

Key backbone security trends

DDoS threat landscape report 2025





Unique insights from the core of the Internet

Our global Internet backbone, AS1299 – ranked the world’s #1 - gives us a unique perspective on the constantly evolving DDoS threat landscape, and the impact it is having on the wider Internet.

Using our own network data, this report highlights the main global DDoS trends we observed in 2024 – from the overall network impact of DDoS and evolution of specific attacks vectors to the significance of major social and geopolitical events in a cyberattack context.

As law enforcement agencies around the world continue to combat the criminal networks behind DDoS on the ground, we have also highlighted the major operations during the year. With the ongoing challenge of DNS amplification attacks in 2024, we have also taken a closer look at some of the factors which make this such a compelling threat.

How is the
DDoS threat
evolving?



Highlights and key trends 2024



Game on: the gaming industry in the spotlight

The online gaming industry was the main DDoS target in 2024. Of the peak attacks during the year, the second largest hit one of the biggest platforms in the US.

Cyber warfare got physical

Cyberwar had a tangible physical impact in the world during 2024, and although the headlines were largely focused on subsea cable sabotage, it is only a matter of time before bad actors become sufficiently emboldened (or desperate enough) to target other critical elements of the Internet infrastructure.

Less conspicuously, the DDoS cannons continued to rumble on the cyber battlefield, as nation states continue to rely on it as an effective part of the hybrid war machine.

Unsurprisingly, the geographical profile of DDoS attacks continued to reflect the ongoing war in Ukraine and we even saw this spill over into neighbouring European countries – in particular Poland, the Baltic states, Sweden and Finland.

The global cybercrime fight-back intensified

In 2024, multiple international operations were launched to combat cybercrime - largely targeting criminal networks and dismantling illegal infrastructure. These efforts included takedowns of DDoS-for-hire services, ransomware groups and dark web marketplaces.

Enhanced legislative measures and cross-border collaboration played a key role in strengthening global cybersecurity and reducing the impact of cybercrime.

The rise of Anonymous Sudan

In 2024, Anonymous Sudan, a hacktivist group claiming to operate from Sudan, executed a series of high-profile cyberattacks. Their operations included over 35,000 distributed denial-of-service (DDoS) attacks targeting hospitals, cloud services such as Microsoft Azure, and platforms such as OpenAI's ChatGPT. These attacks caused widespread disruption and drew significant international attention.

The group often cite political and ideological motives, positioning themselves as defenders of Islamic values; though some experts speculated links to other geopolitical interests. Law enforcement agencies around the world intensified efforts to counteract their activities, leading to the indictment and arrest of suspected members by the end of the year.



New attack vectors identified in 2024

In 2024, **Imperva** identified two major application-layer DDoS attack vectors: **HTTP/2 Rapid Reset** and **HTTP/2 Continuation Frame Attacks**. These advanced techniques highlight the increasing sophistication of attacks.

These vectors exploit vulnerabilities in the HTTP/2 protocol to disrupt services and bypass traditional mitigation measures. They highlight once again the ever-changing nature of the threat landscape, and the need for robust cybersecurity strategies and counter-measures.

The DNS Amplification volume increased

Following a brief lull in 2022, we reported the return of DNS Amplification in 2023. Despite widespread efforts to secure DNS servers across the Internet ecosystem, this DDoS trend intensified in 2024 and had a major impact on the DDoS threat landscape as a whole. That said, this began to flatten out towards the end of the year.

Less Carpet Bombing Activity in 2024

Carpet Bombing activity dropped in 2024 which, given its effectiveness was something we didn't expect to see.

Big attacks became bigger, but not necessary longer

The average size of attacks almost doubled in 2024 but the average duration remained the same, which meant that attacks have become more intense. The ratio packet length increased which can largely be explained by the popularity of DNS-driven attacks.

Overall, there has been a strong 3-year increasing trend for average packet size (Gbps) and the sheer number of attacks, all of which call for sustained vigilance.

One of the largest attacks in 2024 targeted Cloudflare with a staggering 4.2 Tbps peak.

Increased use of AI in cyberattacks during 2024

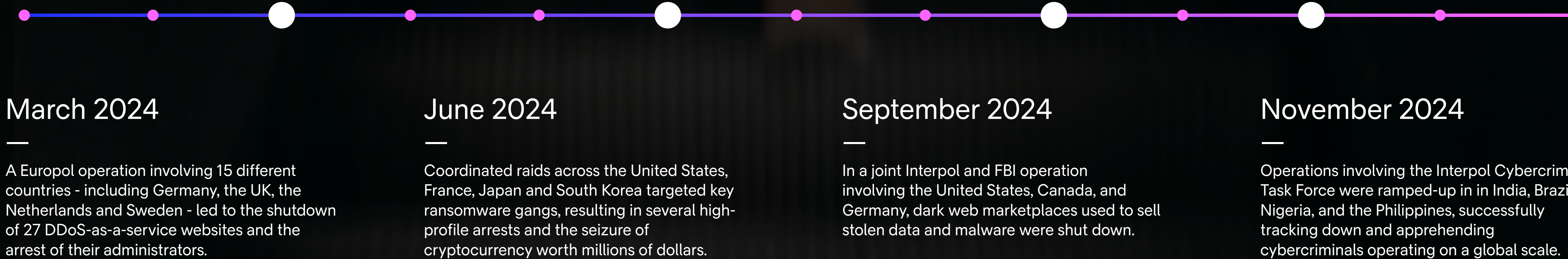
In 2024, we saw the increased application of artificial intelligence (AI) in the execution of attacks that are harder to detect and mitigate. Examples include the usage of AI to create highly personalized phishing campaigns, automate vulnerability exploitation and circumvent traditional security measures.

This highlights an urgent need for advanced AI-driven defenses to counteract increasingly complex cyber threats. A tangible example of this is where a **ChatGPT crawler can be triggered to attack a victim's website via an HTTP request to an unrelated ChatGPT API**:

<https://github.com/bf/security-advisories/blob/main/2025-01-ChatGPT-Crawler-Reflective-DDOS-Vulnerability.md>



Major anti-DDoS operations in 2024



DDoS in 2024: the numbers

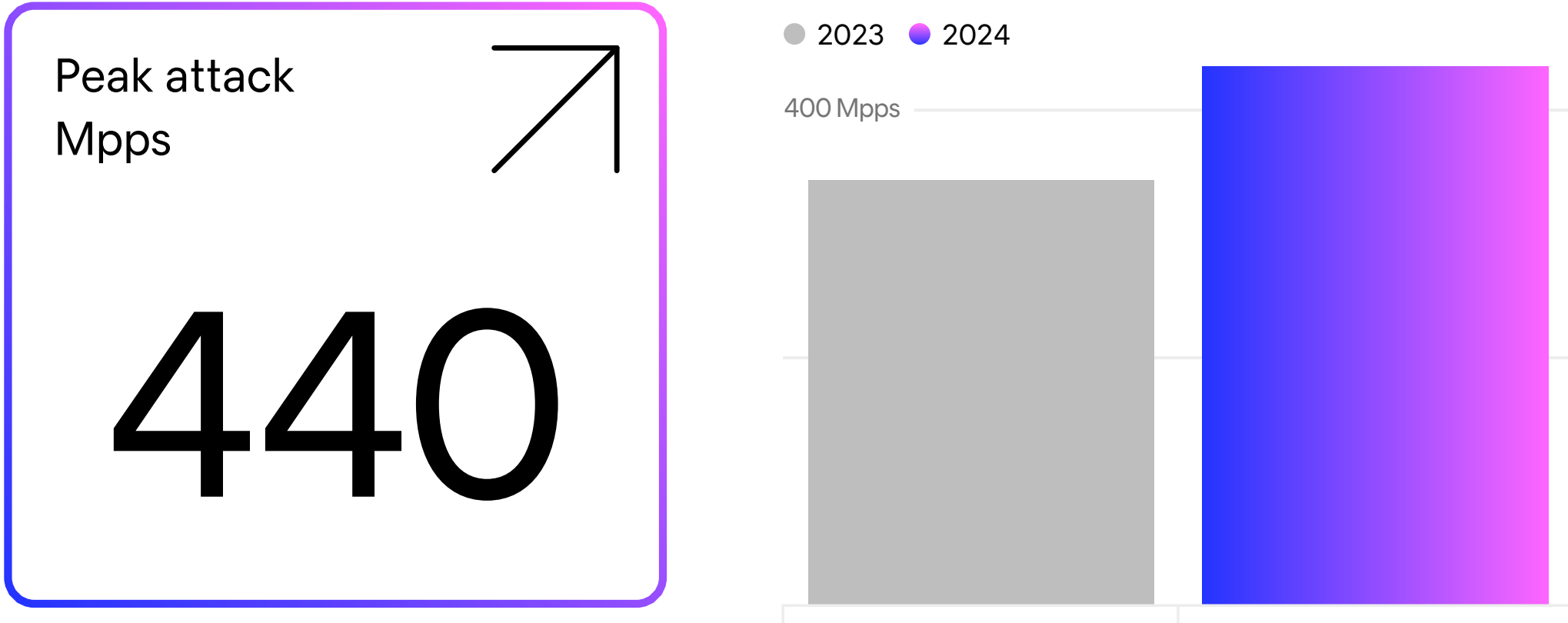
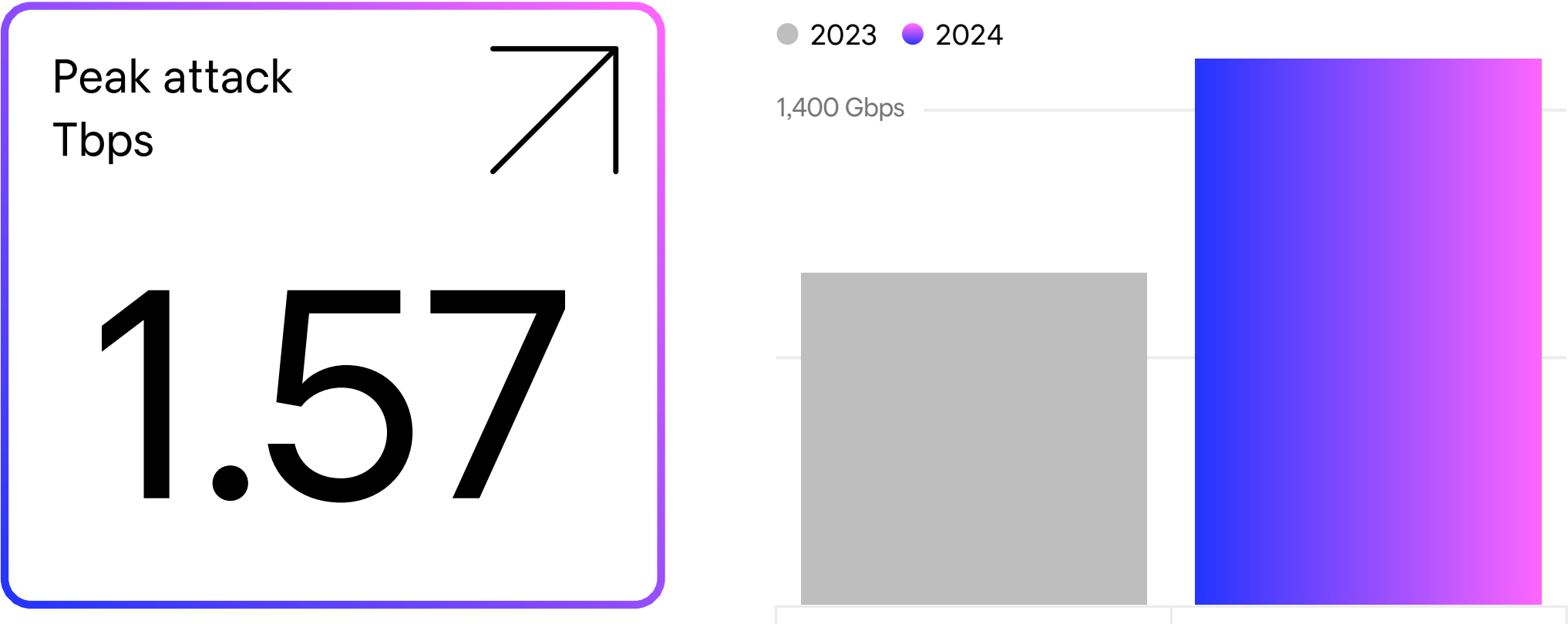




Overall DDoS network impact & peak attack traffic

The largest volumetric attack hit 1.57 Tbps in Oct 2024 (up 63% from 2023). This was driven by TCP SYN and DNS Amplification traffic towards US cloud providers

In terms of packets-per-second, the largest peak reached 440 Mpps in Aug 2024 (up 28% on 2023). This was largely driven by UDP flood attacks towards Asian gaming sites.

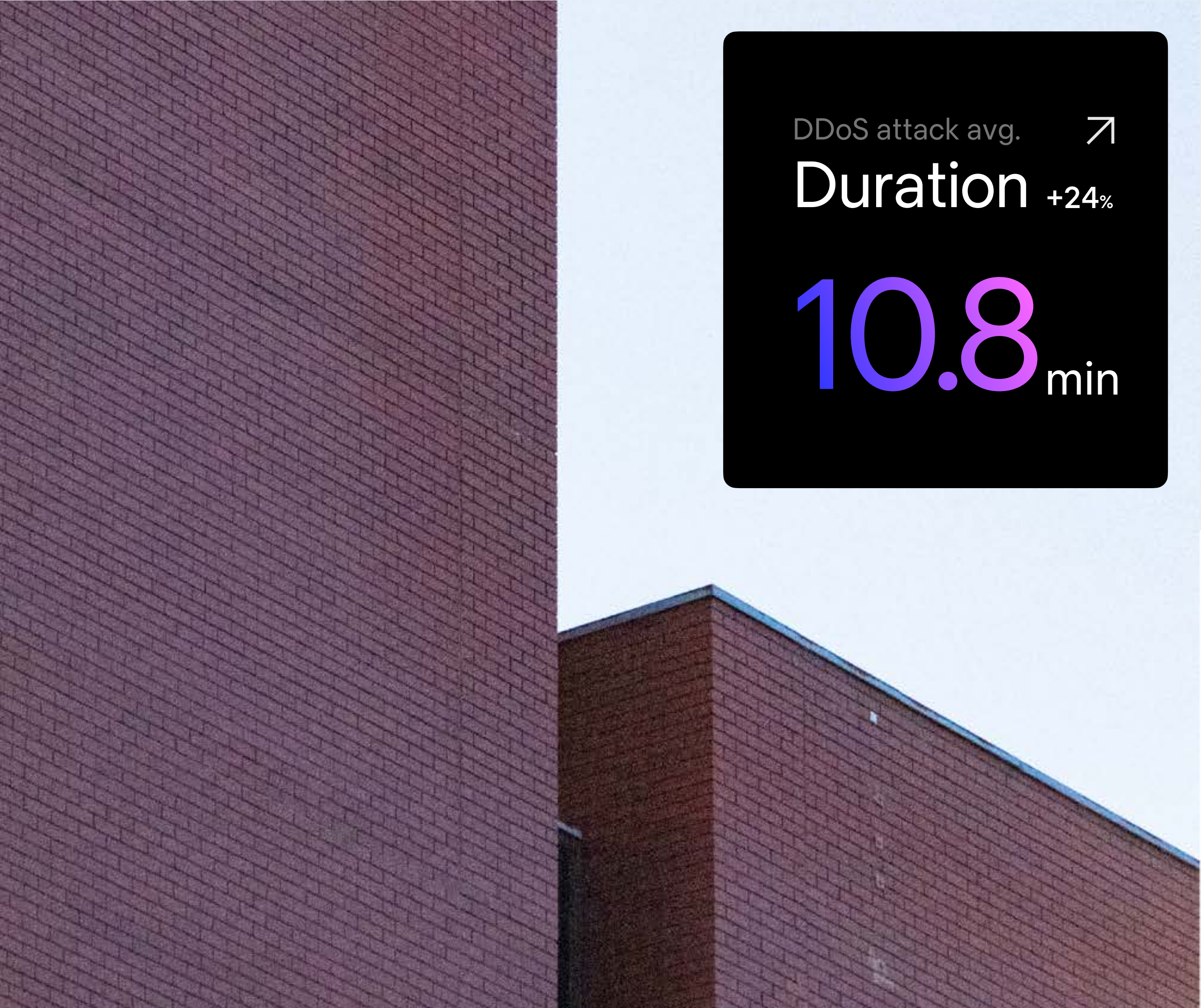




Average attack size and duration

The average volumetric attack size in 2024 was 23.0 Gbps – an increase of 97% from 2023. In terms of packets-per-second, the average size reached 6.2 Mpps, up 24% from 2023.

The average duration of attacks also increased by 24% in 2024. This relatively modest increase is believed to be the result of fewer Carpet Bombing attacks.



DDoS attack avg. ↗

Duration +24%

10.8 min

DDoS attack
average size ↗
+97%

23 Gbps

DDoS attack
average size ↗
+24%

6.2 Mpps

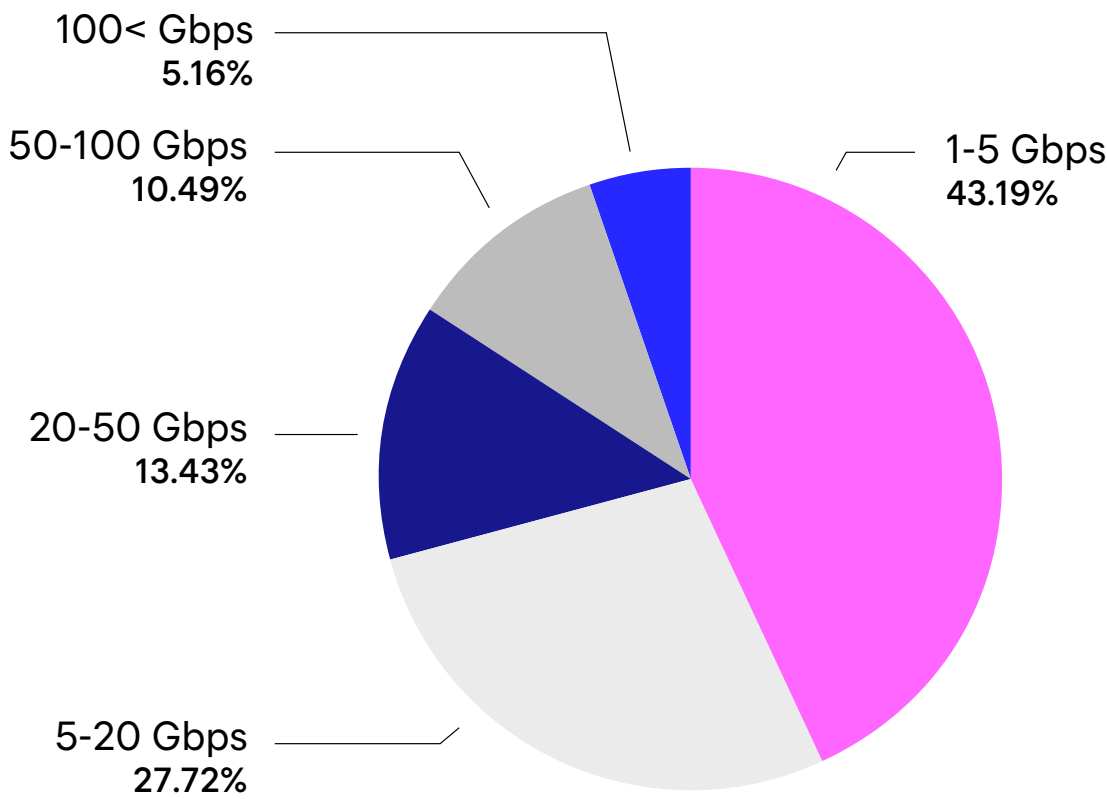


Attack size distribution

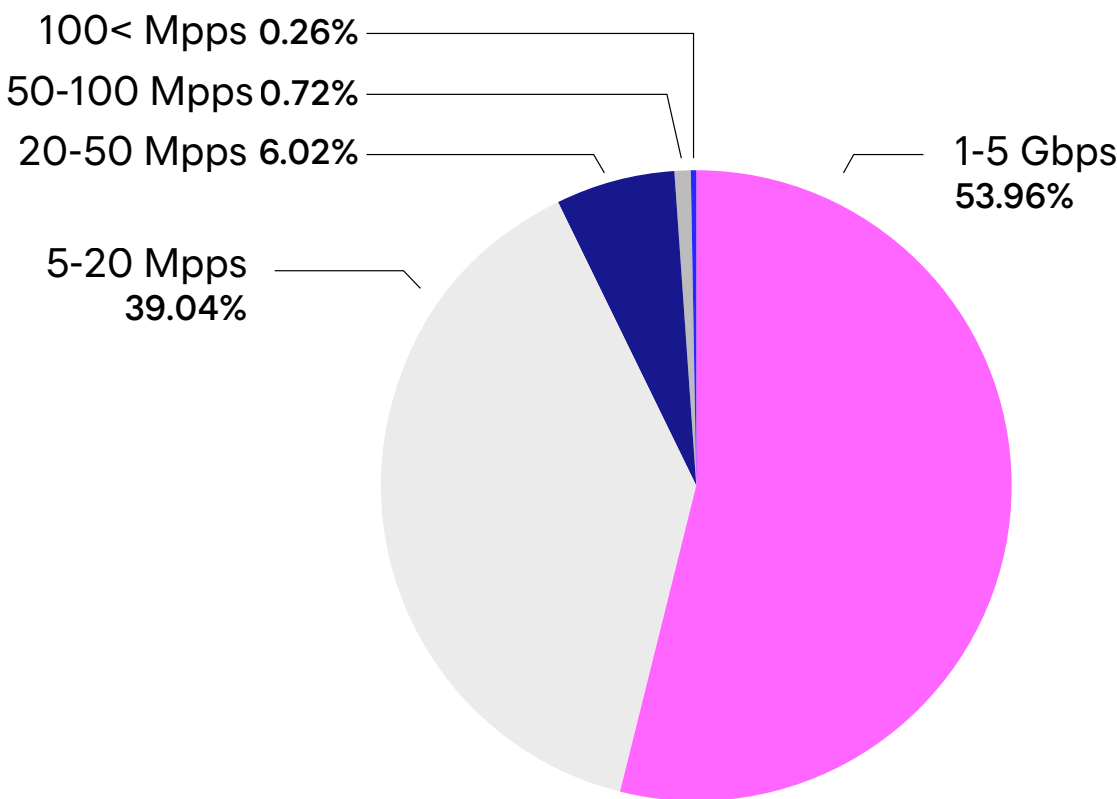
In 2024, attack duration was largely the same as 2023. Like attack size, volumes were also driven by DNS Amplification; with more attacks in the mid to upper ranges, and fewer smaller attacks. The same can be said for packet-per-second attacks where the midrange saw the greatest increase.



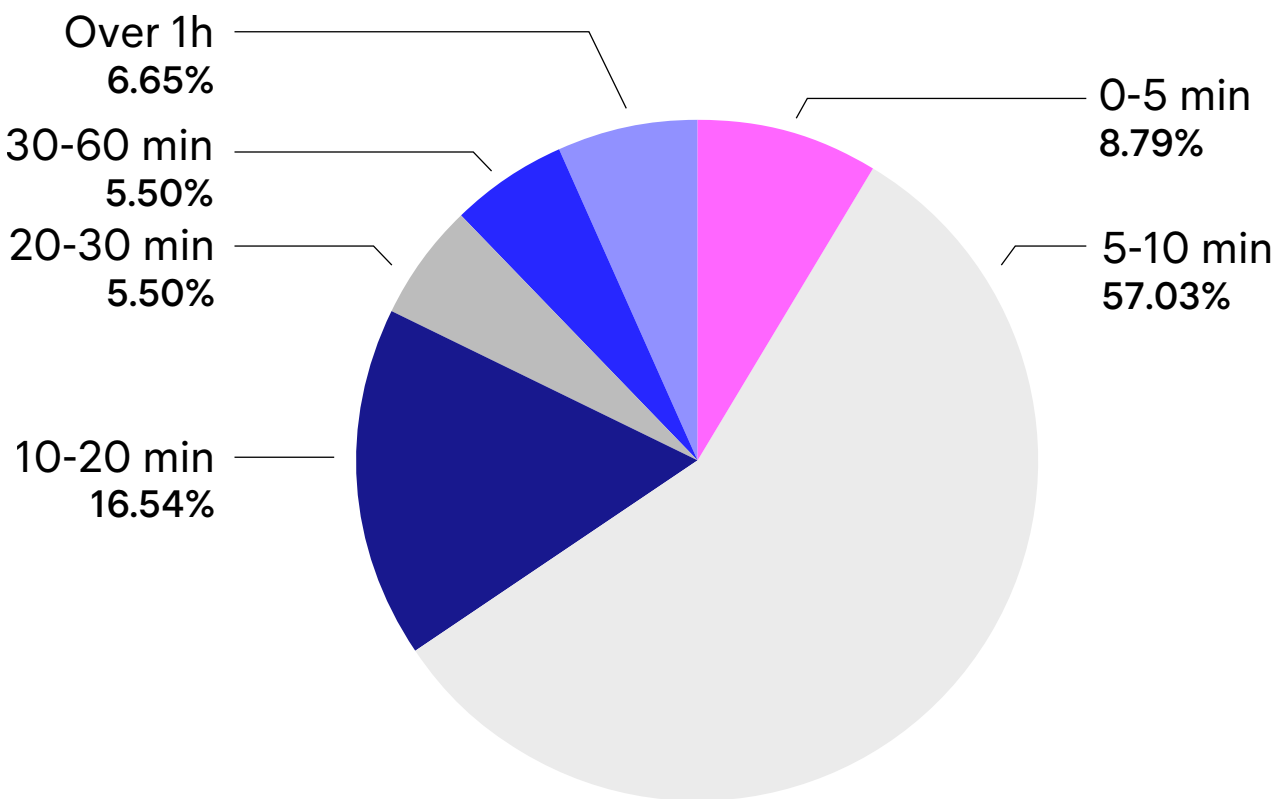
DDoS attack size Gbps



DDoS attack size Mpps



DDoS attack duration



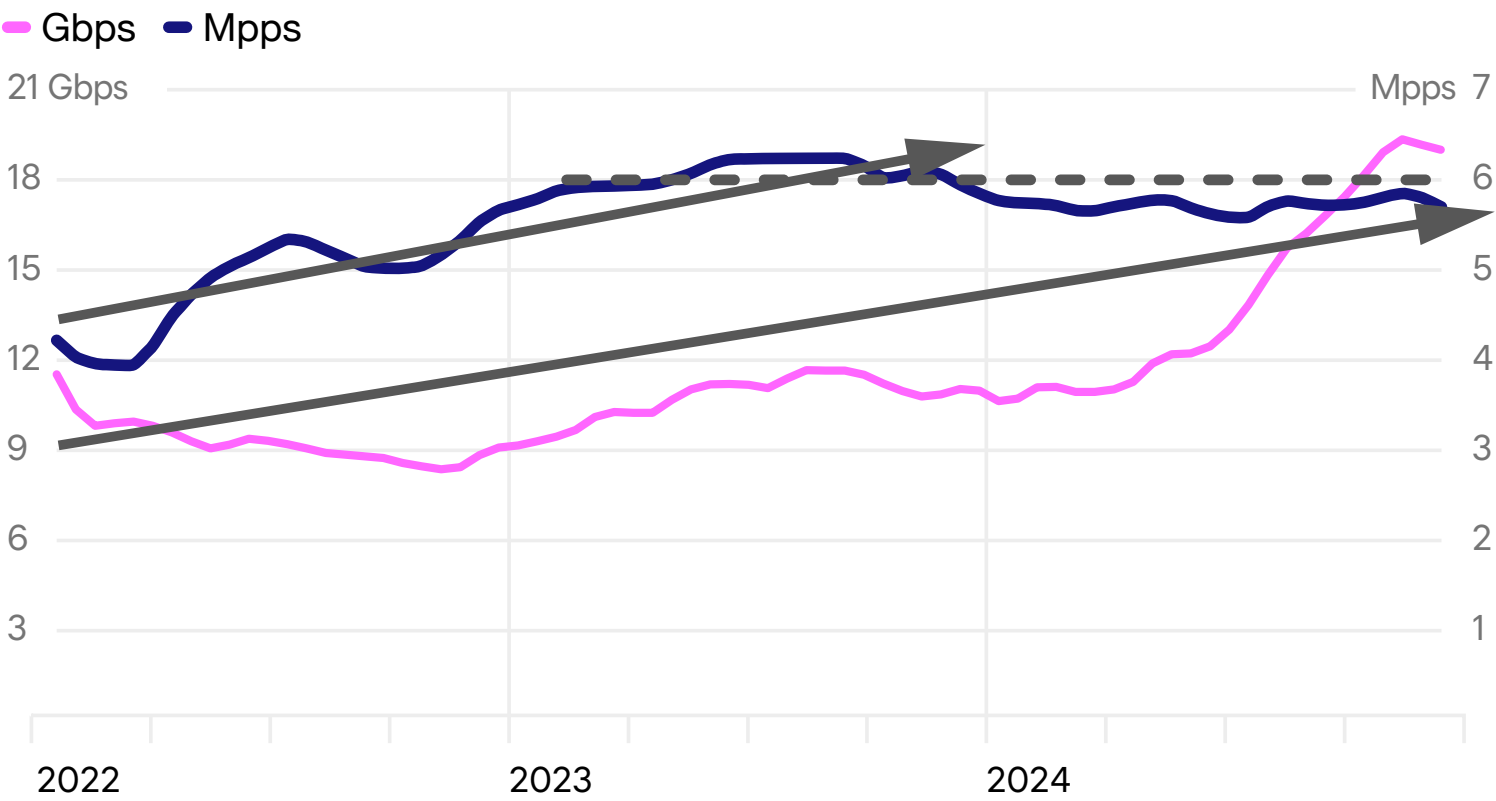


Attack strength and duration over time

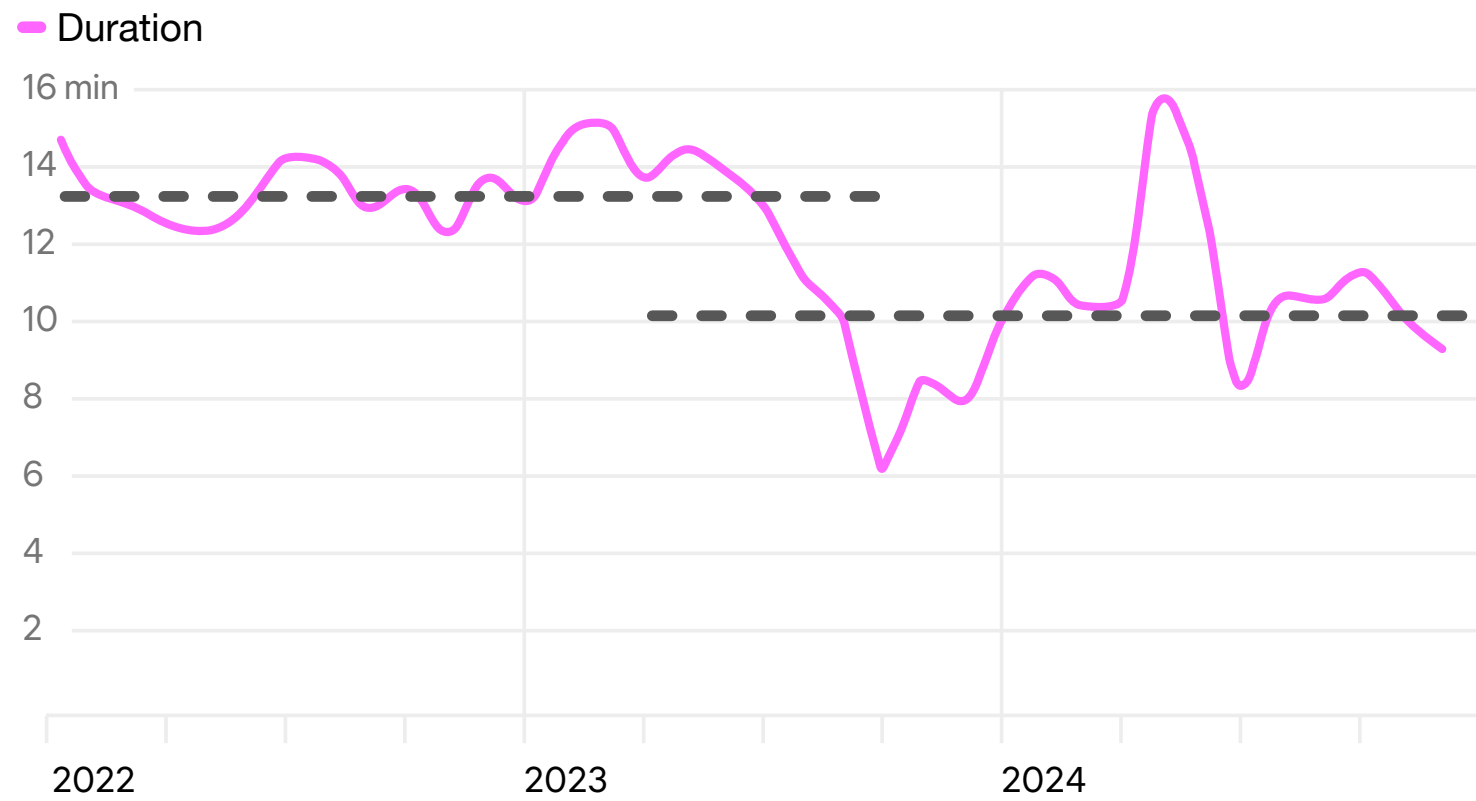
Strong Gbps 3-year growth. Attack strength in Mpps levelled out from the peak seen in late 2023. Attack duration remained at the same level as the second half of 2023. The overall number of attacks has increased significantly over the past 3 years, confirming that DDoS is not going away - far from it.



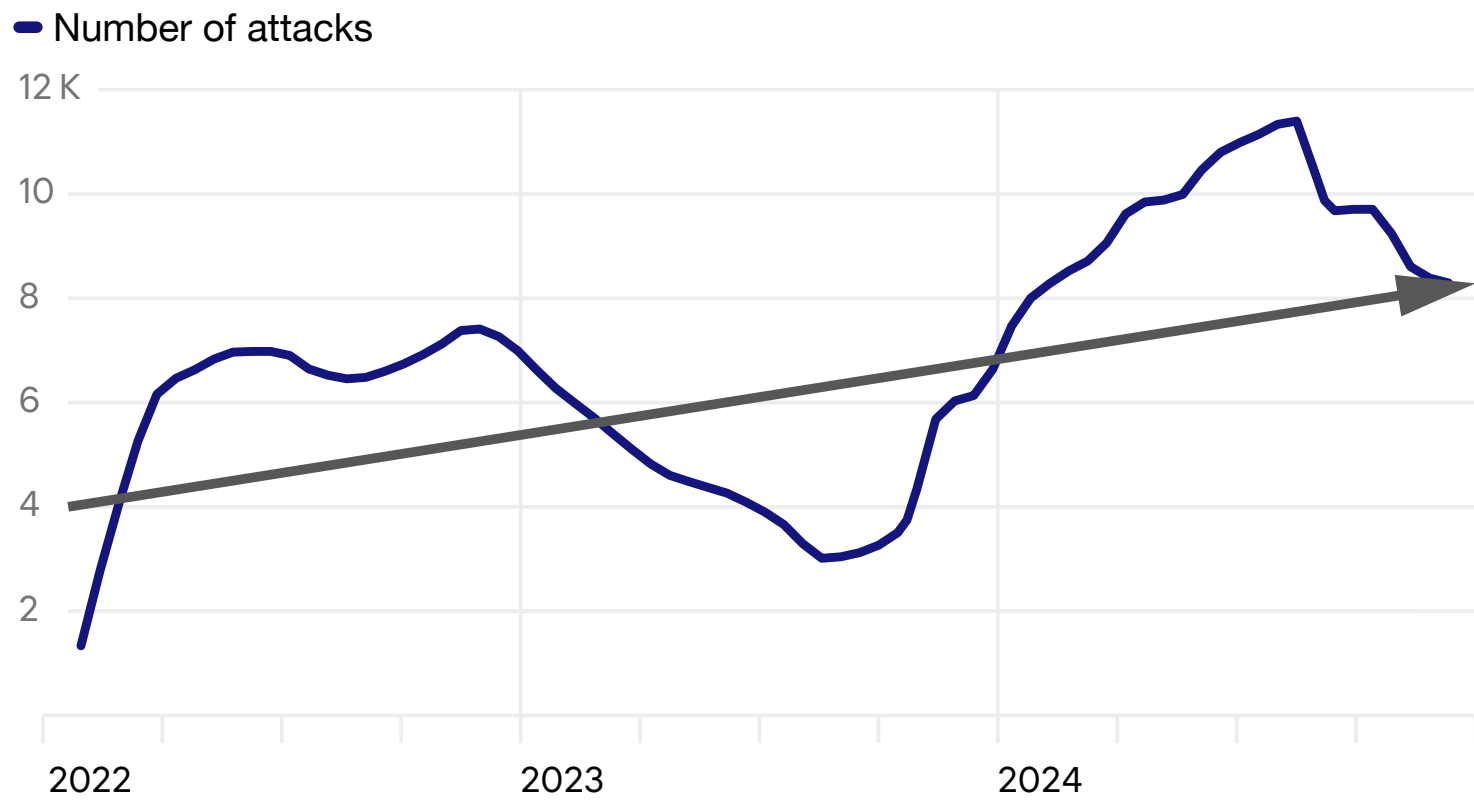
Average DDoS attack size

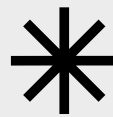


Average DDoS attack duration



Number of DDoS attacks





2024 customer DDoS attack distribution in AS1299

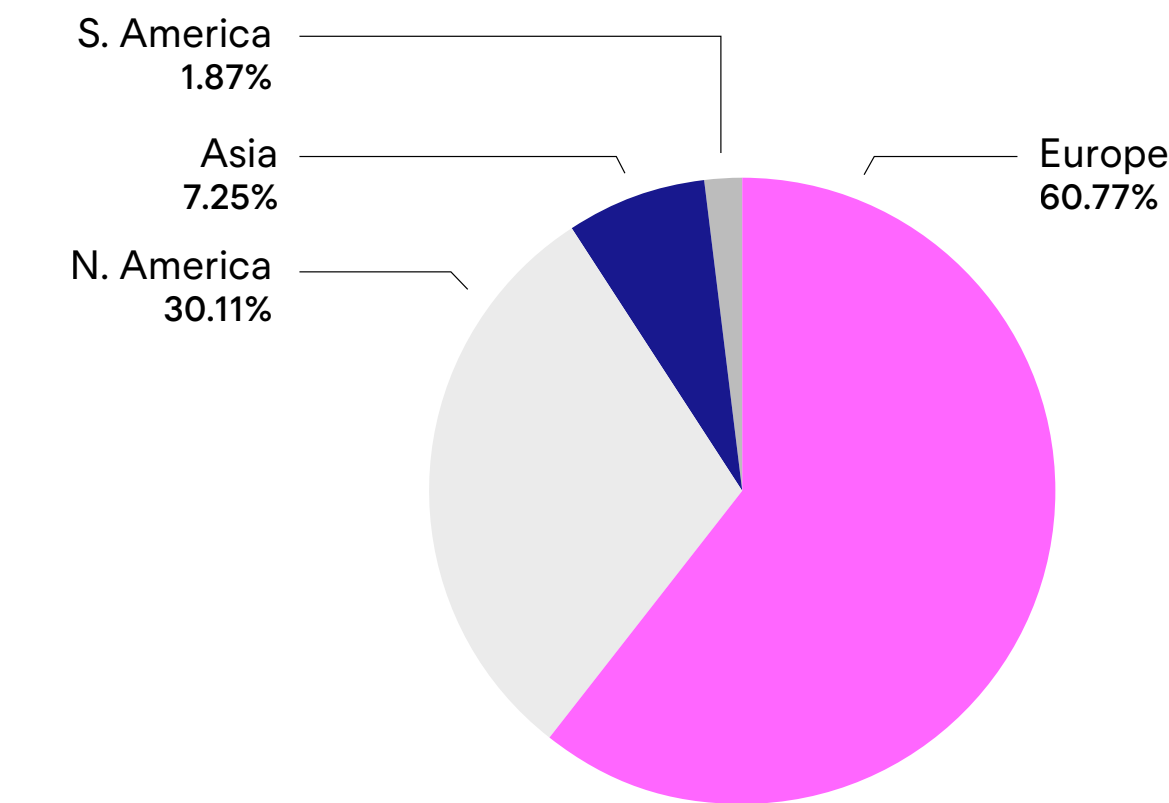
For our customers, we observed that most attacks affected Europe but with less impact on Poland than in 2023. Our customers in Sweden, Germany, and France were the most affected:

- **Sweden:** (a NATO member since March 7, 2024) 2.5x more attacks than 2023, particularly in the banking sector.
- **Germany:** 3x more attacks compared to 2023.
- **France:** 5x more attacks compared to 2023.

From what we can see, this appears to be the proliferation of DDoS attacks related to the Ukraine war into neighbouring countries allied to the Ukrainian cause.

- **Martinique:** despite being a small region, Martinique stands out in North America, perhaps indicating a targeted approach by attackers who are possibly exploiting its connection to France and its governmental data vulnerabilities.

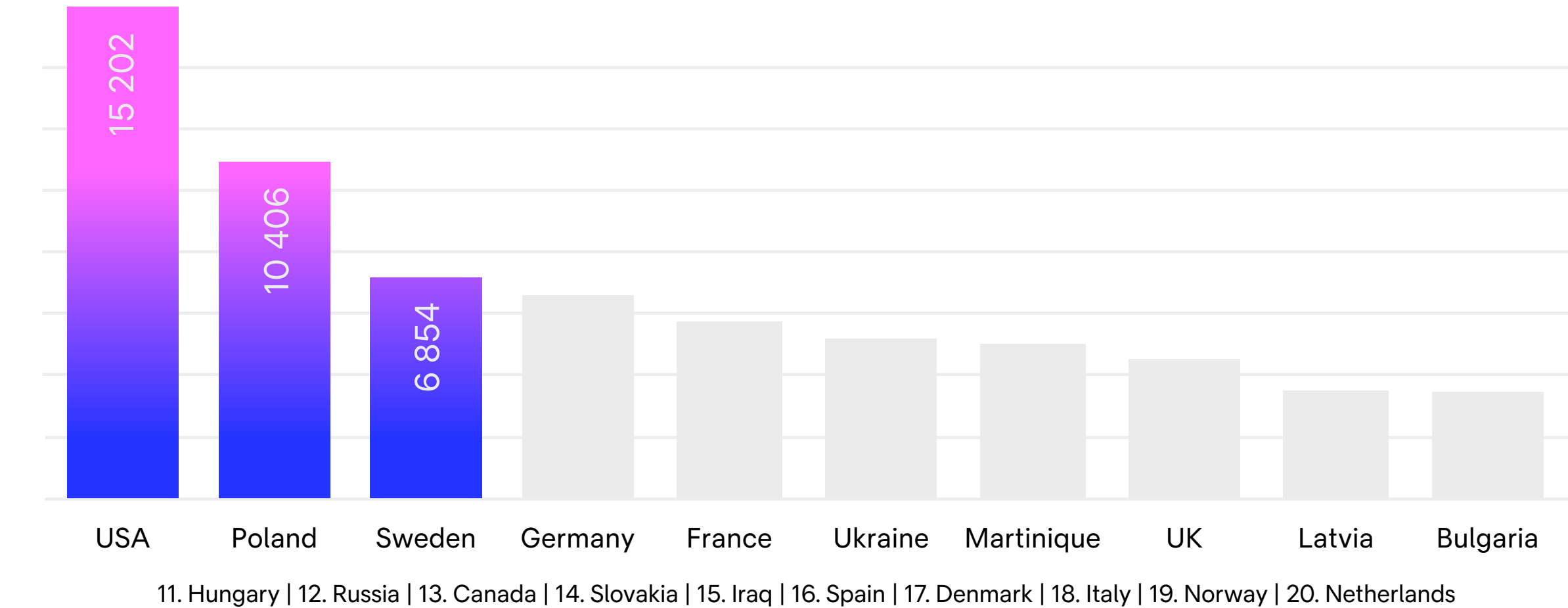
DDoS attack size Gbps



Top 5 attacked country per continent

Europe		N. America	
Poland	21%	USA	61%
Sweden	14%	Martinique	19%
Germany	12%	Canada	9%
Ukraine	11%	Costa Rica	3%
UK	10%	Guatemala	3%
Asia		S. America	
Iraq	35%	Colombia	72%
Singapore	18%	Ecuador	14%
China	13%	Brazil	7%
Japan	12%	Argentina	3%
Mongolia	6%	Fr. Guiana	2%

Top 10 attacked countries

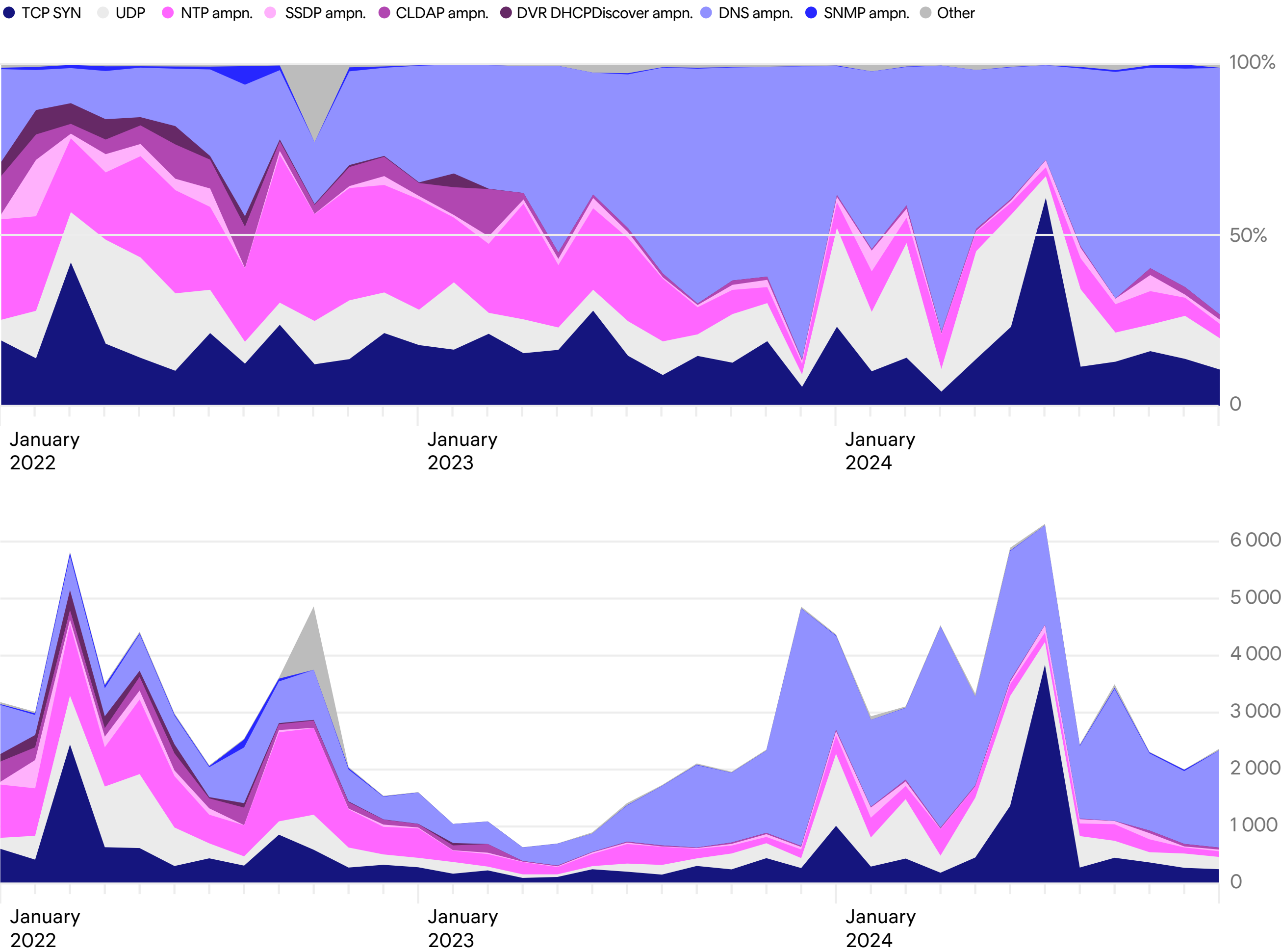




How our DDoS customers are being attacked?

Looking at our DDoS protection customers, DNS Amplification was the main DDoS attack vector in 2024 and following some extreme peaks in late 2023, this levelled out to 55% of all traffic during the year. SYN and UDP attacks were in second and third place, respectively.

Attack type (percentage & total numbers)



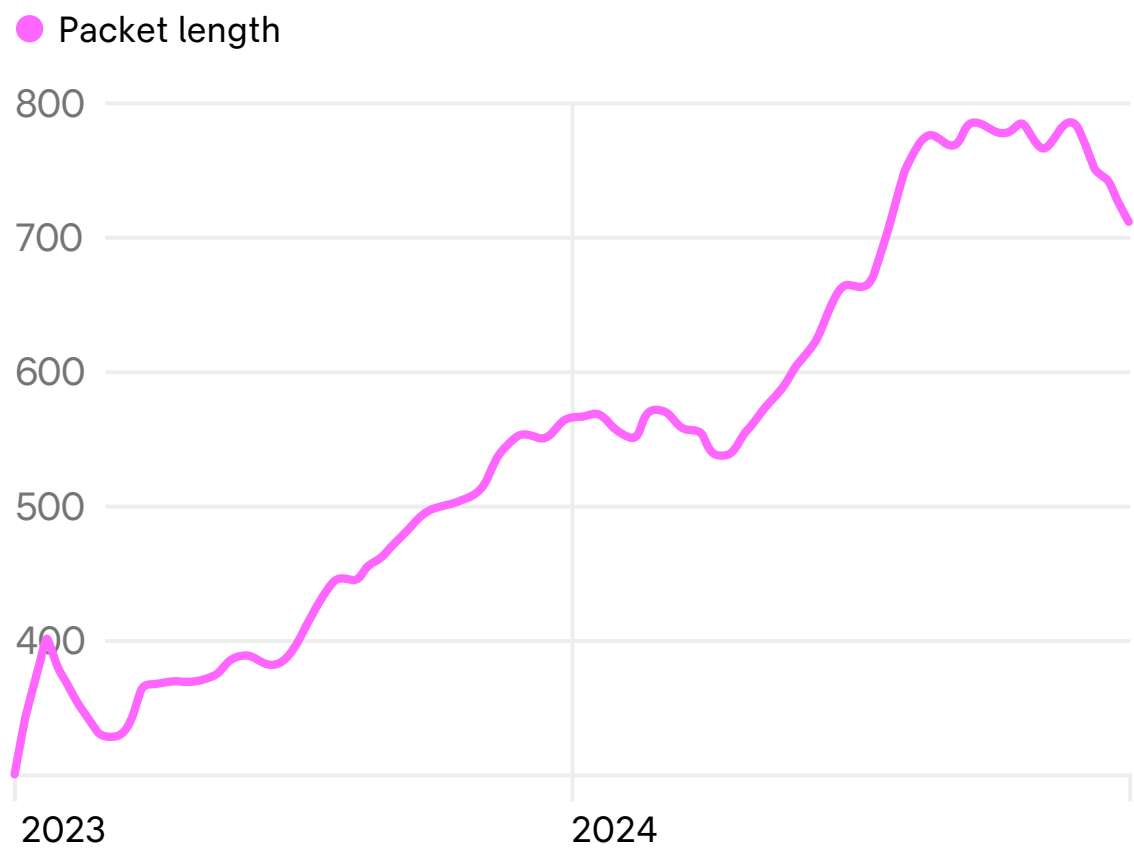


The impact of DNS Amplification in our network

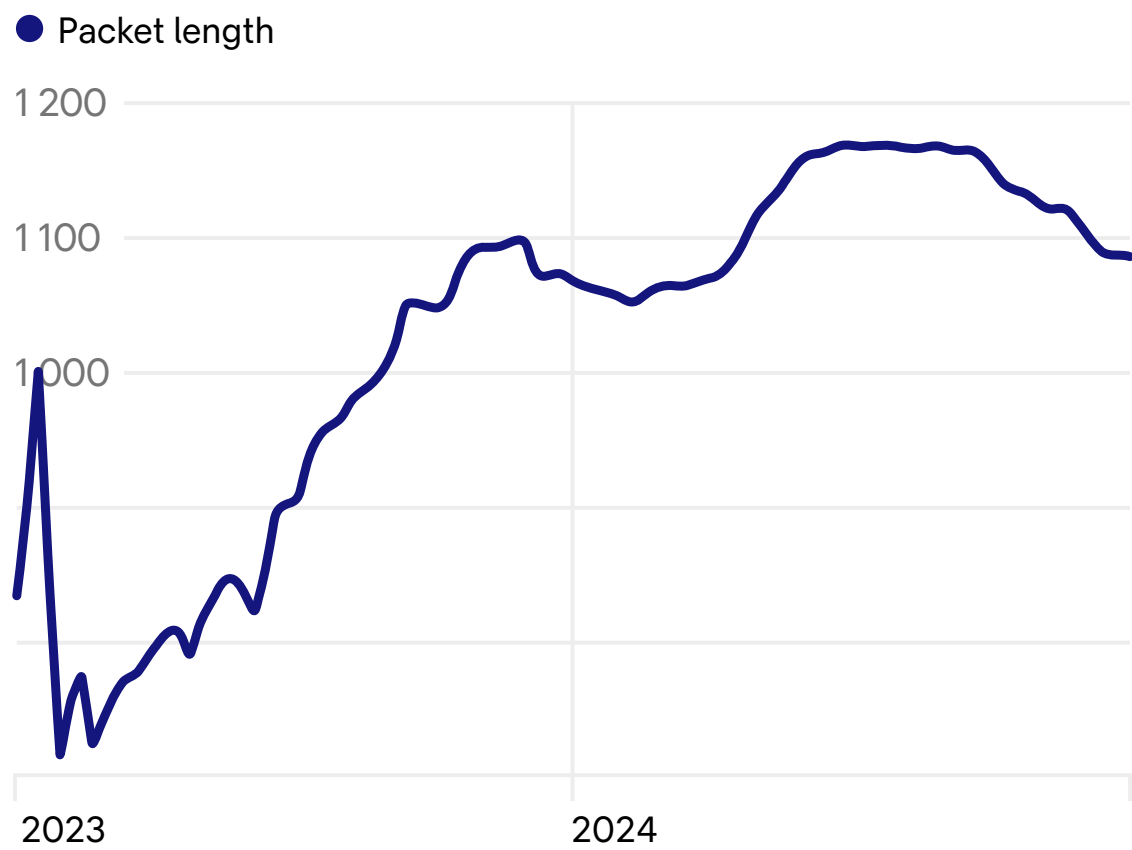
Despite tailing-off towards the end of 2024, average packet length has doubled from approx. 350 to 700 Bytes over two years. This is largely driven by DNS Amplification.

Following explosive growth in 2023, DNS Amplification attack length flattened out towards the end of 2024. This can largely be attributed to the fact that the efficiency of the technique used to misuse protocol characteristics has peaked.

Attack average packet length



DNS AMP attack average packet length





Why has DNS Amplification become so prolific?

Due to their ubiquity and a toxic combination of misconfiguration, default settings, and the inherent nature of the DNS protocol itself, Open DNS service ports are frequently used for DNS amplification attacks.



The enablers include:

1. Default open configuration

Many DNS servers, especially those configured for recursive resolution, are left open by default. System administrators may fail to restrict access to trusted IP ranges or disable recursion for unauthorized users.

2. Inherent UDP protocol weaknesses

DNS queries ordinarily utilise the User Datagram Protocol (UDP), which is a connectionless protocol where small queries can create larger responses. By exploiting this, attackers can easily spoof source IP address and amplify the traffic directed towards a specific target.

3. Ease-of-use and server mismanagement

DNS is a fundamental pillar of the Internet, with many systems relying on it for basic network functionality. To avoid disruption, administrators may neglect to properly secure DNS servers, or there may simply be insufficient understanding or awareness about DNS security best practices .

4. Effective amplification

DNS amplification attacks exploit a fundamental flaw in DNS queries – in particular, those requesting DNSSEC records or ANY queries. The result is a significantly greater response than the original request. Attackers send these queries using the victim’s IP address as the source, in turn flooding the victim with an amplified response.

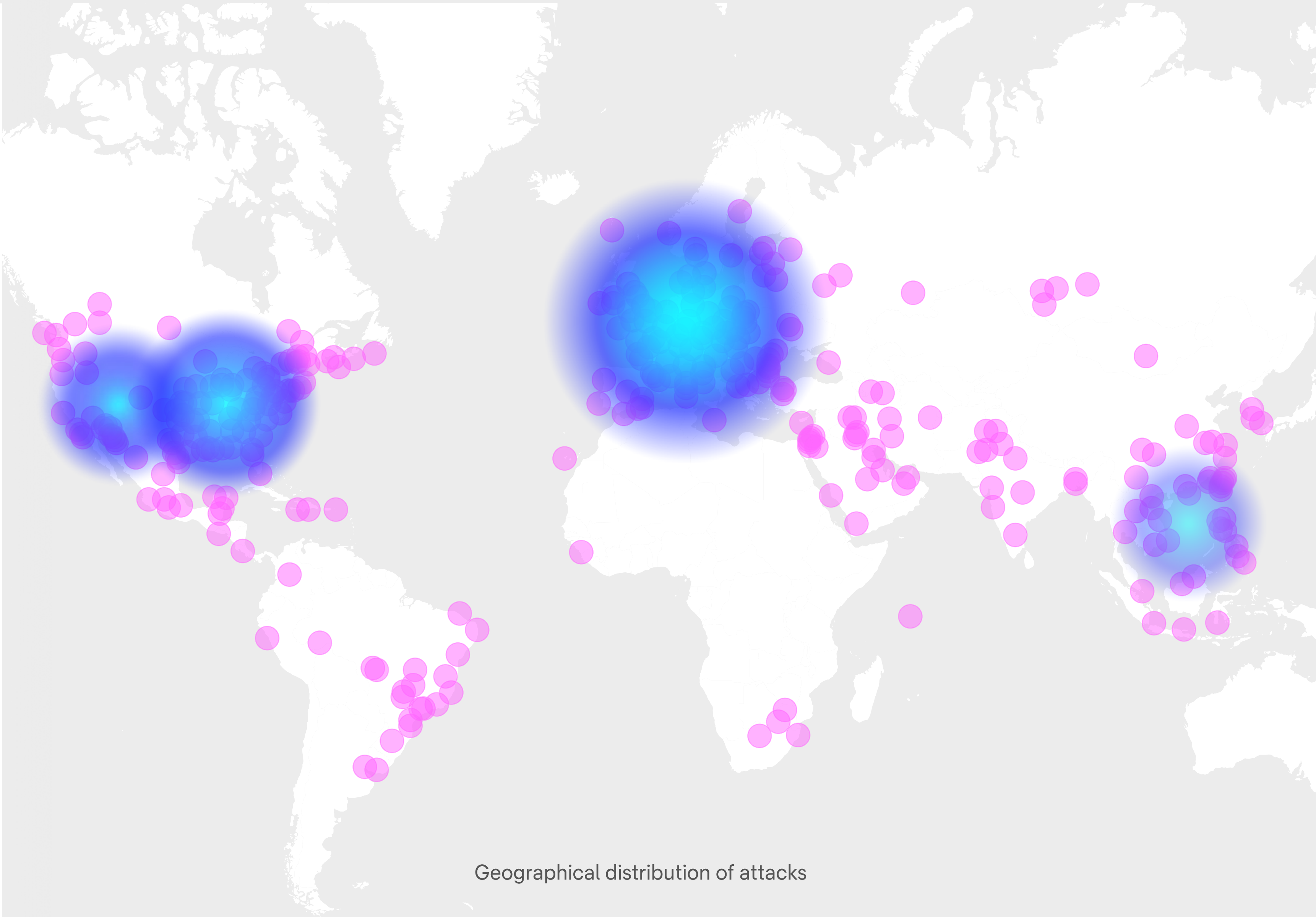
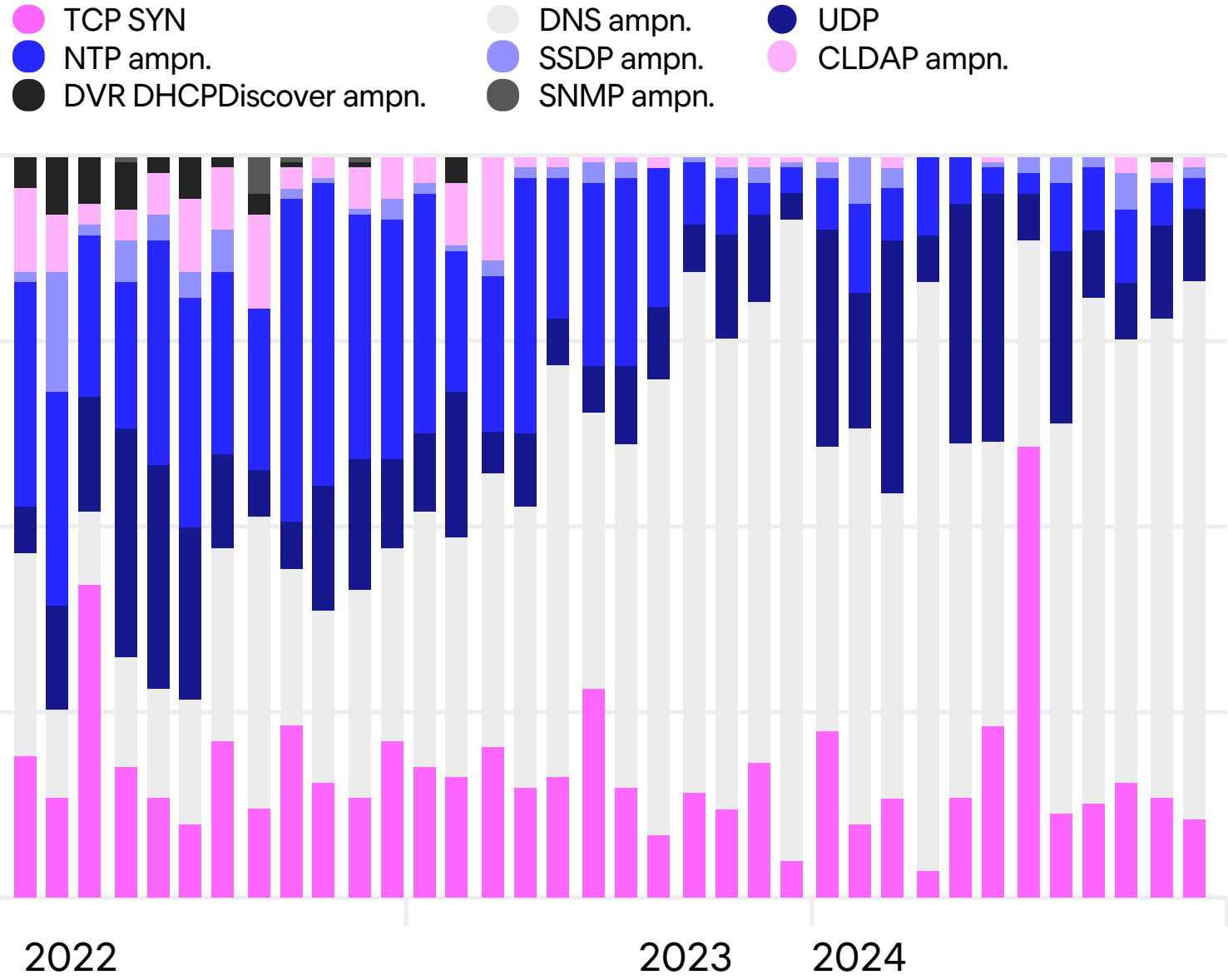
5. Legacy server vulnerabilities of hardware

Older or unpatched DNS servers may be open to abuse. Unfortunately, these systems often remain inadvertently exposed to the Internet.



The global picture in AS1299

Looking at all traffic in AS1299, we saw a pretty even spread of attacks across North America, Europe and Asia, with the United States seeing the greatest intensity of DDoS activity.



Geographical distribution of attacks



Global attack trends

When it comes to global attack vectors, SYN, UDP and NTP amp were the most common in 2024. Though it needs to be remembered that we are monitoring the bigger attacks and that this is also a reflection of the type of company buying our DDoS protection service - generally larger wholesale and enterprise networks.

- SYN and UDP are the top attack vectors
- There is an even continental spread across North America, Europe, and Asia when compared to 2023.
- South America is still very low. Panama was a very local phenomenon last year, and Brazil also remains low.
- We didn't see any major DDoS attacks during the US election., nor did we observe any volumetric DDoS attacks globally related to the 2024 'super election year'. This could indicate either improved cybersecurity measures or a strategic shift by attackers to focus on other targets.

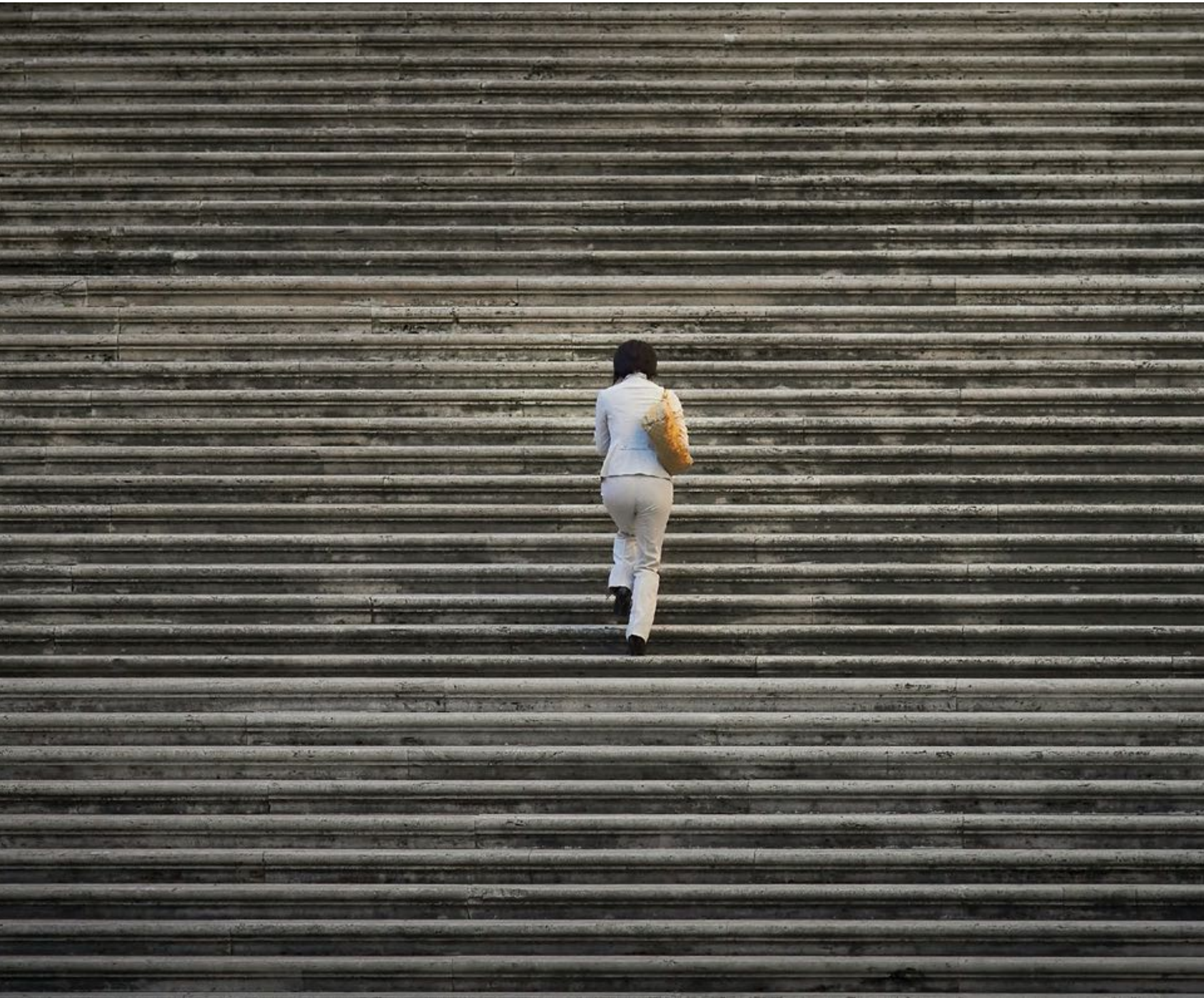
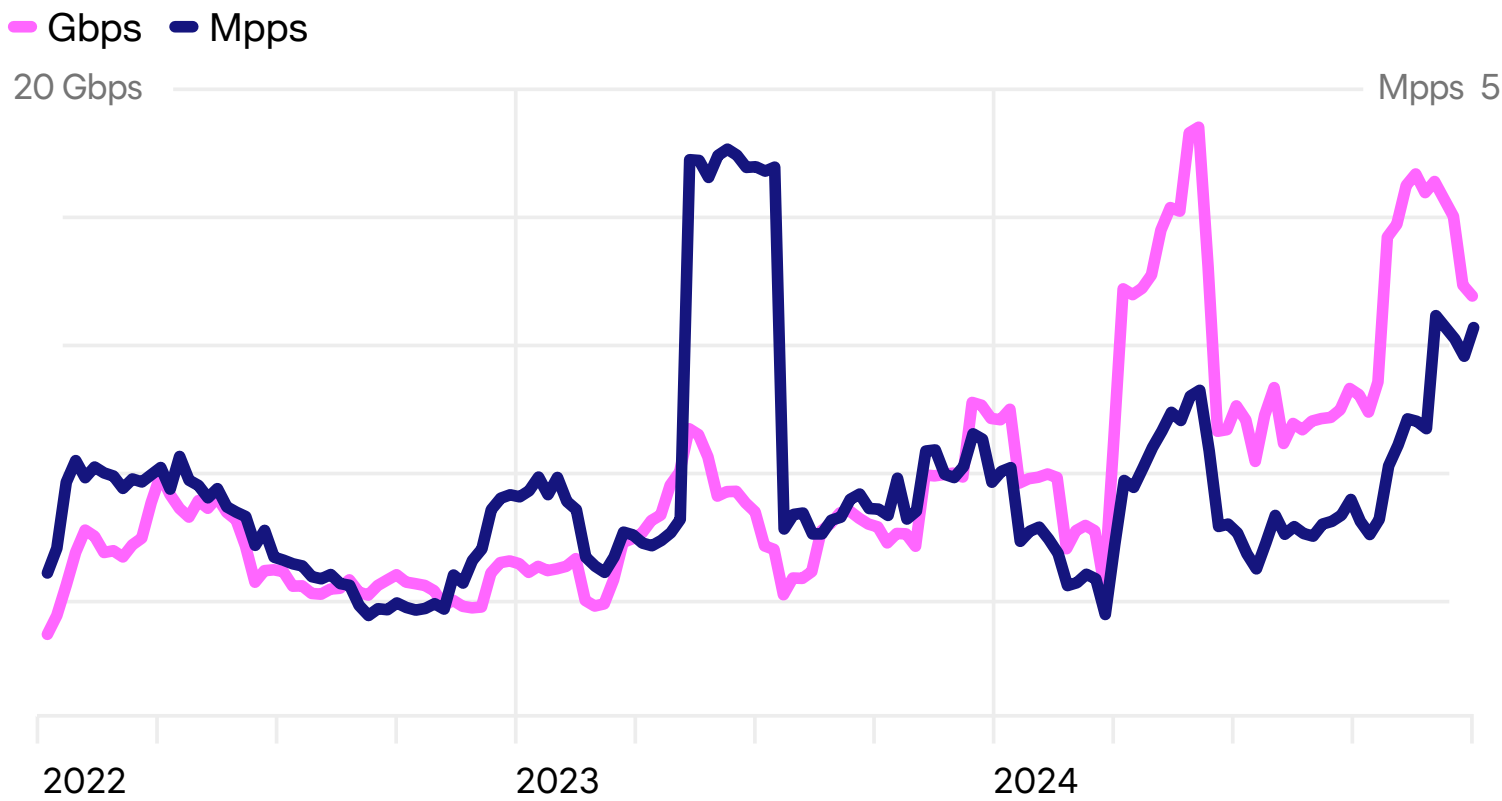




DDoS attacks and hybrid warfare

DDoS continues to be a critical weapon in the hybrid warfare arsenal. In 2024, there was an increasingly physical component to cyber warfare, with a number of submarine cables damaged as a result of suspected sabotage. DDoS attack strength continues to escalate over time – both in terms of average Gbps and Mpps.

Average DDoS attack size per week



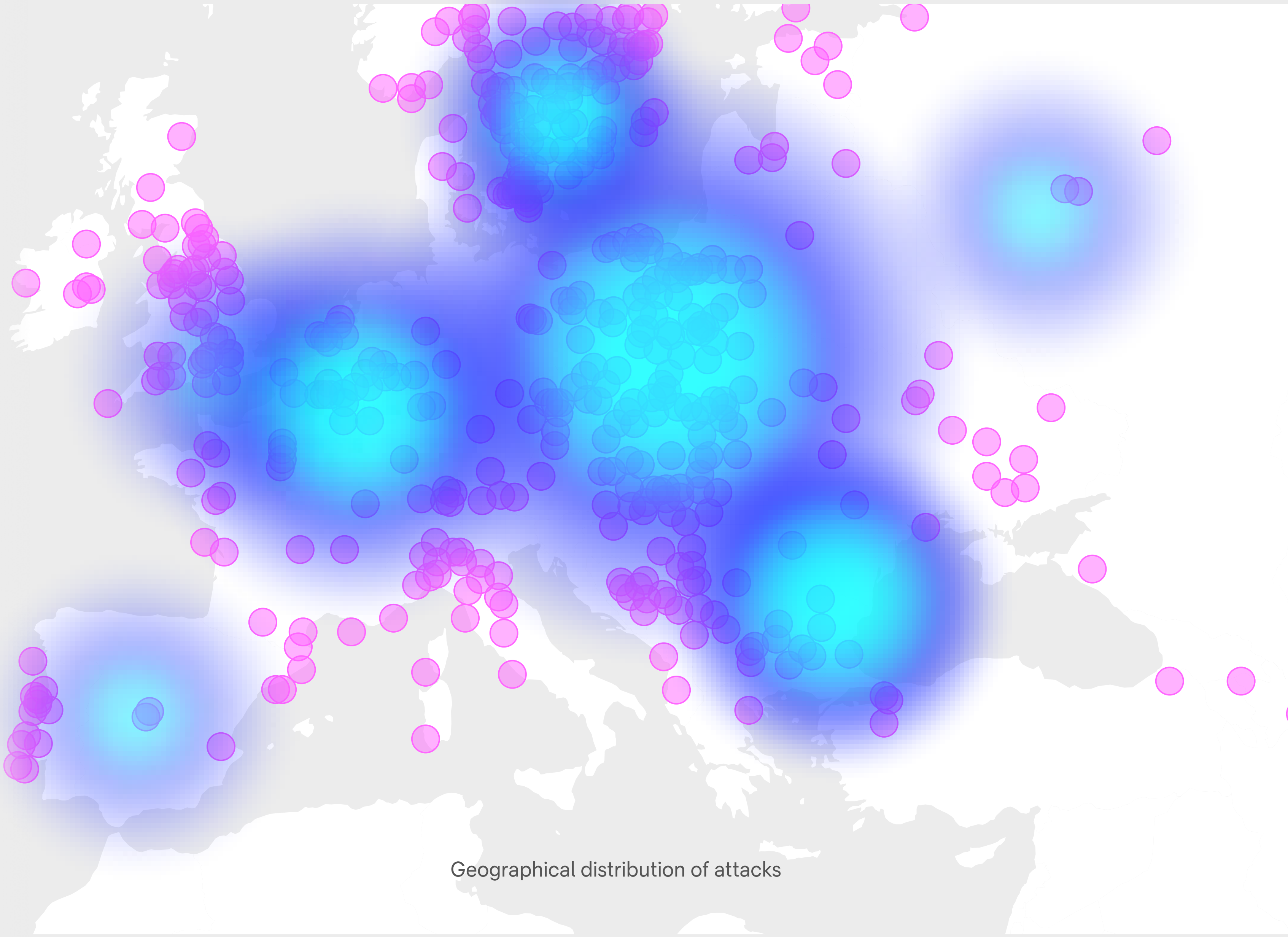


DDoS attacks and hybrid warfare

—

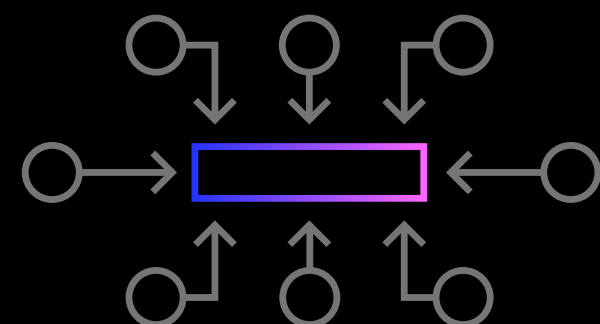
In Europe, there is DDoS spillover from the Ukraine conflict into neighboring countries, with Poland being the second most attacked country globally, and Ukraine in fifth place.

This is most likely a consequence of the ongoing hybrid attacks against NATO countries and the allies of Ukraine in Europe.





Glossary and terminology



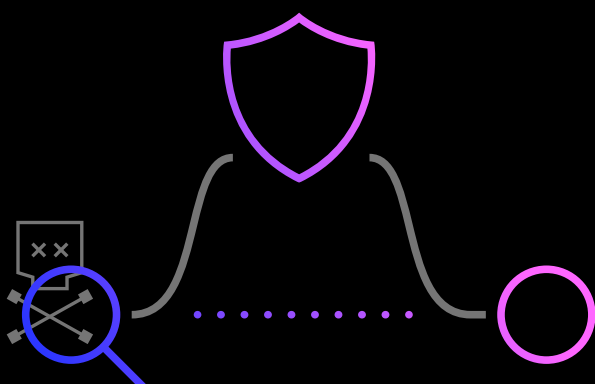
Attack vector

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.



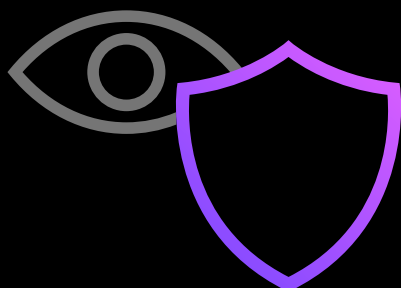
DNS Amplification

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.



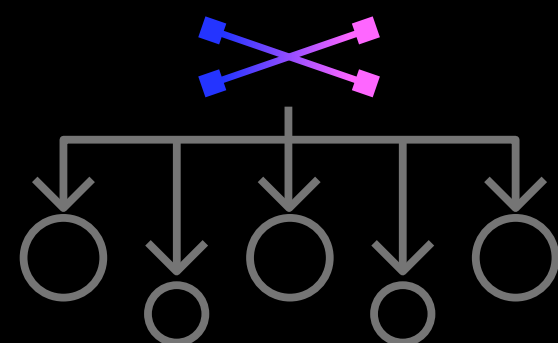
Auto-mitigation

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.



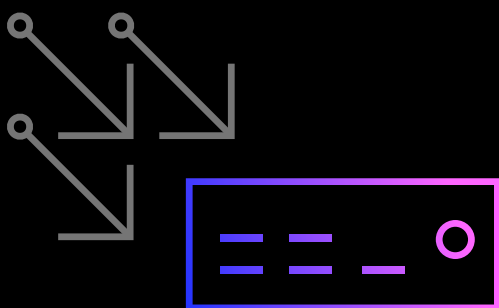
Carpet Bombing

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.



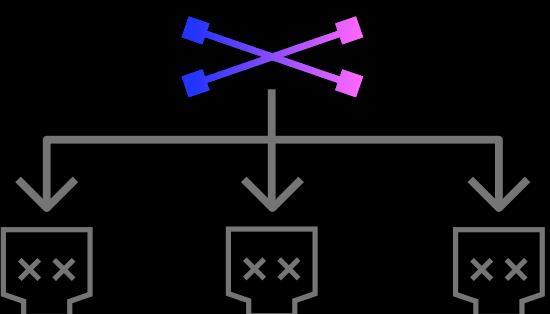
NTP Amplification

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.



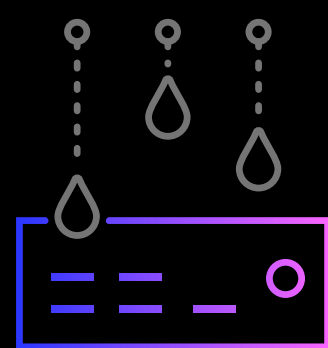
SYN attacks

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.



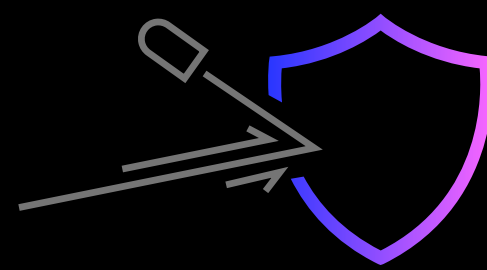
DDoS-as-service / Botnets

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.



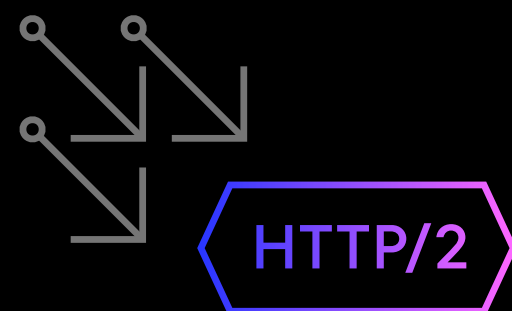
DNS Water Torture Attack

As the historical torture method of dripping water onto a person's forehead, this type of attack incessantly "drips" requests for non-existent records onto the DNS server, gradually exhausting its resources, causing slow and agonizing disruption for the infrastructure.



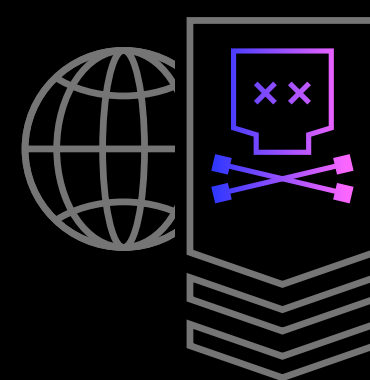
Bulletproof hosting

Refers to a type of web hosting service that allows customers to host websites and other online content without strict oversight or regulation. These services are often associated with illegal activities such as spamming, malware distribution, phishing.



HTTP/2 attacks

An exploit of vulnerabilities in the HTTP/2 protocol to disrupt web server operations or compromise data integrity. These attacks can include resource exhaustion, protocol manipulation, or exploiting implementation flaws.



Cyber warfare

Malicious cyberattacks between conflicting nation states, aiming to cause comparable harm to actual warfare and/or disrupt vital computer systems and network infrastructure. Intended outcomes include espionage, sabotage, propaganda, manipulation or economic warfare.



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 77,000 km of optical fiber and customers in 128 countries. 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 [X \(formerly Twitter\)](#)

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, 2025. All Rights Reserved.