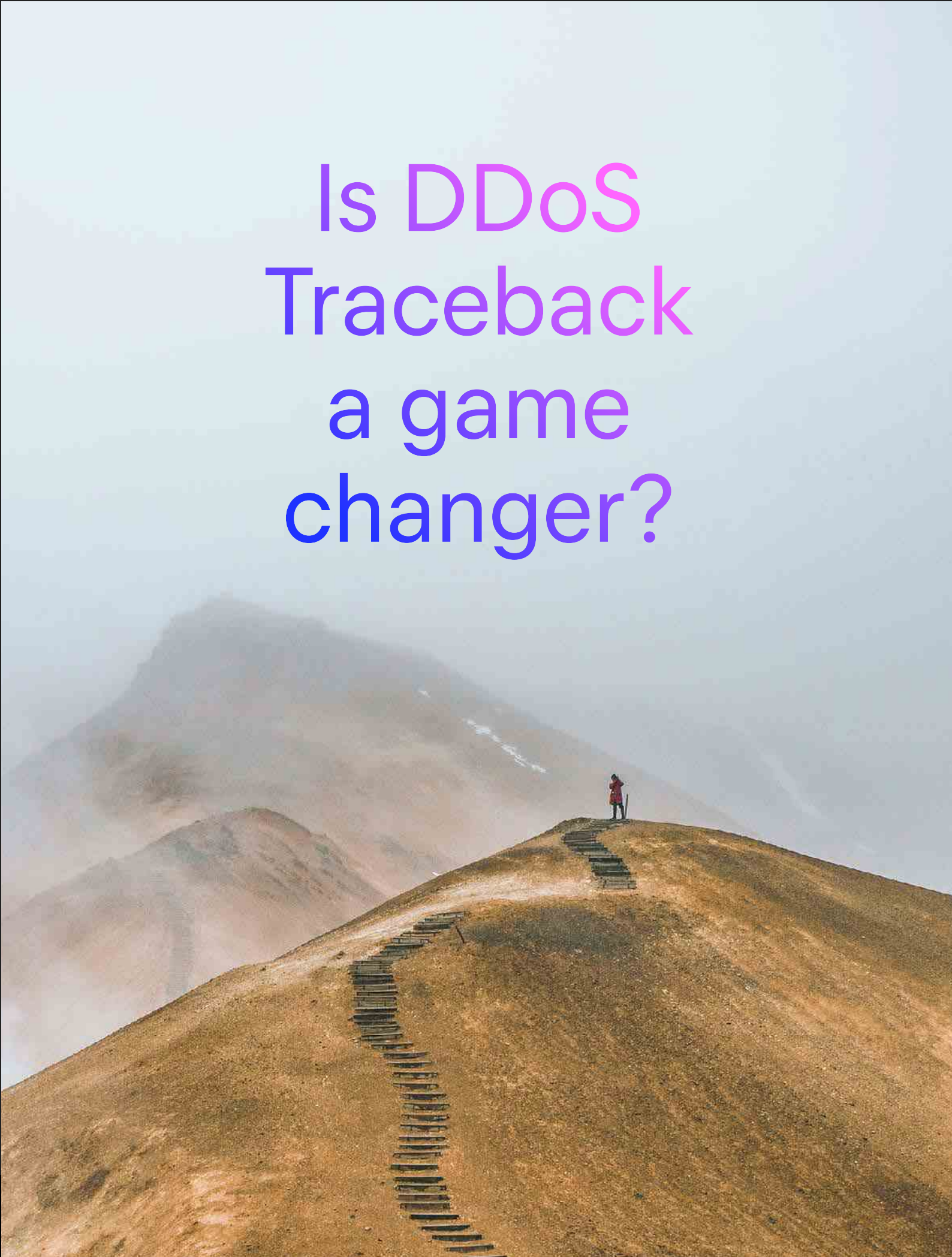
DDoS threat landscape report 2023



Unique insights from the core of the internet

Operating the world's #1 Internet backbone gives us a unique global perspective on the constantly evolving DDoS threat landscape.

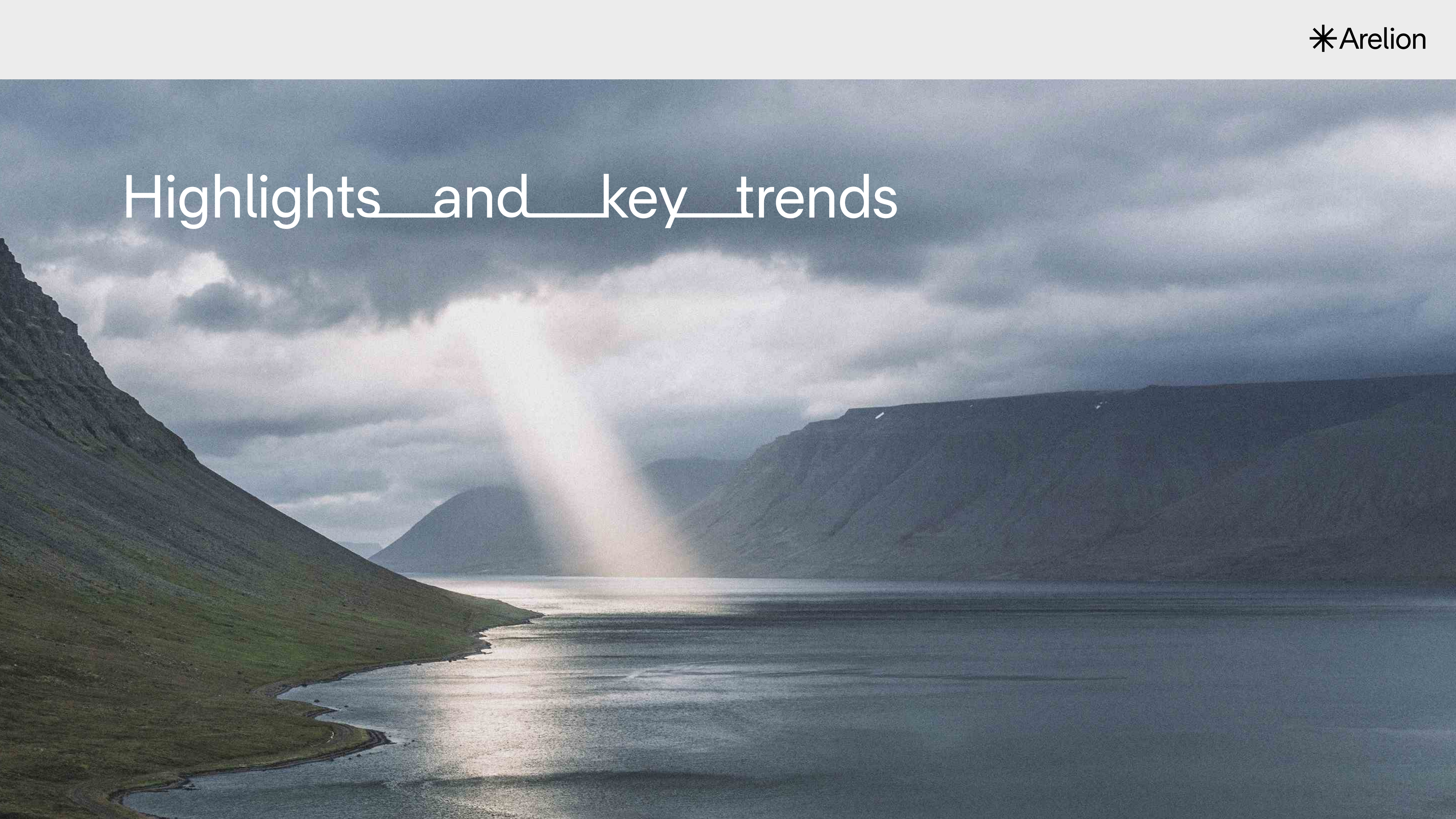
Using our own network data, this latest report highlights the key global DDoS trends we observed in AS1299 during 2022 – from the overall impact of DDoS attacks, to the evolution of specific attacks vectors and significance of major social and geopolitical events.



Is DDoS
Traceback
a game
changer?

An anti-spoofing initiative that makes it much more difficult for DDoS attack providers to operate.

Highlights and key trends





Europe: the DDoS battlefield

There was a greater concentration of DDoS activity in Europe during 2022 – most likely as a consequence of the ongoing war in Ukraine.

As the Ukrainian authorities sought safe harbor for their digital state registries and databases, the distribution of attacks moved away from active conflict areas and into global cloud centers. This was a consequence of both damage to national network infrastructure and the strategic migration of local databases and applications into the cloud.

A different approach was taken by countries not under direct physical attack. Here, greater local reinforcement of in-country IT infrastructure resulted in more local attacks. The divergent approaches towards national-level attacks can be summarised as: ‘distribute’ or ‘defend’.



The DDoS arms race

Overall, the number of DDoS attacks in our global network decreased by a 1/3 in 2022 – with 50% fewer attacks towards our customers. Even when the extraordinary 2021 pandemic traffic spikes are discounted, there was a dramatic reduction in DDoS activity within our network by the end of the year.

Although this doesn't necessarily reflect the situation in local networks, the lower global backbone impact was largely due to an industry wide anti-spoofing initiative – the DDoS Traceback Working Group.

Generally, we are seeing a more decisive response by network and IT infrastructure owners to cyber threats, and they are gradually starting to fight back - through better cooperation and by closing the inherent weak spots in the network that cybercriminals have exploited for so long.



Attack distribution & intensity

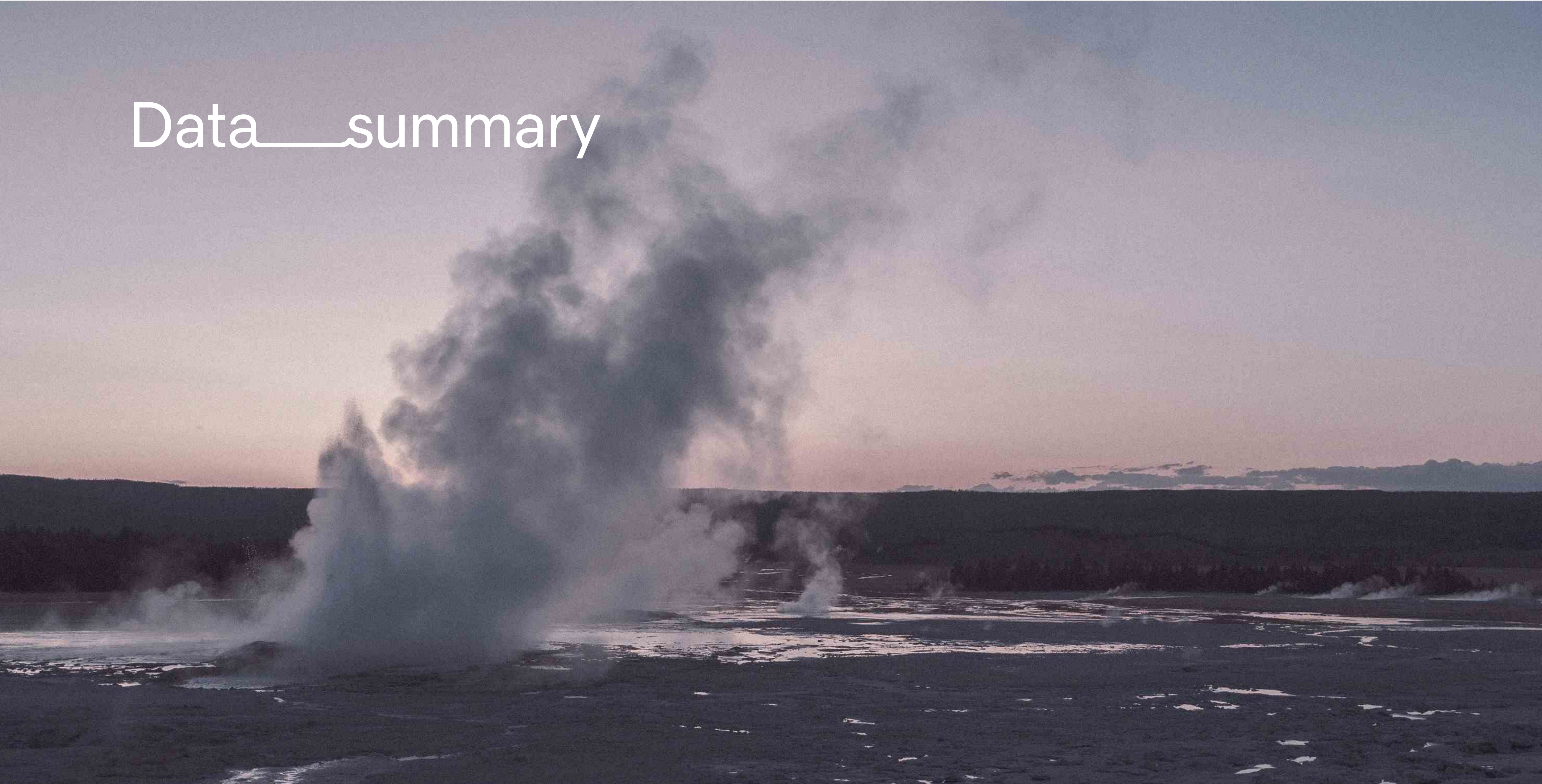
The size of the largest attacks keeps growing. In 2022, peak attack traffic (Mpps) was up 19% from 2021. This trend is not only a reflection of overall Internet traffic growth, but also the continuing shift towards fewer, but more spectacular attacks.

The average size of attacks experienced by our DDoS customers increased in 2022, both in terms of bits and packets.

Whilst there has been an increase in the number of large attacks, the vast majority of attacks are still small. These are mostly driven by free tier stress-test or DDoS-as-a-Service attacks instigated by amateur cybercriminals.

We saw the biggest increase in the 5-20 & 20-50 Gbps attack ranges, mainly as a result of DNS and NTP attacks, but also memcache due to its high amplification factor.

Data summary

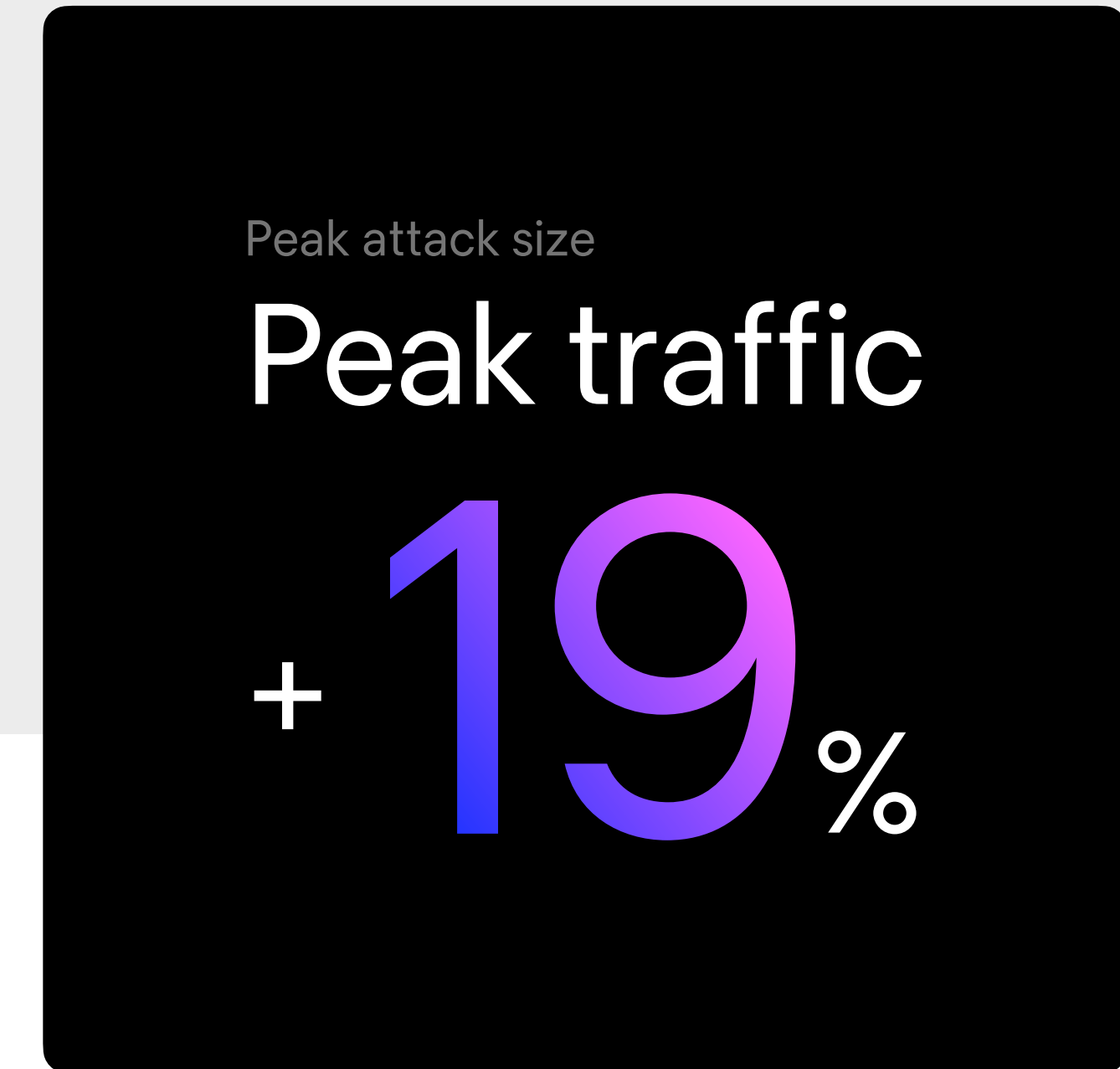
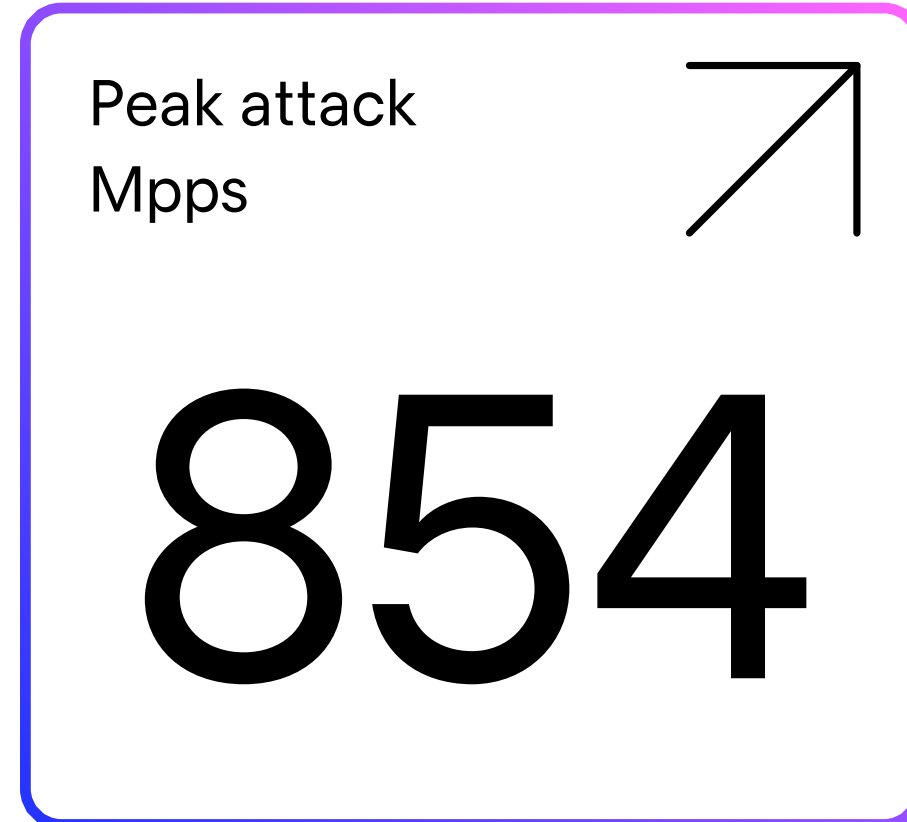
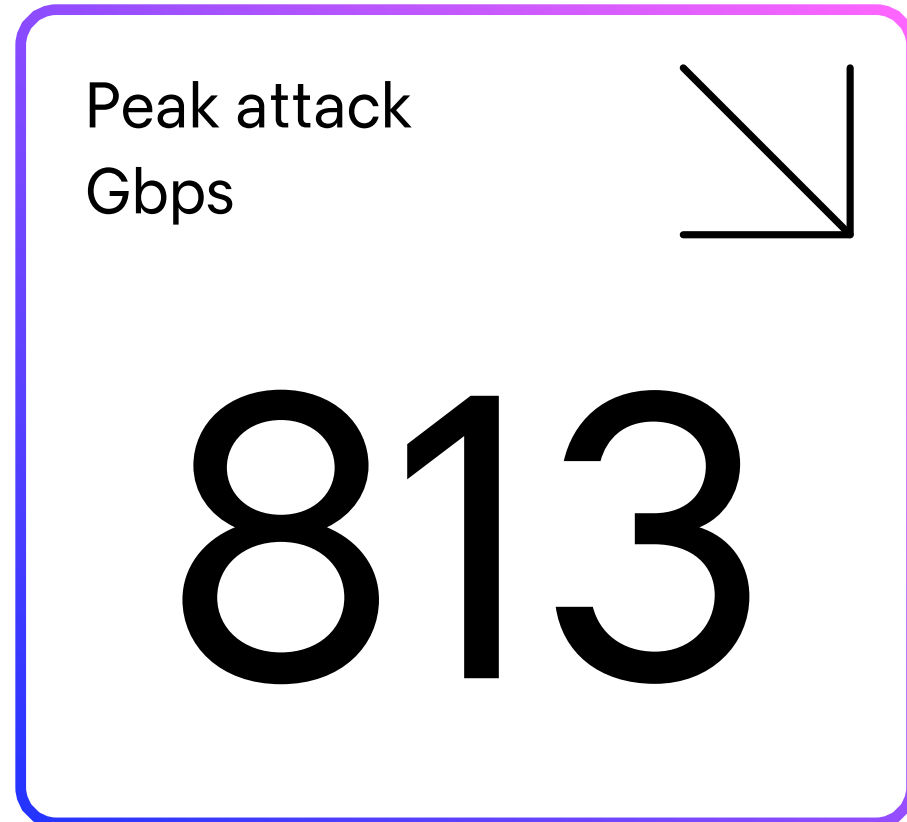




Network impact – peak attack size

The size of the largest attacks keeps growing. In 2022, peak attack traffic (Mpps) was up 19% from 2021.

This trend reflects overall Internet traffic growth and is also evidence that there is a continuing shift towards fewer, but more spectacular attacks.



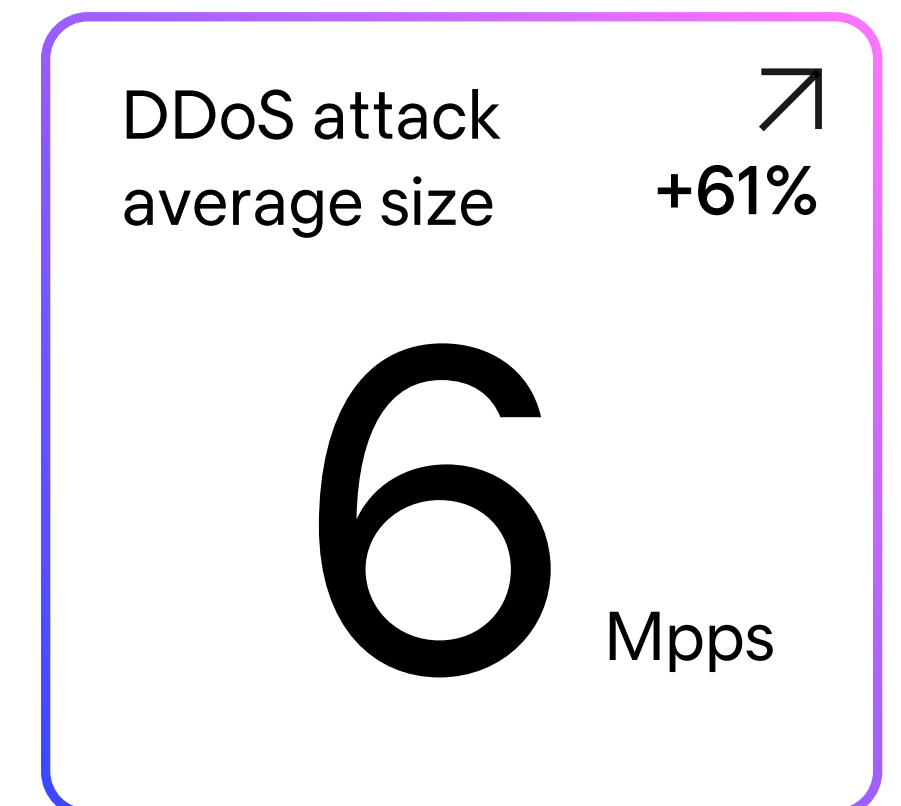
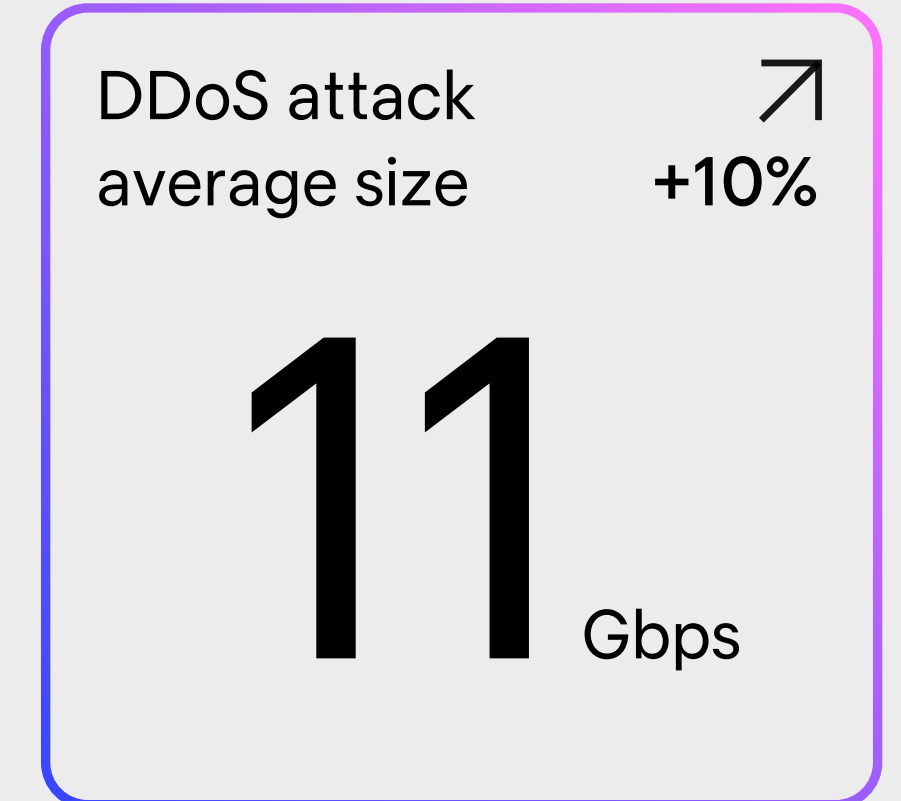
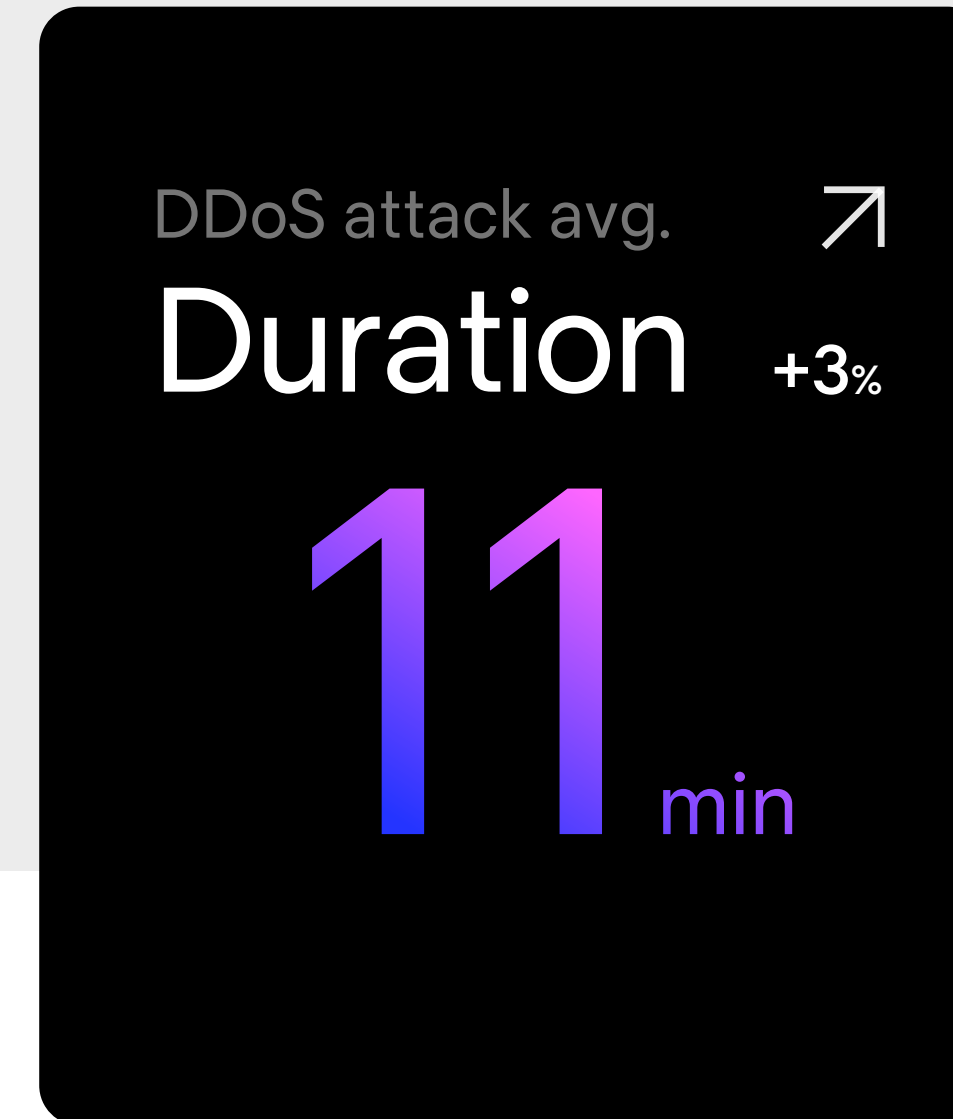


Average attack size and duration

The average size of attacks experienced by our DDoS customers increased in 2022, both in terms of bits and packets. Packet intensity has fluctuated throughout the year, but the general trend is upwards. The average duration of attacks has increased marginally since 2021. Looking at the bigger picture, the increase in average size is driven by a shift towards a greater number larger and fewer mid-sized attacks.

Attack average packet length per day

— AVERAGE PACKET LENGTH



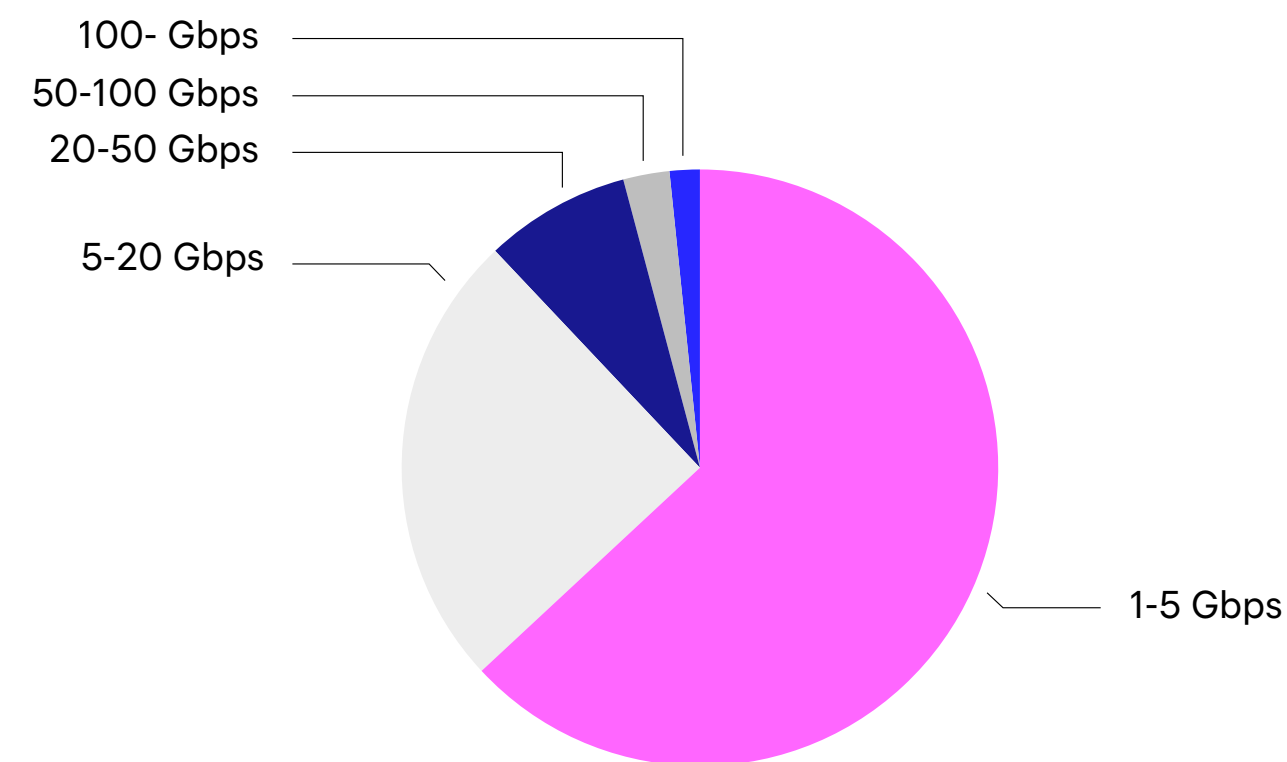


Overall size distribution

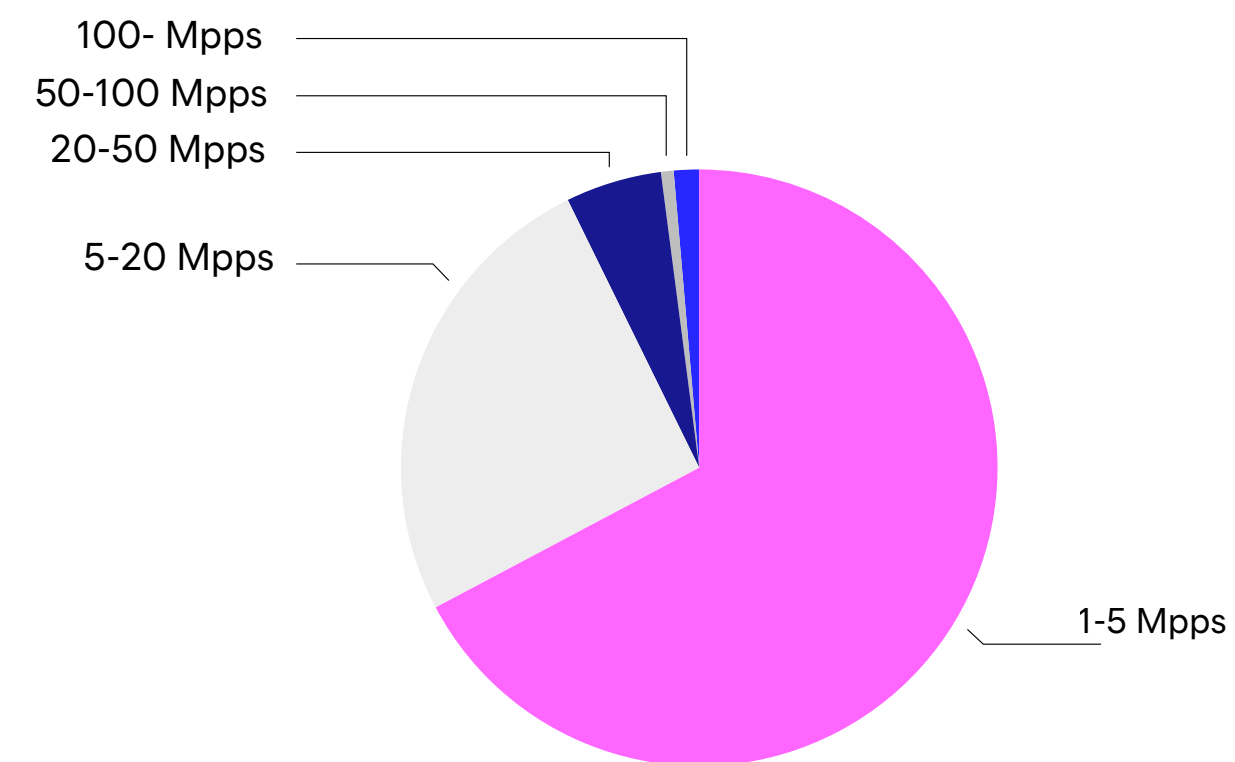
When looking at the overall size distribution of attacks in our backbone, we see that while there has been an increase in the number of large attacks, the vast majority of attacks are still small. These are mostly driven by free tier stress test or DDoS-as-a-Service attacks instigated by amateur cybercriminals. We saw the biggest increase in the 5-20 & 20-50 Gbps attack ranges.

This is because NTP and memcache attacks (the main DDoS drivers) have a much larger amplification factor and are more effective as a result (NTP 556x, memcache 10-51,000x and DNS 28-54x). All of this reinforces the need for a basic level of customer protection to mitigate the abundant smaller attacks, together with a solid insurance policy (a capable provider with effective DDoS protection services) for the larger ones.

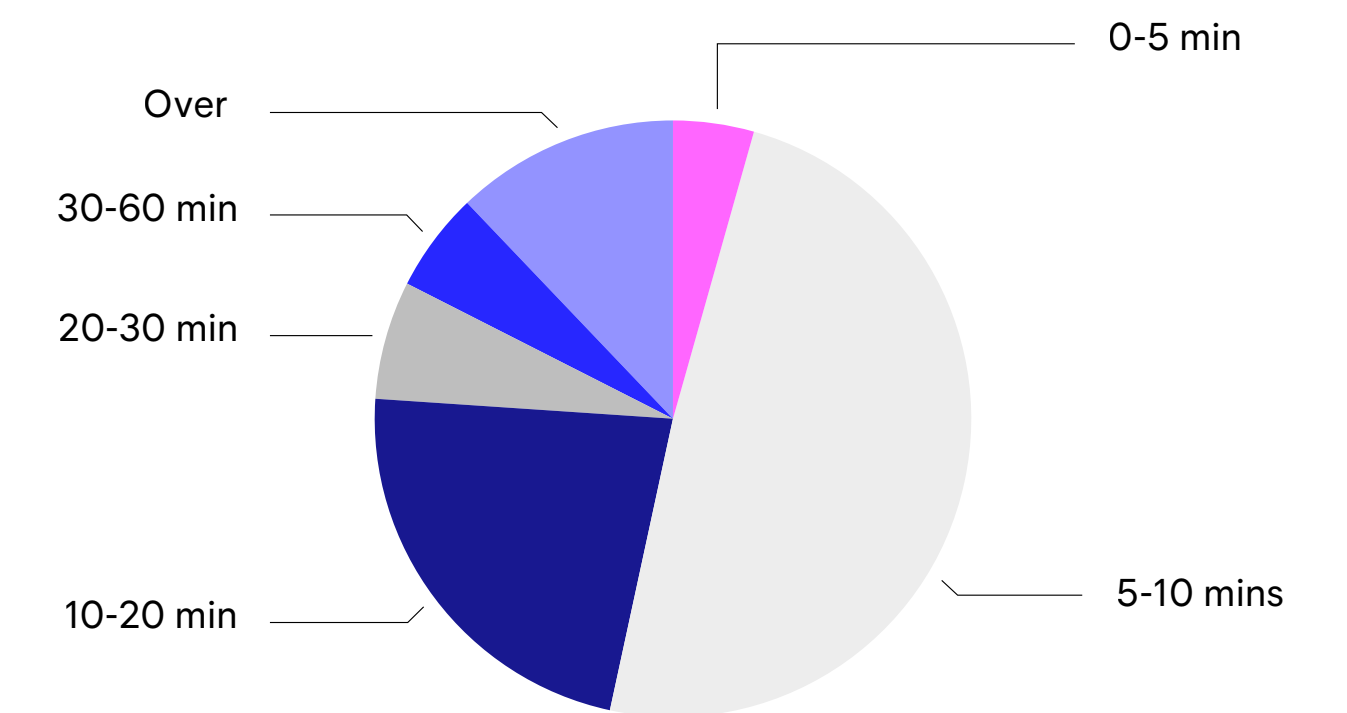
DDoS attack size Gbps



DDoS attack size Mpps



DDoS attack duration





Attack vectors towards our customers

There was a noticeable trend towards larger (bps) attacks targeting our customers at the end of the year. In terms of distribution, DNS & NTP are still the two most common attack vectors, with NTP decreasing slightly during the year. We also noticed a decline in UDP-based spoofing attacks as servers are slowly being secured throughout the internet and are consequently used less frequently for such attacks. As a result, the underlying threat from reflection attacks is slowly but surely being reduced.

Attack amplification

UDP-BASED
PROTOCOL

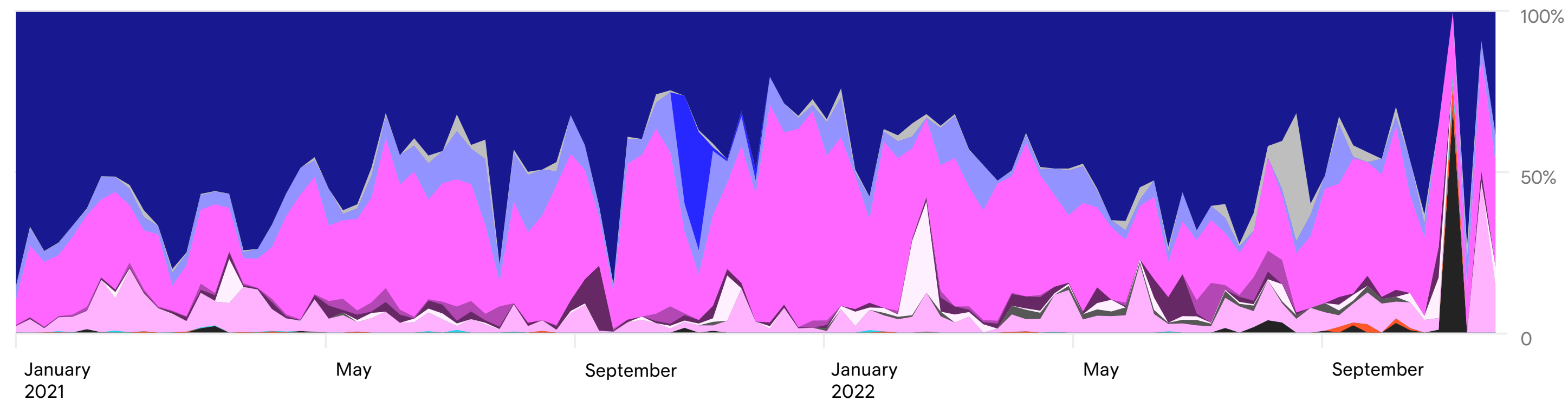
SCALING
MULTIPLE

DNS	28-54 x
NTP	556 x
SNMP	6.3 x
CharGEN	358 x
Memcached	10,000 - 51,000 x

Because of the effectiveness of a high amplification factor, our customers are still facing a significant threat from memcache.

Alert types DDoS customer per week

● DNS ampn. ● IP fragm. ● L2TP ampn. ● LDAP ampn. ● NTP ampn. ● SNMP ampn. ● SSDP ampn.
 ● TCP ACK ● TCP RST ● TCP SYN ● WSD ampn. ● chargen ampn. ● memcached ampn.

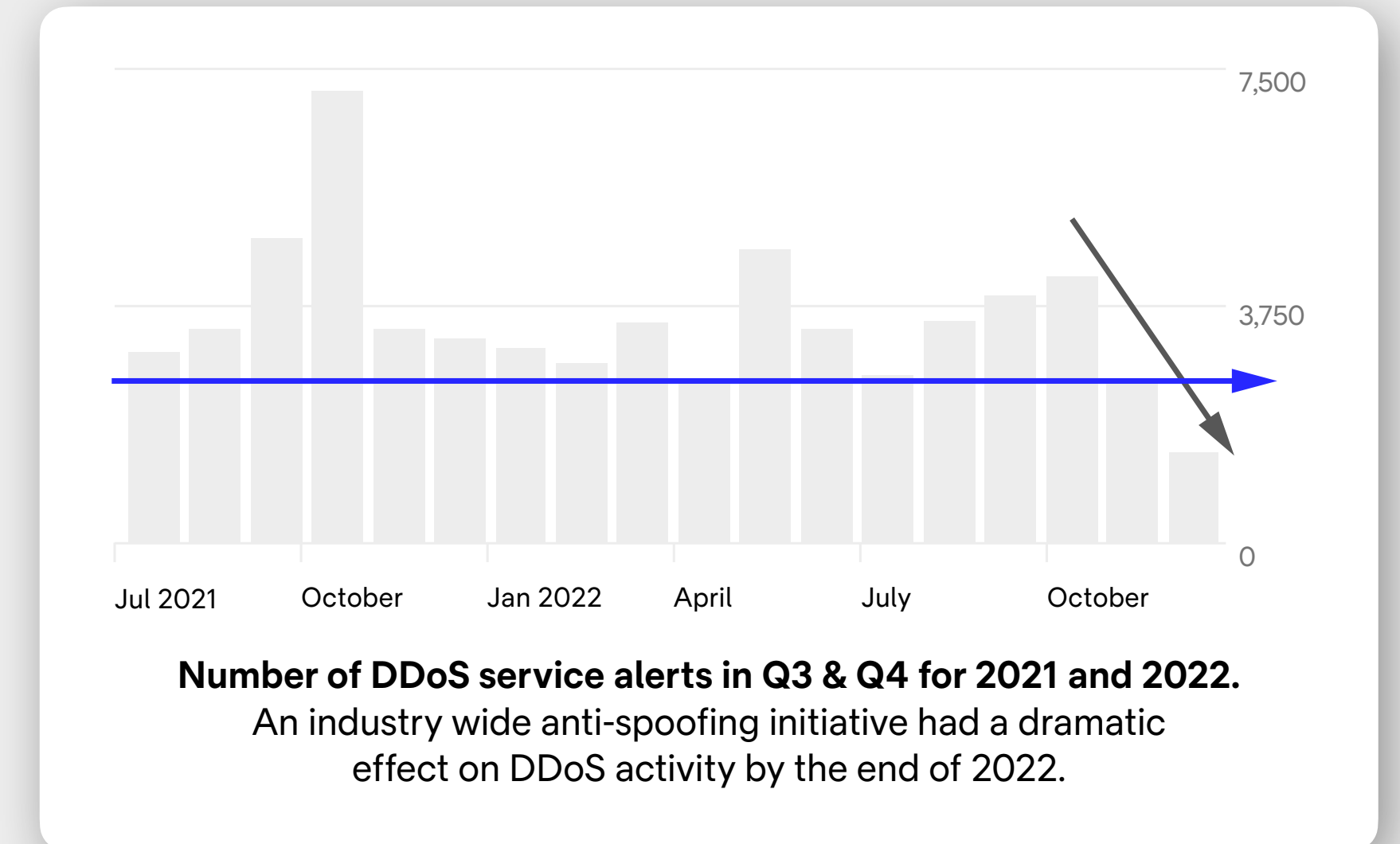




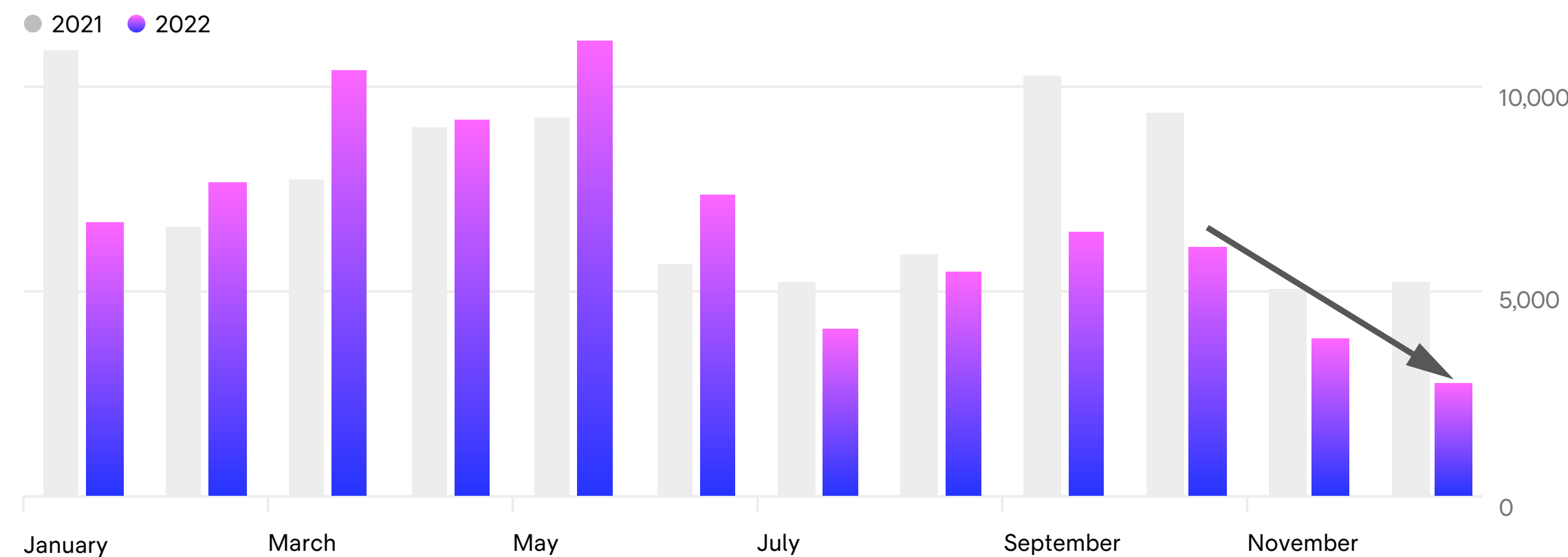
Monthly attack distribution

The number of DDoS attacks in our global network decreased by a 1/3 in 2022, with 50% fewer attacks towards our customers. However, it is worth noting that we observed an exceptionally high amount of pandemic-related DDoS activity during Q1 & Q2 2021, but activity in Q3 & Q4 for both 2021 and 2022 were comparable.

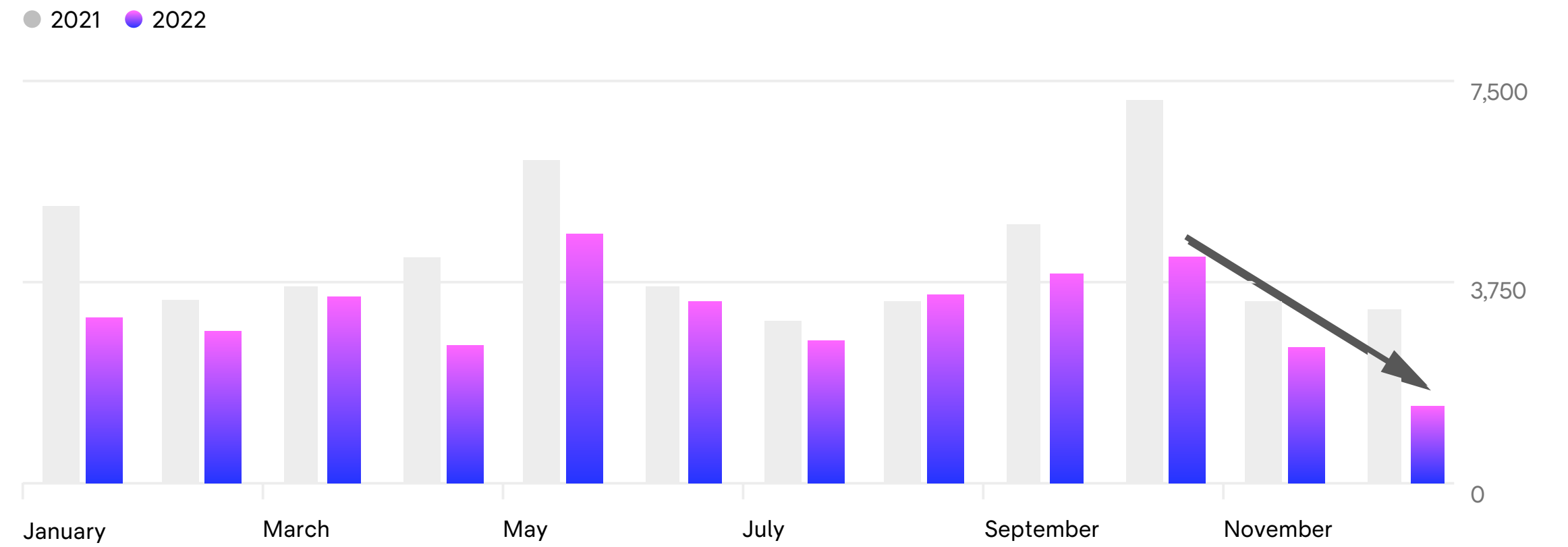
There was a dramatic reduction in DDoS activity within our network during the final months of the year. This was largely due to an industry wide anti-spoofing initiative – the DDoS Traceback Working Group – between backbone providers (see the following pages).



All alert



DDoS service alert





DDoS day-to-day

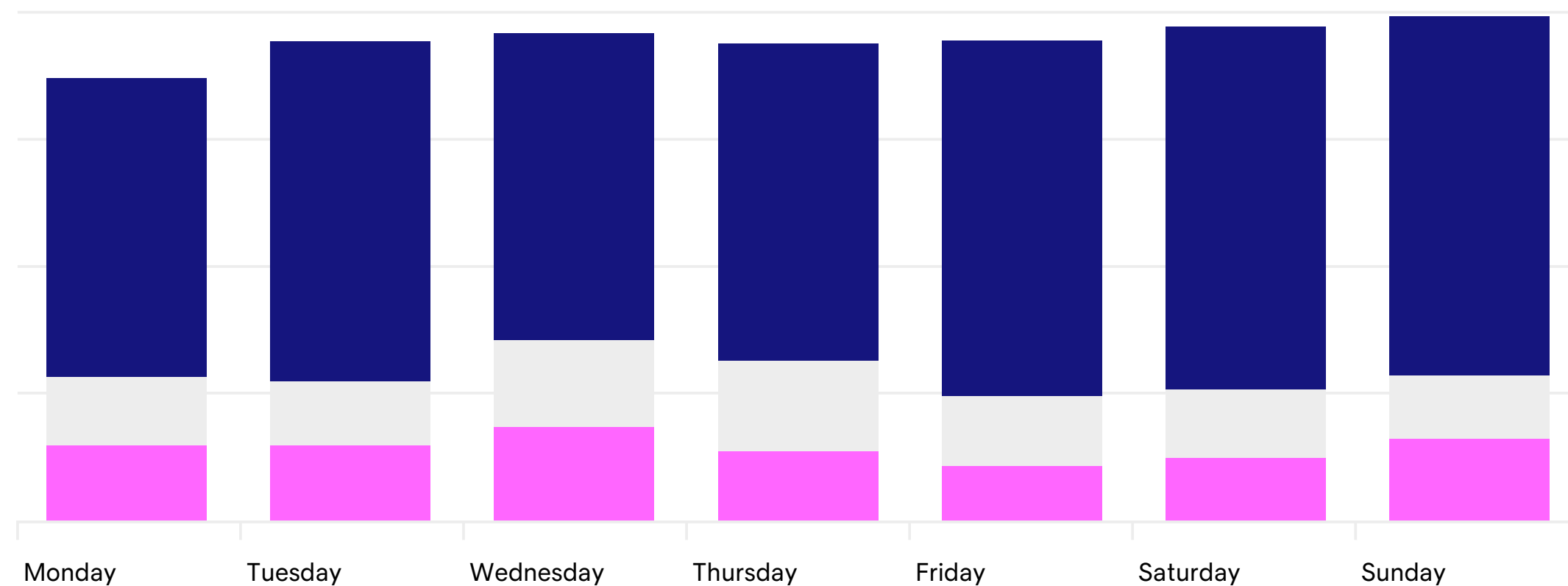
Attacks continue to follow the sun and DDoS doesn't take the weekend off – they are a constant threat every day of the week.



Peak DDoS Hour
22:00
CET

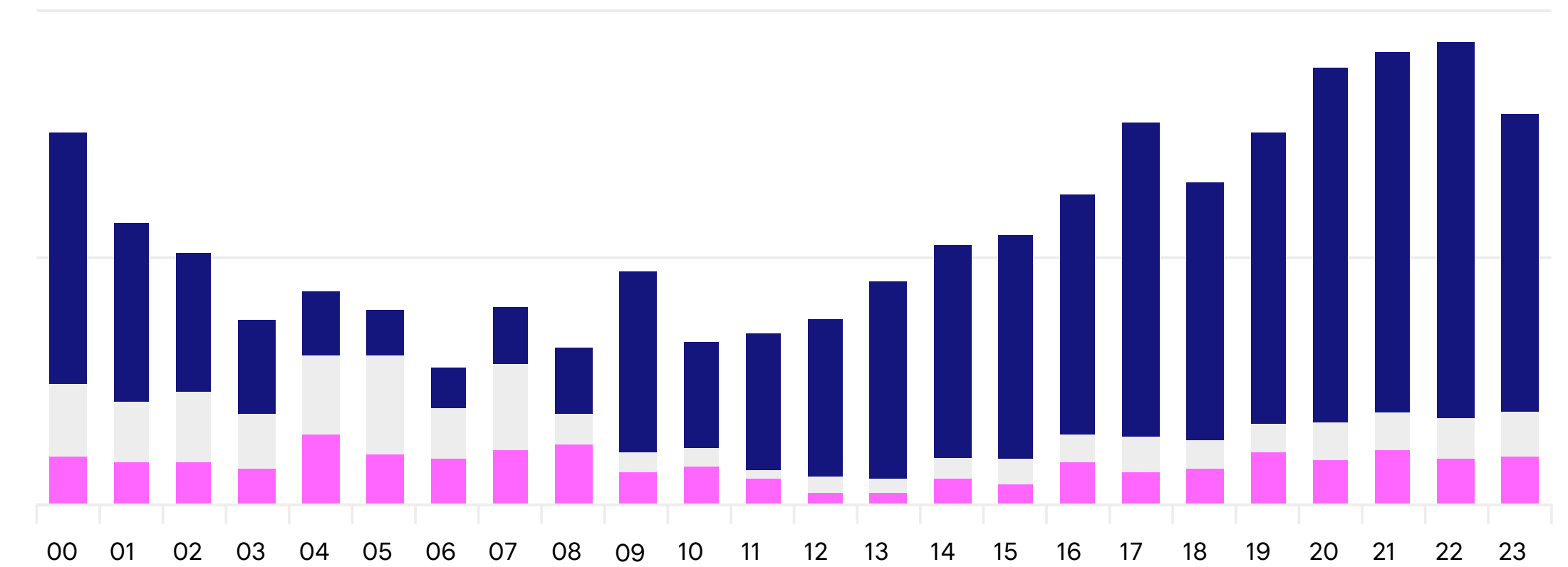
DDoS customer continent weekday

● North America ● South America ● Europe



DDoS customer continent hour CET

● North America ● South America ● Europe



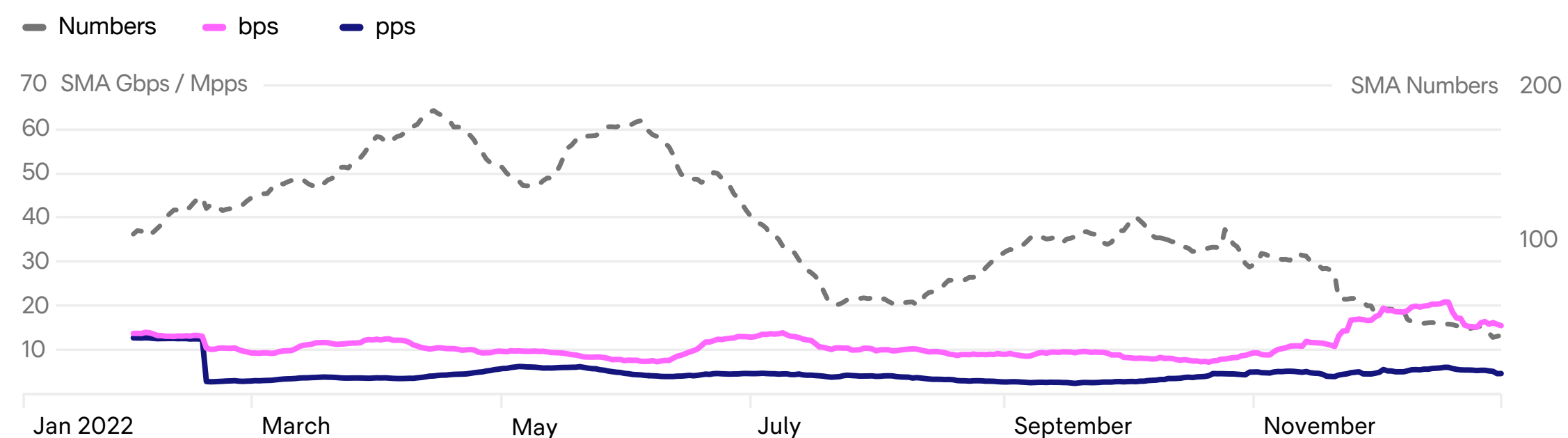


Could DDoS Traceback be a game changer?

During 2022, we started working together with a number of other major backbone networks in the DDoS Traceback Working Group, an initiative to actively track spoofing-friendly networks, and by encouraging customers to implement anti-spoofing mechanisms and/or shutdown bad client networks. Spoofing is a key component of the amplification/reflection attacks that we've seen in recent years. This work proved to be effective and has made it much more difficult for the DDoS attack providers (Stresser/Booter services) to operate.

While this has resulted in a drop in the overall number of attacks, we are seeing an increase in direct-path attacks from botnets, – albeit it to a lesser extent. These are more expensive to purchase since bots are a valuable asset for cyber criminals and if exposed, they risk being shut down when used extensively. Also, proxies are being used more – as a smoke screen to protect the bots from being exposed.

Attack size (all) per day, simple moving avg. 28 days (>1 Gbps, >1 Mpps)





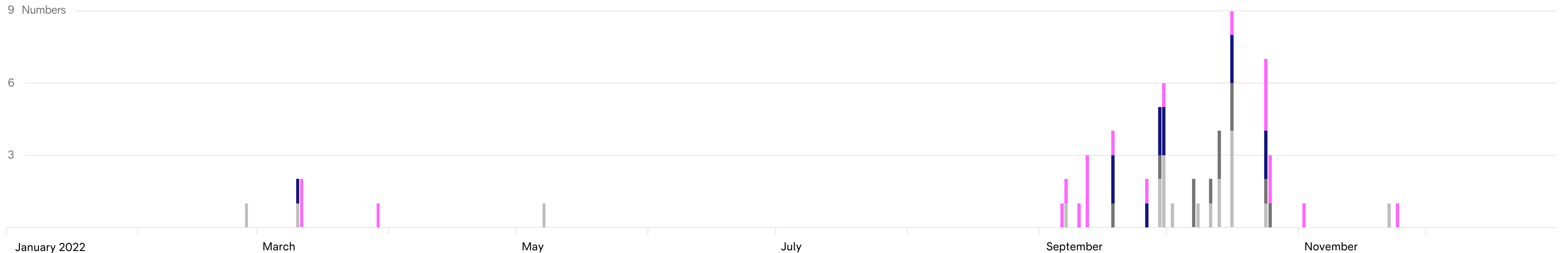
Carpet bombing

Carpet bombing is still a challenge faced by all of our customers, even if attacks have become increasingly less effective. Although attacks were more sporadic in 2022, they are still problematic. The lower intensity can be seen as a real-life manifestation of the DDoS arms race, where the ‘good guys’ currently have the upper hand – although the constant evolution of threats calls for sustained vigilance.



Global carpet bombing severity

● Low ● Medium ● High ● Extreme



Geographical distribution

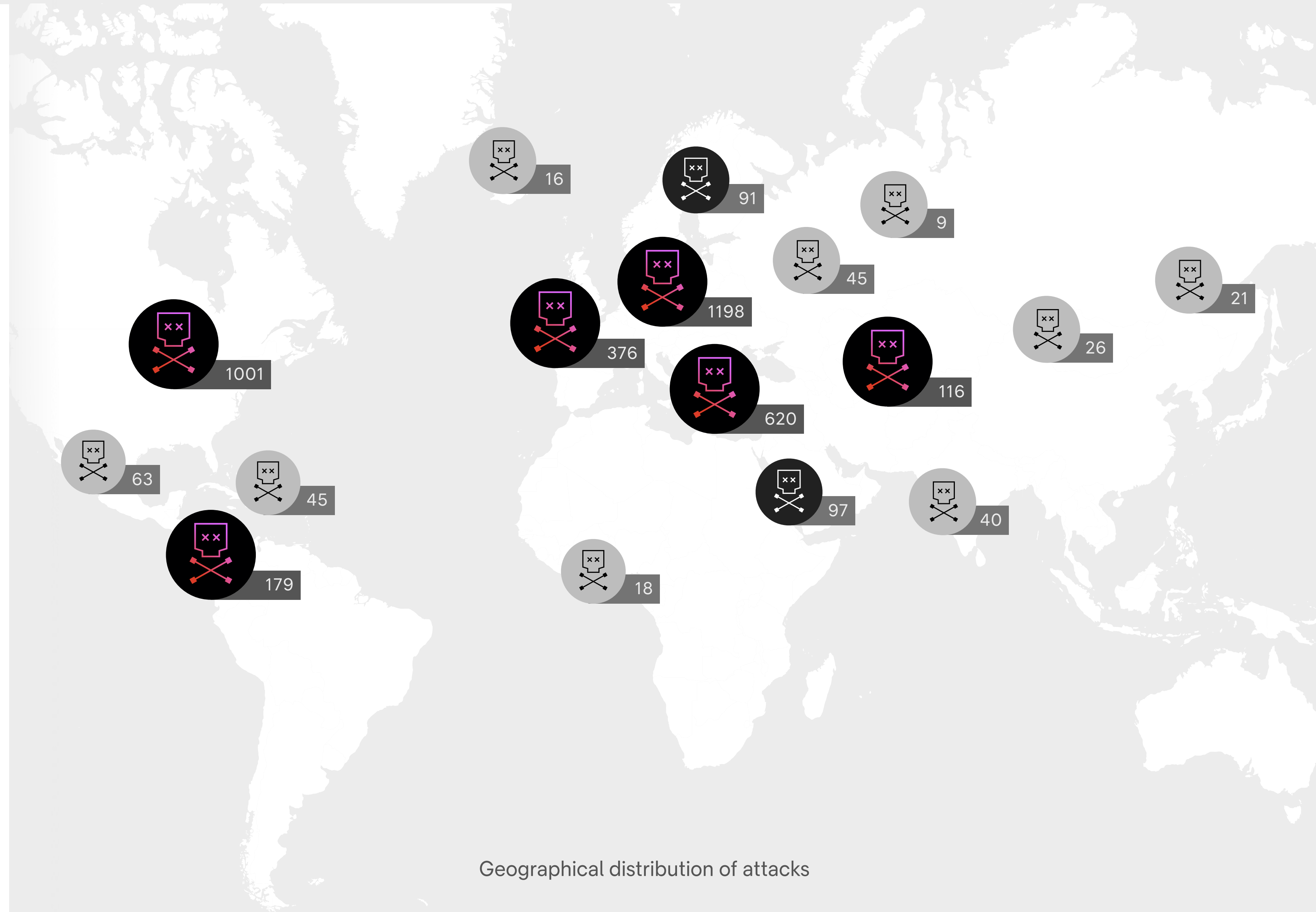




The global picture in AS1299

As with previous years, DDoS attacks appear to reflect major geopolitical challenges and social tensions, and increasingly conflicts between sovereign nation states, where DDoS has become an increasingly significant part of the hybrid warfare arsenal.

We observed less Asia-US DDoS activity and fewer DDoS attacks to and from South America during 2022.



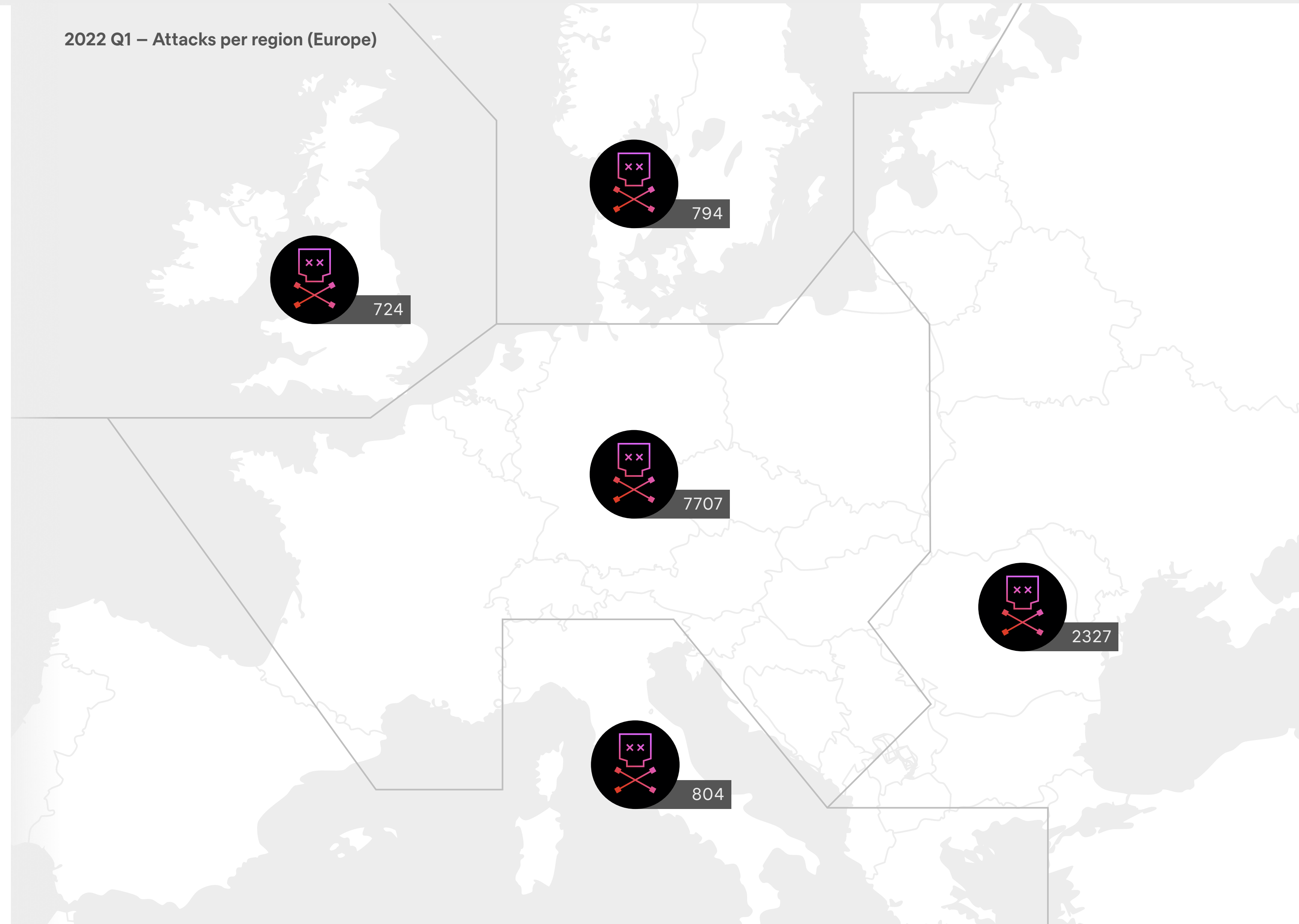


The new battlefield 1/2

In 2022 we saw a greater concentration of DDoS activity in Europe – most likely as a consequence of the war in Ukraine.

As the Ukrainian authorities sought a safe harbor for digital state registries and databases, we saw the distribution of attacks move away from active conflict areas into global cloud centers – both as a result of damage to local network infrastructure, but also as local databases and applications were strategically migrated into the cloud.

2022 Q1 – Attacks per region (Europe)

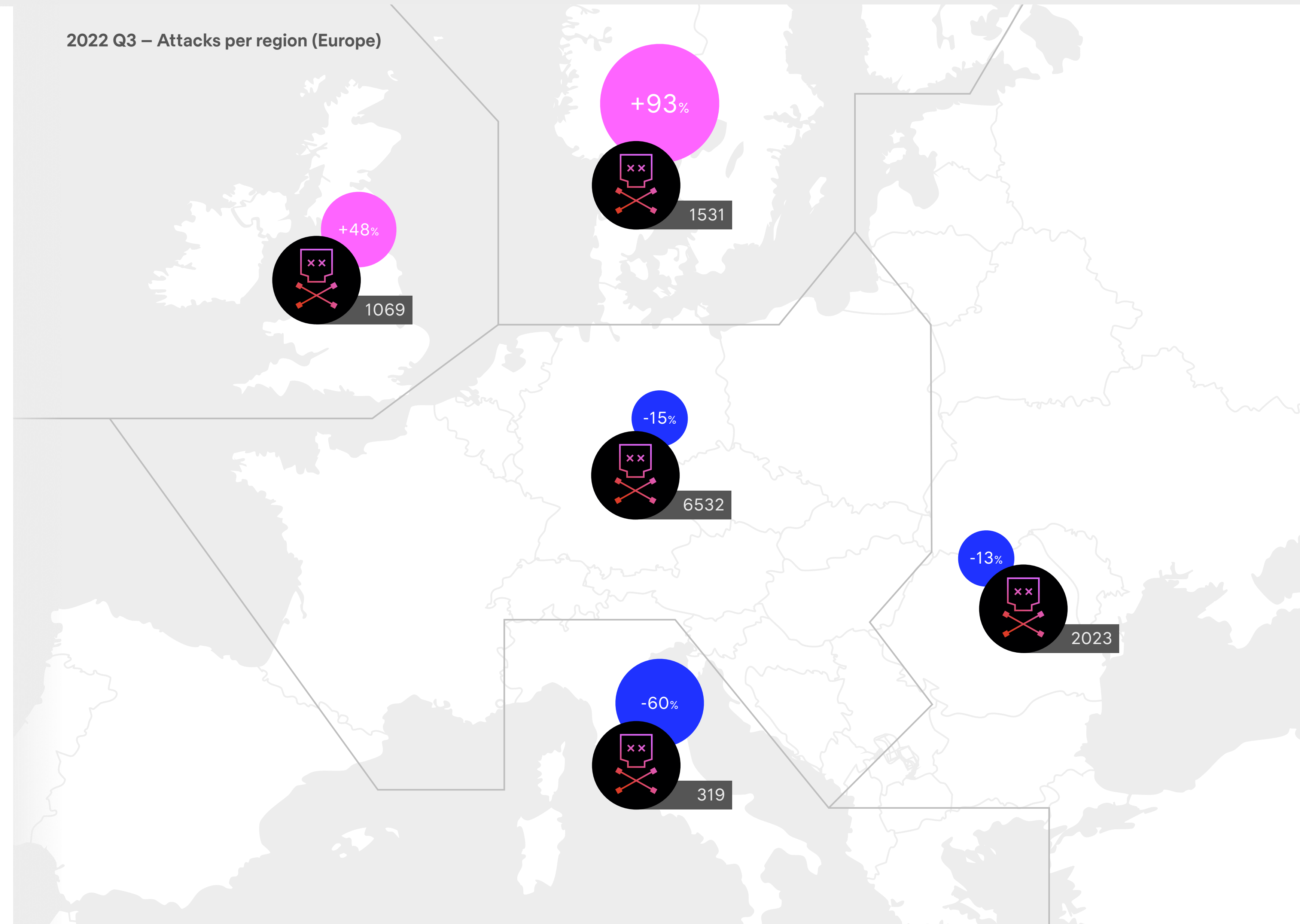




The new battlefield 2/2

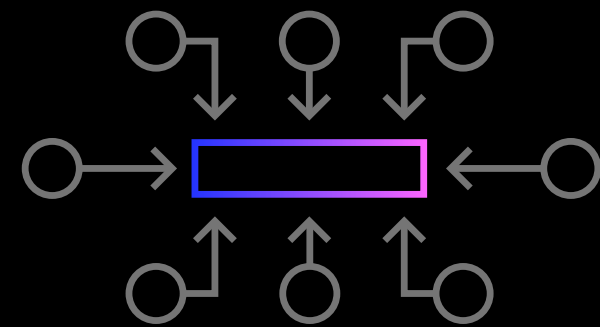
A different approach was taken by countries facing a tangible threat (especially in northern Europe). Even without physical attacks, local reinforcement policies for in-country IT infrastructure made some countries the target for more state-level cyber attacks.

A divergence of opinion regarding defence against sustained national-level attack has resulted in two key approaches – ‘distribute’ or ‘defend’.



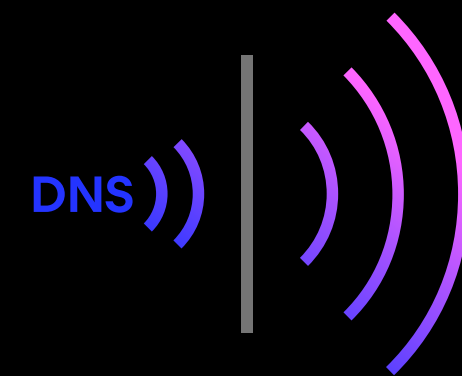


Glossary and terminology



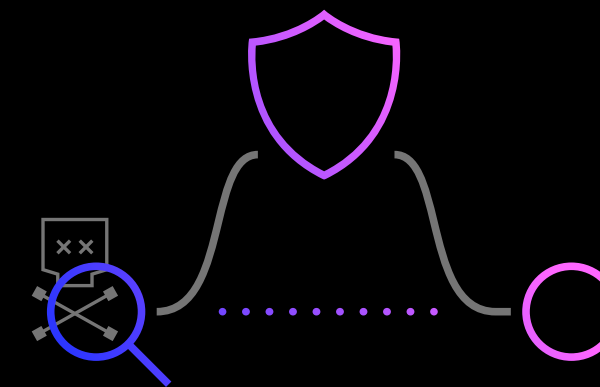
Attack-vector

The particular method or pathway used by cybercriminals to instigate a cyber attack. There are many types of attack vector – some more common than others – and many often employ multiple attack vectors simultaneously for maximum impact.



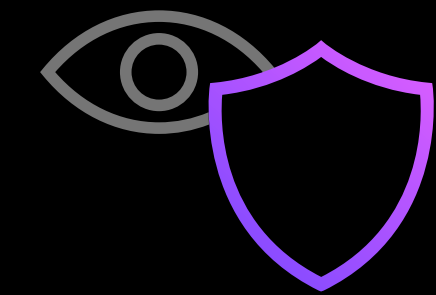
DNS amplification

A reflection attack which floods a target with large quantities of User Datagram Protocol (UDP) packets. It exploits vulnerabilities in domain name system (DNS) servers to turn initially small queries into large data payloads which eventually take down a victim's servers.



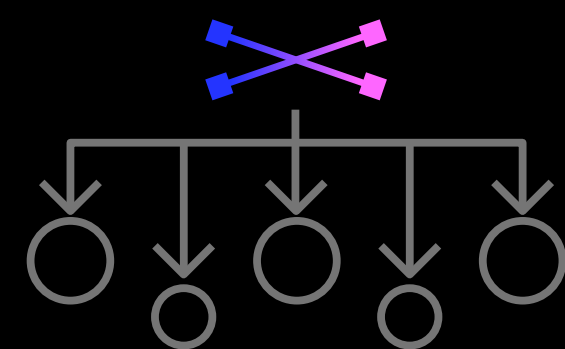
Auto-mitigation

When a DDoS attack is detected, the impacted traffic flow is directed into DDoS scrubbing centers automatically, allowing attack mitigation to begin within a few seconds of attack detection.



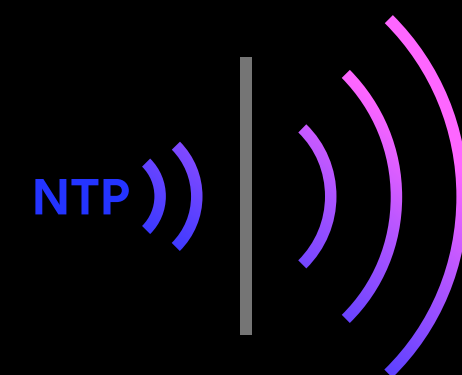
Spoofing

A technique whereby attackers manipulate the source IP address of their traffic to make it appear as if it is coming from a different computer. In other words, they "spoof" the source IP address to evade detection and make it difficult to block traffic and find the origin of the attack.



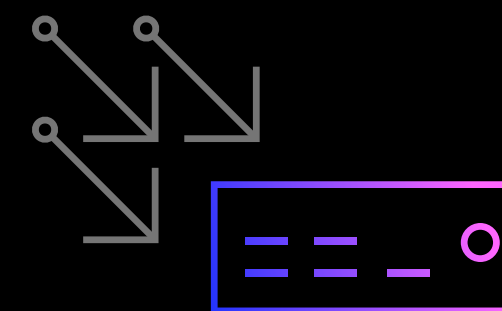
Carpet bombing

A term used to describe attacks that target a range of addresses or subnets, potentially affecting hundreds or even thousands of destination IP addresses. These attacks can impact a service provider's ability to deliver service and are difficult to mitigate.



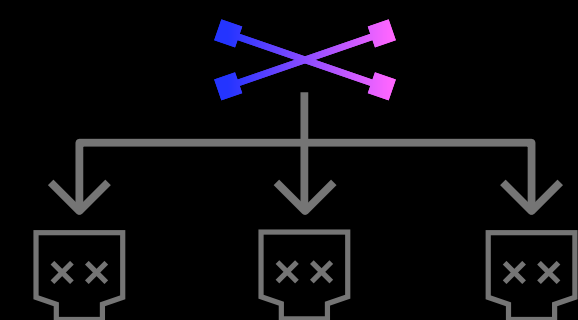
NTP amplification

The attacker exploits publicly accessible Network Time Protocol (NTP) servers to overwhelm a target with UDP-traffic. The server response is much larger than the request, amplifying traffic towards the server and degrading legitimate traffic.



SYN attacks

An attacker rapidly initiates multiple SYN connection requests to a server without finalizing them. The server must wait for half-opened connections, which ultimately consume enough system resources to render the targeted system unresponsive.



DDoS-as-service / Botnets

Cybercrime has become more organized and automated as hackers seek to monetize their network of malware infected assets. This means that attacks are accessible even to bad actors with limited technical knowledge.

DDoS mitigation with superior precision

The Arelion DDoS protection service applies surgical scrubbing techniques to automatically detect and mitigate attacks.

Malicious traffic is dropped within our global backbone network, before it reaches your Internet connection.

Network based mitigation provides a powerful shield for DDoS traffic, ensuring that only legitimate traffic passes through.

Scale to the number of managed objects

We provide a high-capacity solution throughout our global IP backbone that can be scaled to add more Managed Objects (MOs) and mitigation capacity to support evolving threats and to support your growing protection needs.

Flexible pricing

Our pricing model is designed in accordance with your risk profile, making it more economical than in-house edge solutions.

Features

- Protection against evolving attack vectors: volumetric, protocol, application
- Surgical host-level mitigation
- Manual or automatic protection
- 24/7/365 protection

Security highlights

- Physical and logical security from design to deployment
- A network-wide Acceptable Use Policy (AUP)
- Customer service authentication procedures
- Transparent customer data handling policies



About us

Formerly Telia Carrier, Arelion is a leading light in global connectivity services. We've been keeping the world connected since 1993 and today our global IP backbone, AS1299, is ranked number one in the world.

Our network spans Europe, North America and Asia, with 70,000 km of optical fiber and 1,700 MPLS end points. Our award-winning customer service team supports our expansive customer base, who rely on us for their business-critical services.

Follow us on [LinkedIn](#) and [Twitter](#)
Discover more at www.arelion.com

This information set forth herein is intended for general informational purposes only and is provided "as is" without any representation, warranty or condition of any kind, either express or implied. There is no assurance as to the accuracy or completeness of such information and circumstances may change. Use of the information is entirely at the consumer's risk, and nothing herein constitutes an offer to sell any service or product or is intended to imply, create or modify a contractual or other relationship. No part of this document is to be copied, reproduced, distributed or disseminated in any way without the prior written consent of Arelion.

©Arelion AB. 2023. All Rights Reserved.