

Key backbone security trends

DDoS threat landscape report 2024



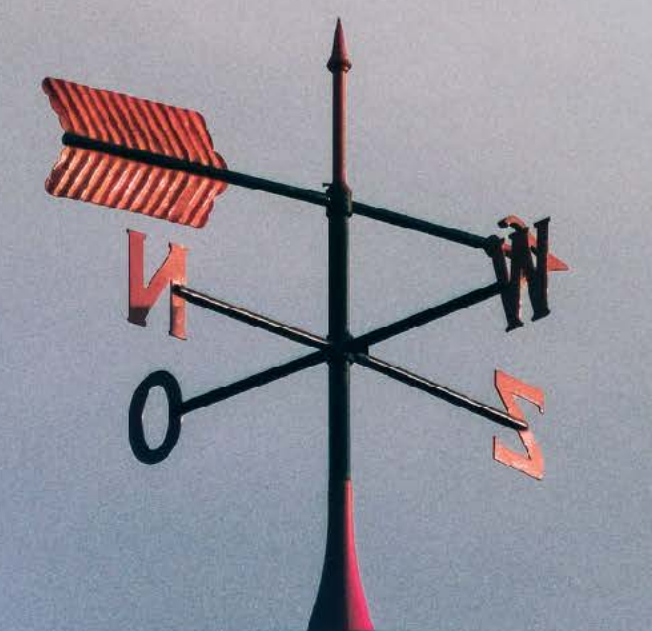
Unique insights from the core of the Internet

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 2023 – 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.

Has the cyber- power balance shifted?

As network owners strengthen their defences, cyber attacks keep evolving and peak attack traffic continues to grow.



Key insights and trends 2023





The big attacks just get bigger

Peak attacks continue to grow

Peak attacks reached 960Gbps in 2023. This demonstrates the continued importance of volumetric protection.

Attacks of this size are enough to bring down many larger networks, let alone an on-prem device, which even if mitigated, would most likely break the network it is attached to.

Global decrease in large volumetric DDoS attacks

Although we've seen a global decrease in large volumetric DDoS attacks of late, we've also noticed an increase in these locally – on a national level. This we think is the combination of many factors.

Large amplification attacks are now harder to carry out successfully, especially in view of recent cooperation across our industry. Enabling anti-spoof filters has forced the attacker to use a "direct-path" when exploiting their botnets. This limitation makes detection easier and these attacks much more vulnerable to take-down initiatives. As a result, cyber criminals need to be more careful and choose wisely when using attack resources.

Overall decline in packets-per-second

It seems that hackers are increasingly working "smarter not harder". As DNS amplification has improved, fewer packets-per-second are needed for an effective attack, which is one less thing that could trip the existing defences of an organization.

Attack duration is down

But this doesn't mean attacks are less serious. Larger, more intensive attacks over slightly shorter periods ultimately cause the same damage overall. From the data we've observed, it appears that average duration is being dragged down by unsuccessful attacks being called off quicker, and the resources reassigned to alternate, unprotected targets. This re-affirms the notion that some DDoS protection is definitely much better than none at all.



New attack types & new tools to fight them

Preemptive measures to secure the Internet infrastructure

The fight continues to prevent hackers using the Internet infrastructure against itself. The ongoing decline in open ports is evidence that the Internet community continues to actively limit the resources available to hackers.

Arelion, with its key role in the global Internet community, continues to work on this kind of ‘passive DDoS protection’ – an important tool in the war of attrition against malicious DDoS traffic.

New battlegrounds emerge and security gaps are being exploited

DNS Amplification is back – after a brief dip and a period of relative calm in 2022, brute force is in vogue again, and it was the dominant attack vector in 2023. This is largely because:

- **QUIC** – accounts for a large proportion of Chrome traffic and is UDP based - making it difficult to protect against.
- **Virtual servers** and so-called ‘bulletproof hosting’ suppliers are the next big battlegrounds, and once again, we’re back at a point where net neutrality and net security are starting to seem mutually exclusive.

DNS water torture attacks are more common

DNS Water Torture Attacks are on the rise. This attack vector was first publicly disclosed in February 2020 by researchers from Israel's Ben-Gurion University of the Negev.

Although this type of attack isn’t new, we saw an uptick in DNS Water Torture Attacks towards our customers in Q1 and Q2 2023.



A turbulent world impacts attack patterns

The ongoing cyber-tug-of-war

As a result of the industry-wide push to shutdown or restrict networks used for, or potentially used for, spoofing networks, DDoS attacks continue to evolve towards direct path attacks sourced directly from botnets.

As a result, we are seeing more non-spoofing attack traffic such TCP SYN or SYN/ACK attacks, which are often smaller in volume but of higher intensity (packets-per-second).

DDoS attack vectors targeting web sites

Towards the end of the year, a new type of DDoS attack based on HTTP/2 was widely used to bring down web sites – in particular, within the banking and government sectors in Sweden and other countries.

This type of attack presents challenges for networks everywhere because mitigation is less straightforward.

Cyber warfare mirrors trends in ground war

The ebb and flow of the ground war in Ukraine reflects attack trends in countries such as Russia and Ukraine – and neighbouring countries like Poland.

Cyber warfare is now an established part of nation state conflict and is not limited to just governmental assets.

As numerous heads of state and military start talking of a “pre war” era, especially in Europe, resilient cyber-defences cease to become a luxury.

DDoS_ data_summary

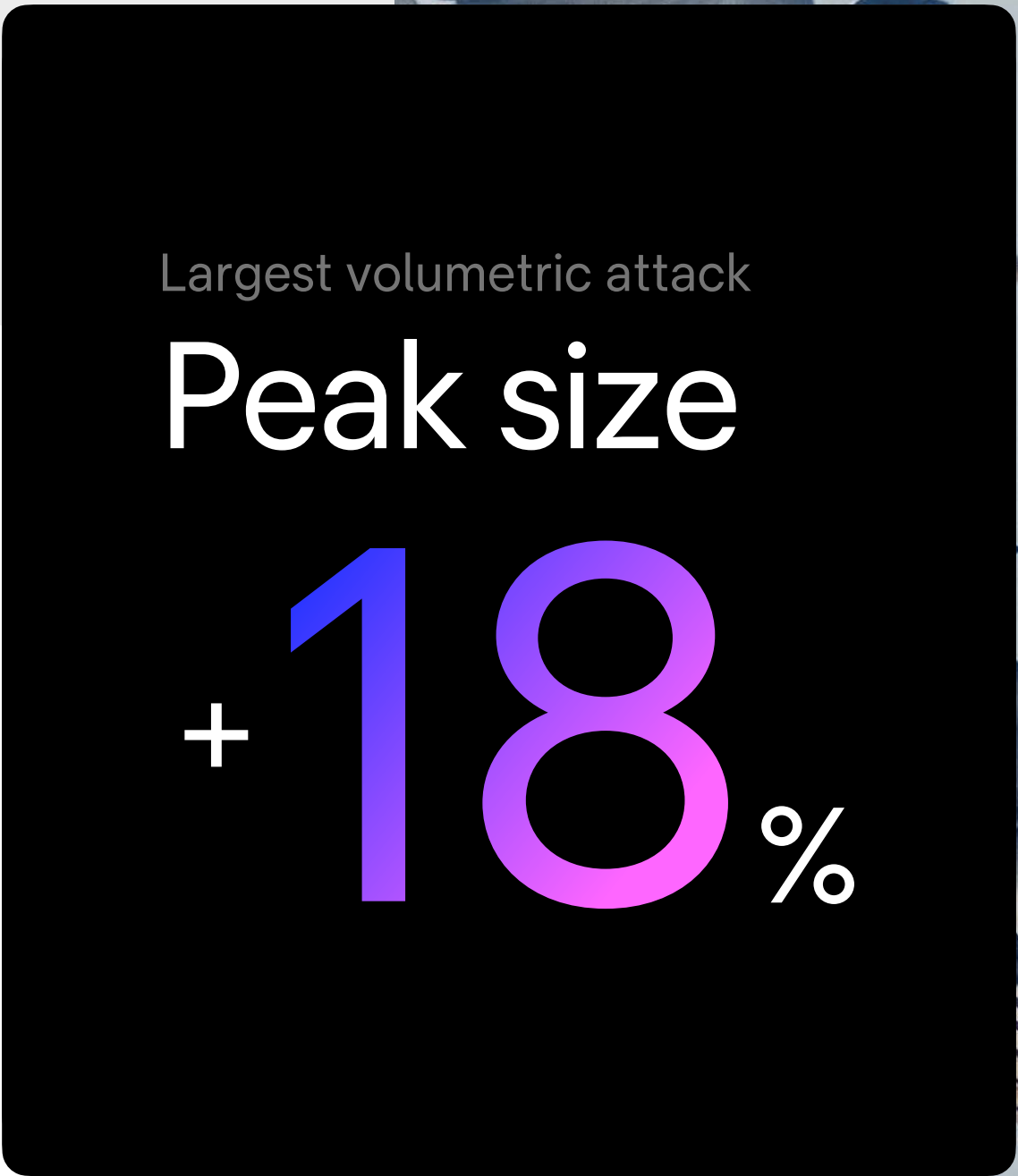
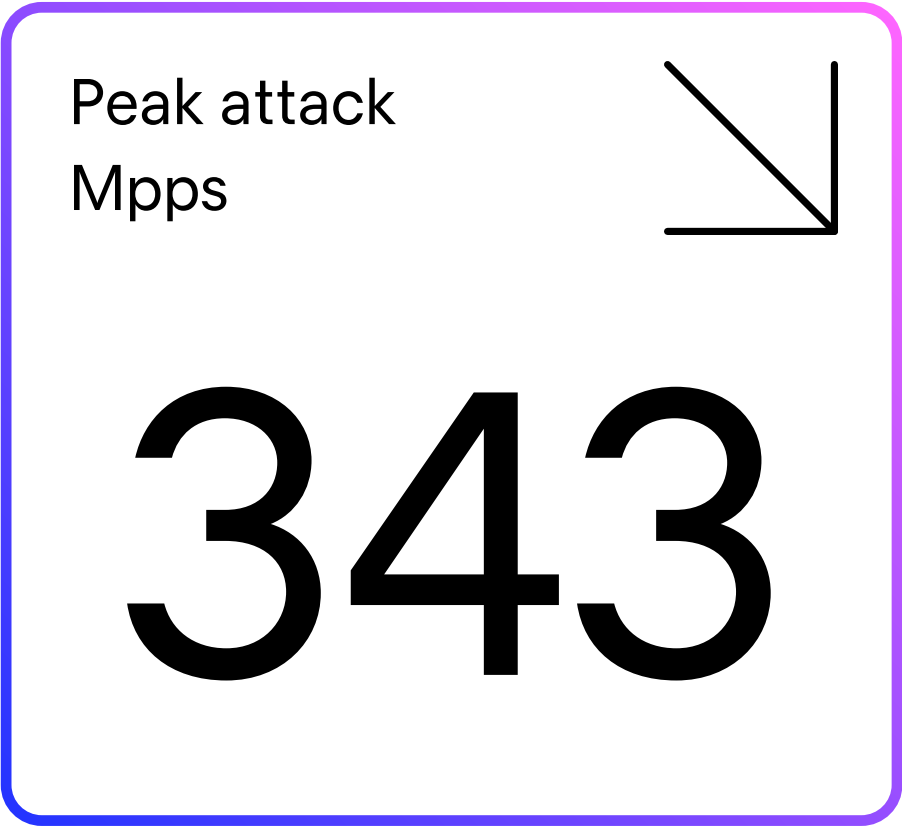
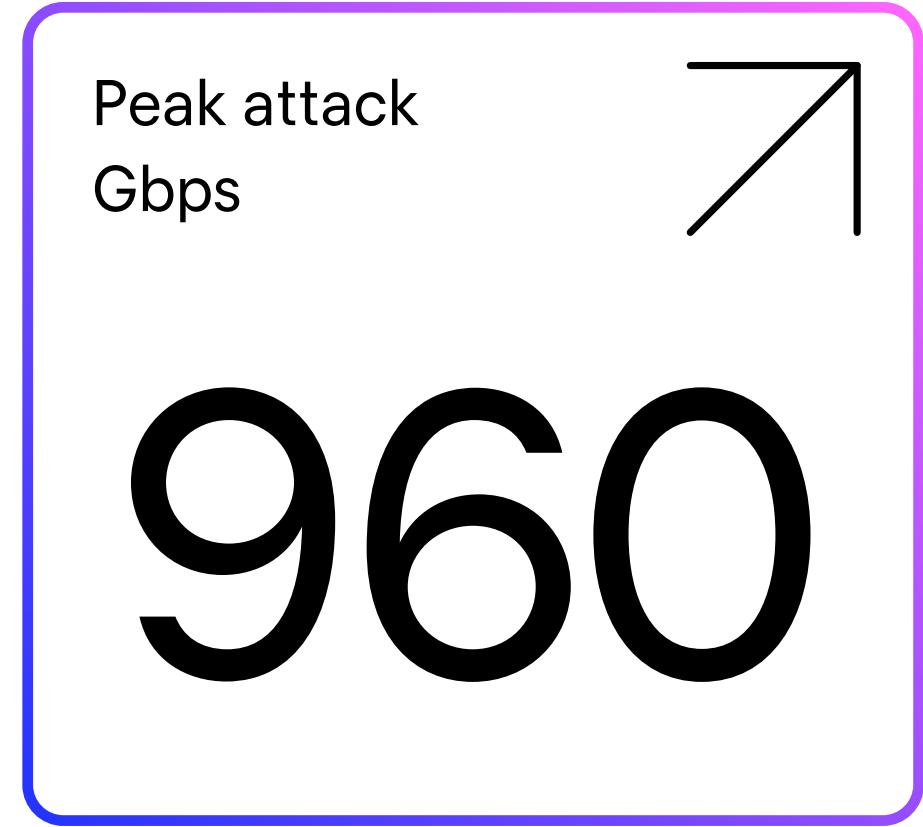




The DDoS network impact: peak attack traffic

The largest volumetric attack in 2023 peaked at 960 Gbps (up 18% from 2022). This came from a UDP-based attack in Europe.

At 343 Mpps, the largest pps attack came from a multi-vector TCP SYN, SSDP Amplification attack in North America.

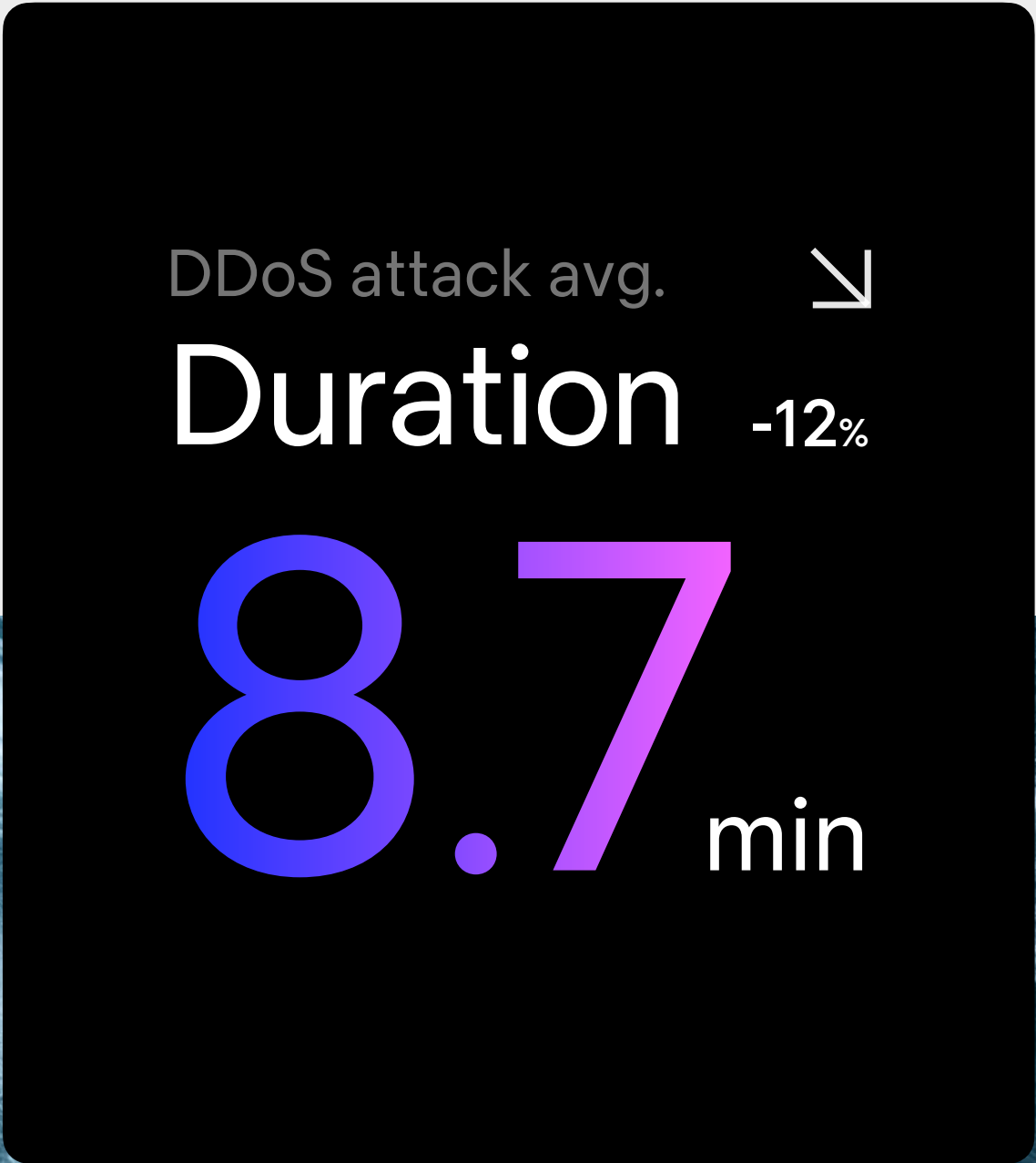
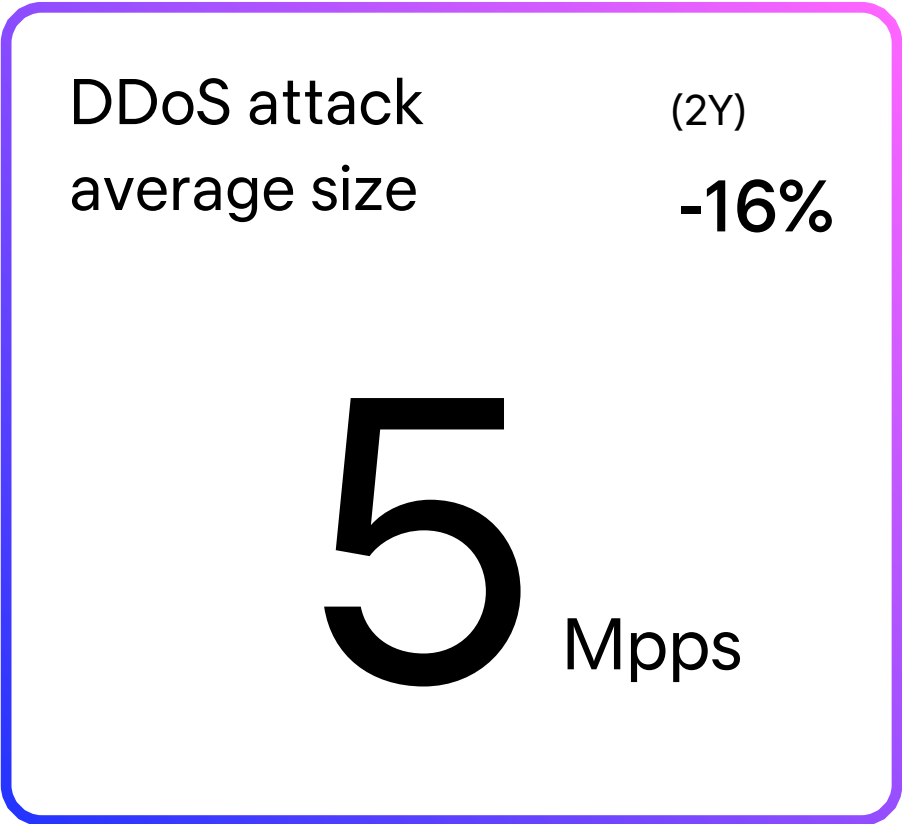
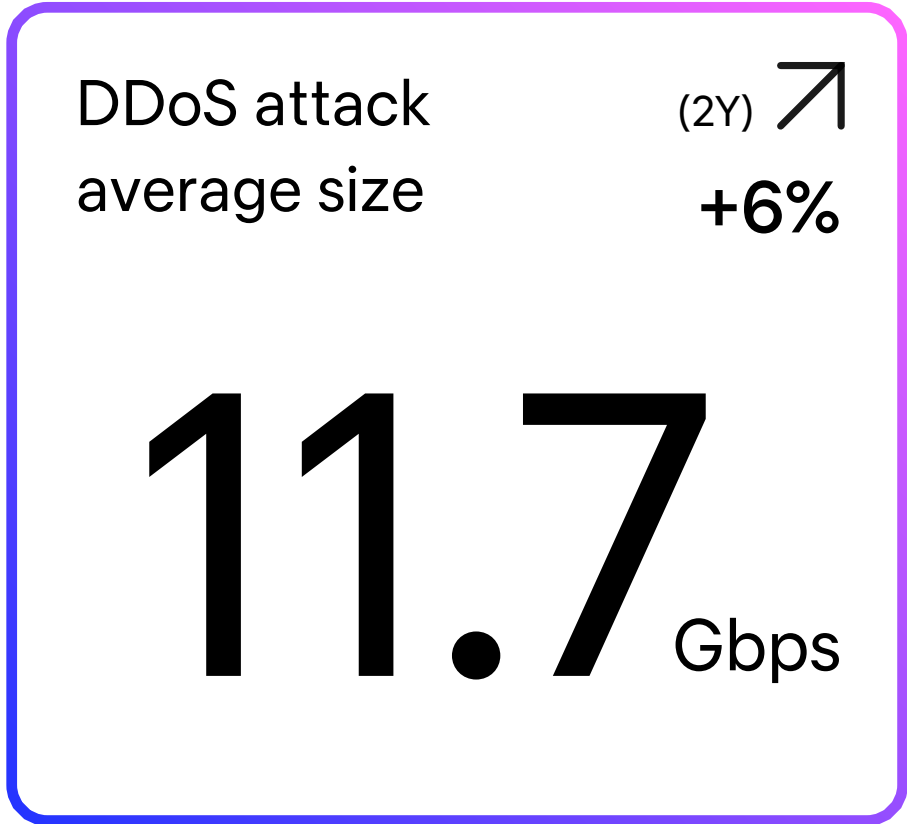




Average attack size and duration

Attack duration is down, but this doesn't mean attacks are less serious. Larger, more intensive attacks over slightly shorter periods ultimately cause the same damage overall.

From the data we've observed, it appears that average duration is being dragged down by **unsuccessful attacks being called off quicker**, and the resources reassigned to alternate, unprotected targets.



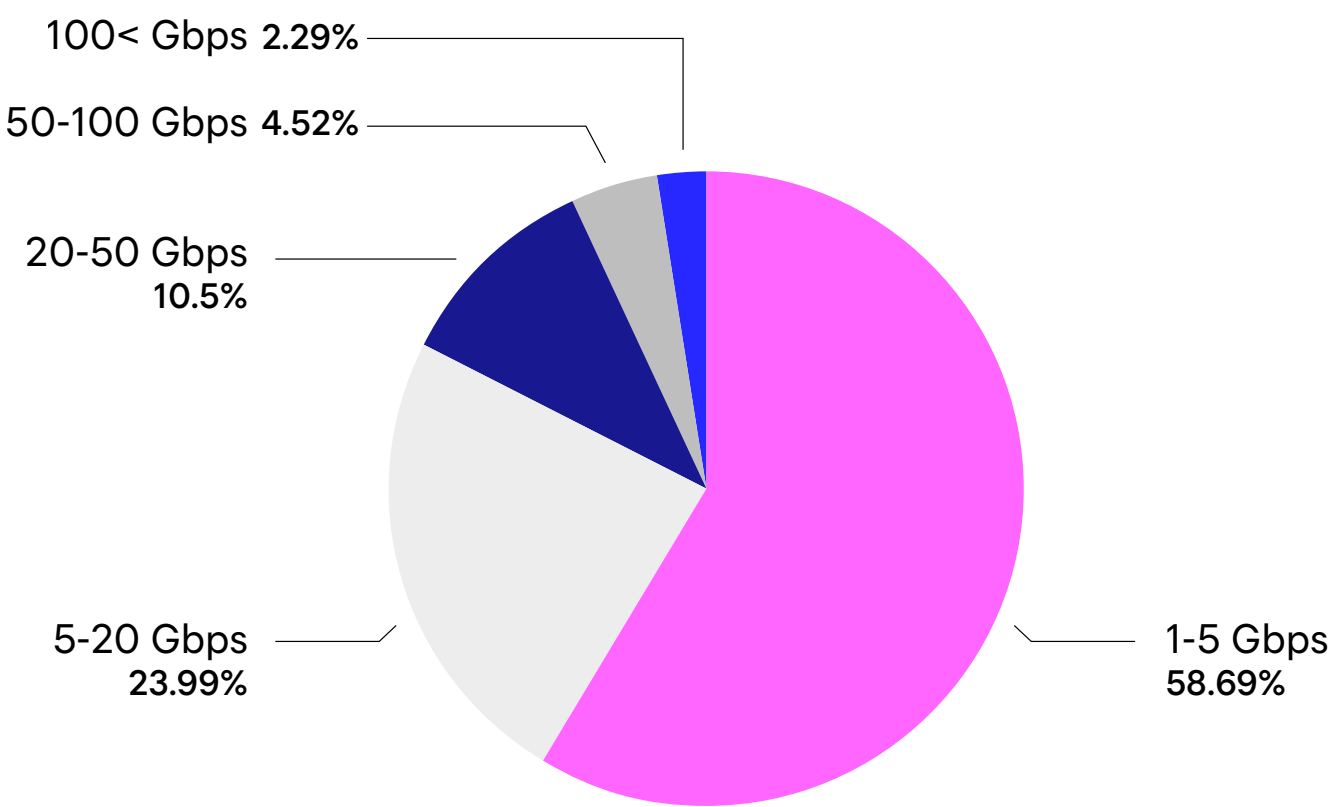
Attackers are quicker to abort failing attacks, and instead move on to less protected targets



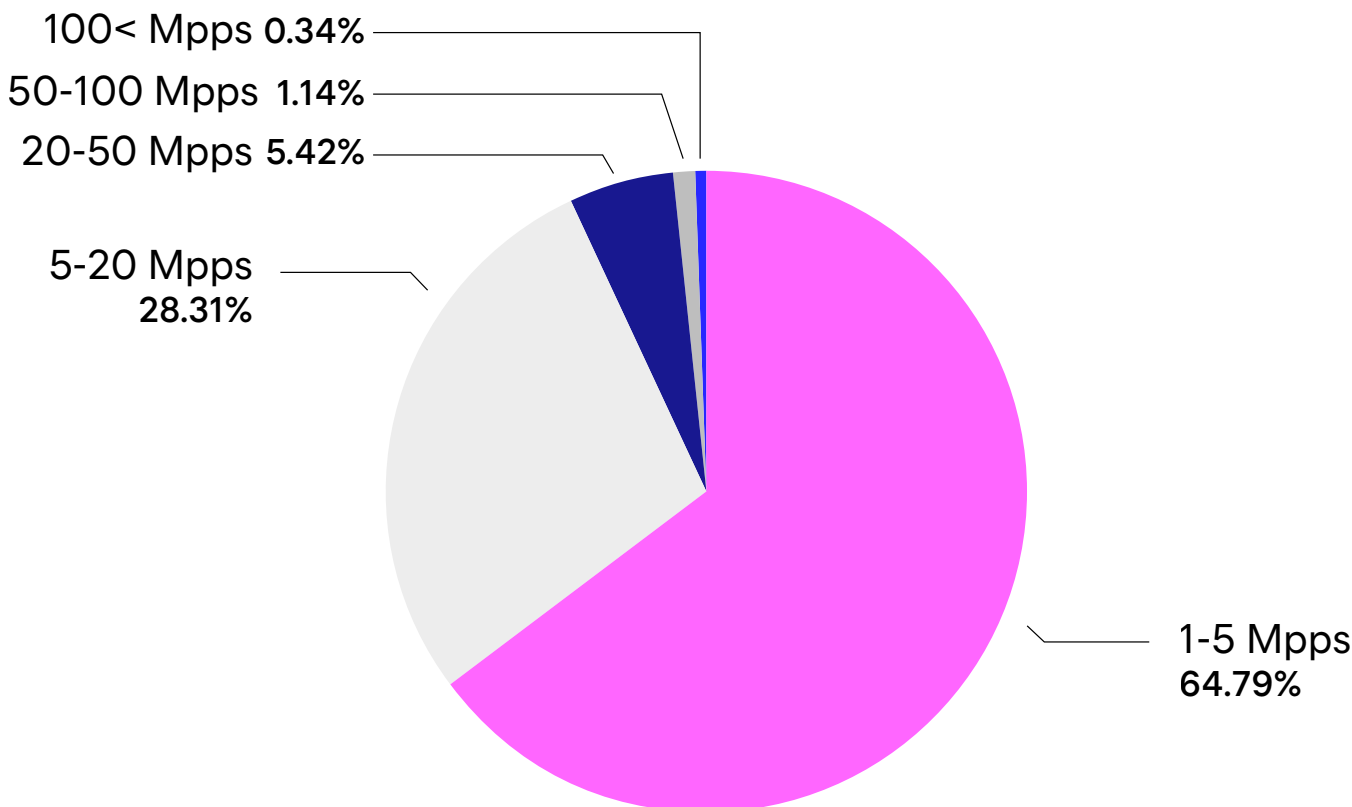
Attack size distribution

Generally, attack size distribution in 2023 was fairly similar to that in 2022. The vast majority of attacks are still small and mostly driven by free-tier stress test or DDoS-as-a-Service attacks instigated by amateur cybercriminals.

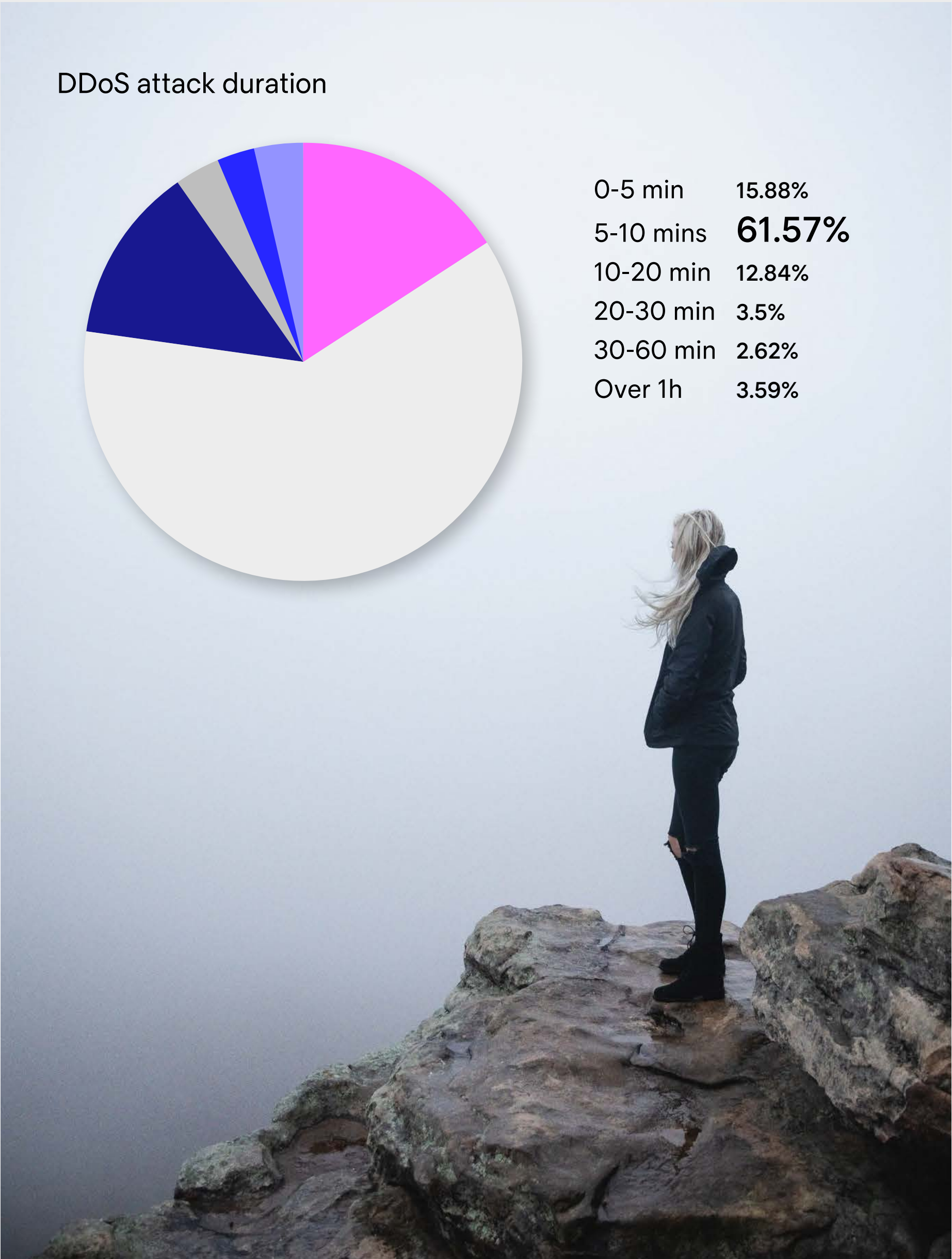
DDoS attack size Gbps



DDoS attack size Mpps



DDoS attack duration



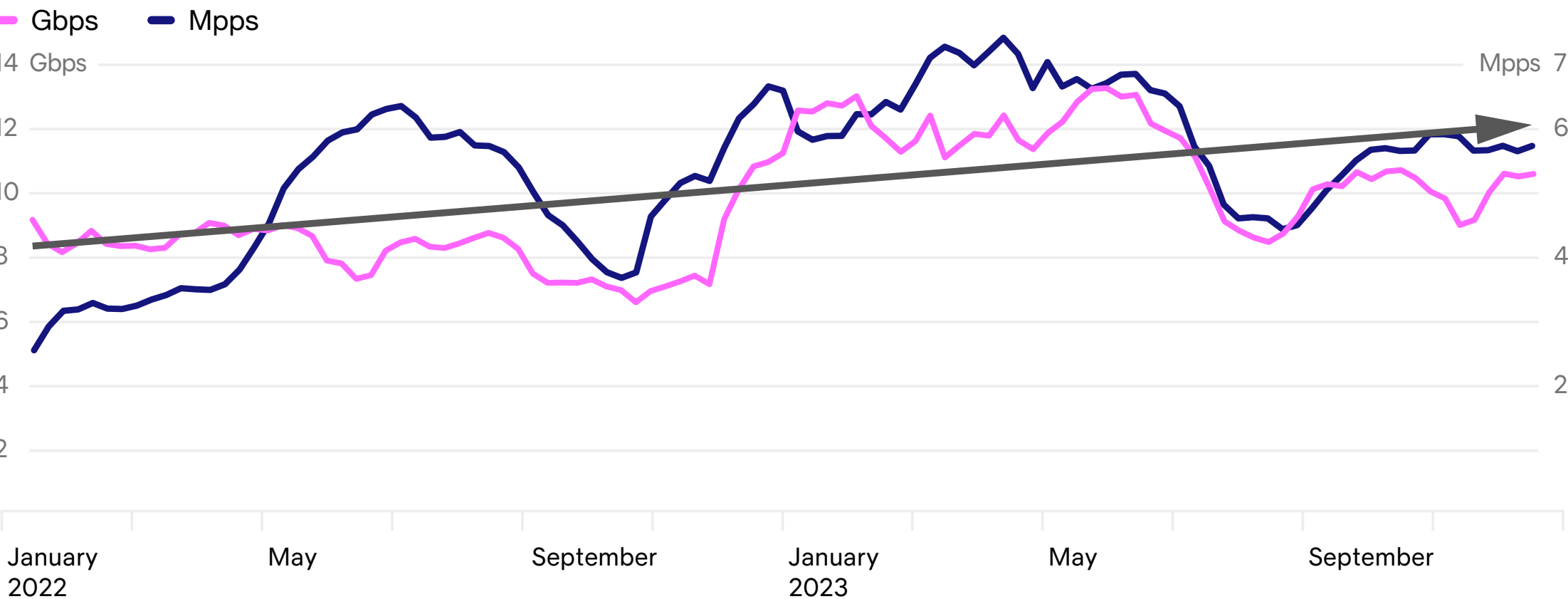


Attack strength and duration over time

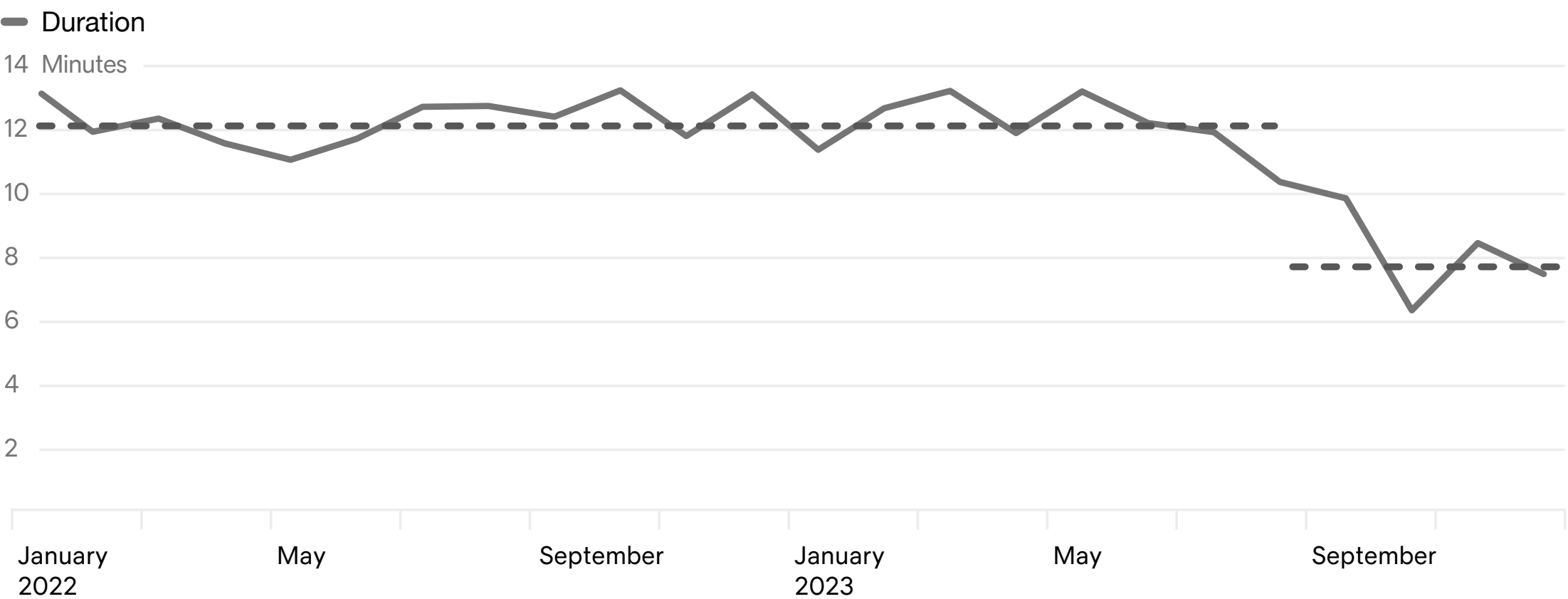
Year-on year, attack strength (in terms of both Gbps and Mpps) is increasing. This is predominantly driven by DNS amplification attacks. Average attack duration fell from a consistent level towards the end of 2023 – largely as a consequence of the increase in DNS amplification.



Average DDoS attack size Gbps and Mpps



Average DDoS attack duration





How our DDoS customers are being attacked

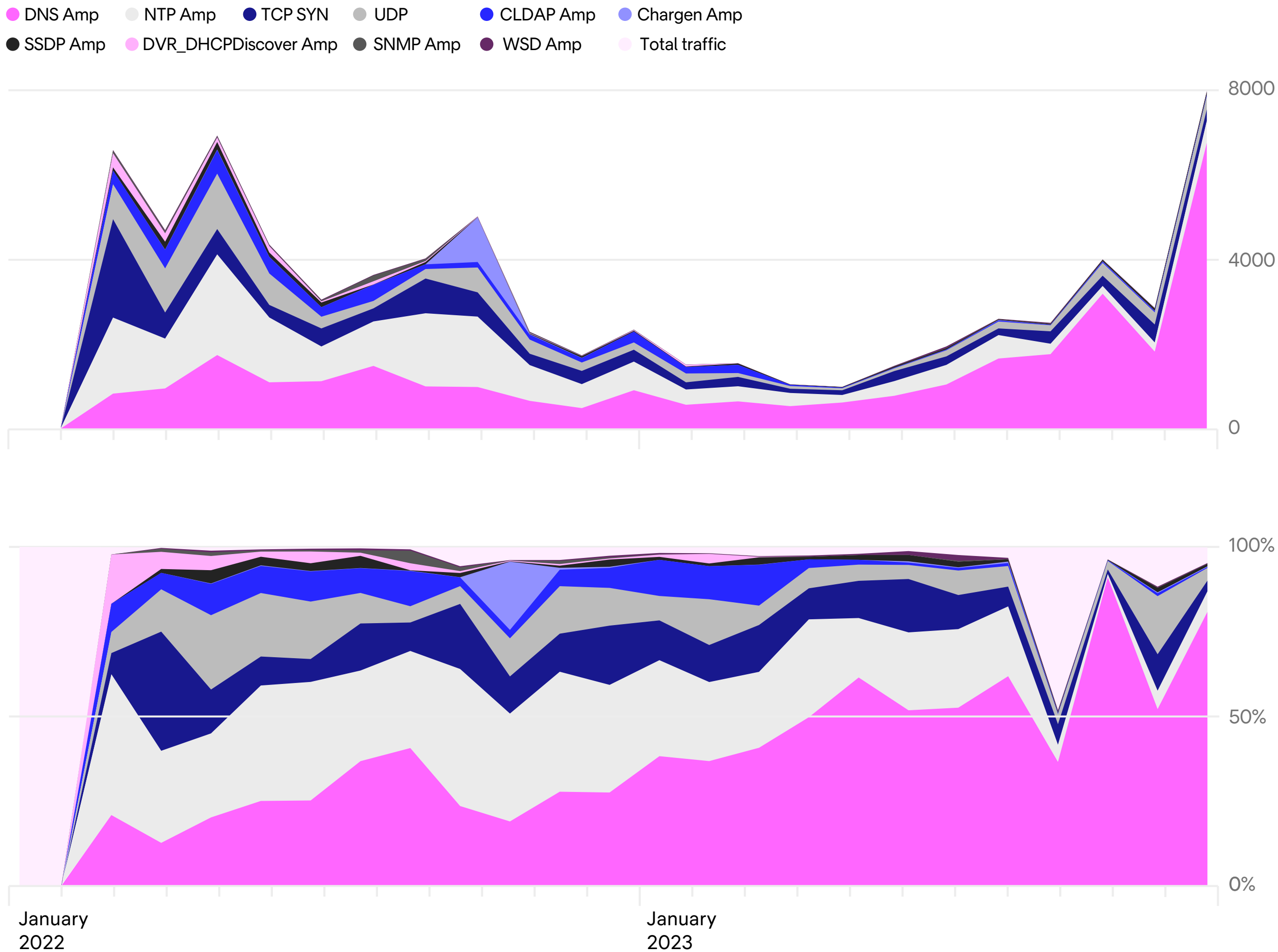
Following steady growth over the past four years, **DNS Amplification** was the most common type of attack in 2023, and by the end of the year, it constituted 80% of all attacks.

The most common attack vector in 2023 was **UDP over HTTP** (port 80) and **HTTPS** (port 443). The increasing popularity of the QUIC protocol makes it an easy target for amplification attacks, posing a greater challenge to defend against than attacks using TCP as the data transport layer.

Attackers are now mainly **exploiting compromised or acquired virtual machines** (VMs) and virtual private servers (VPS). Unlike compromised IoT device botnets, virtual servers offer more bandwidth and computational resources.

Additionally, there is a rising trend in **bulletproof hosting** over the past two years.

Attack type (percentage & total numbers)





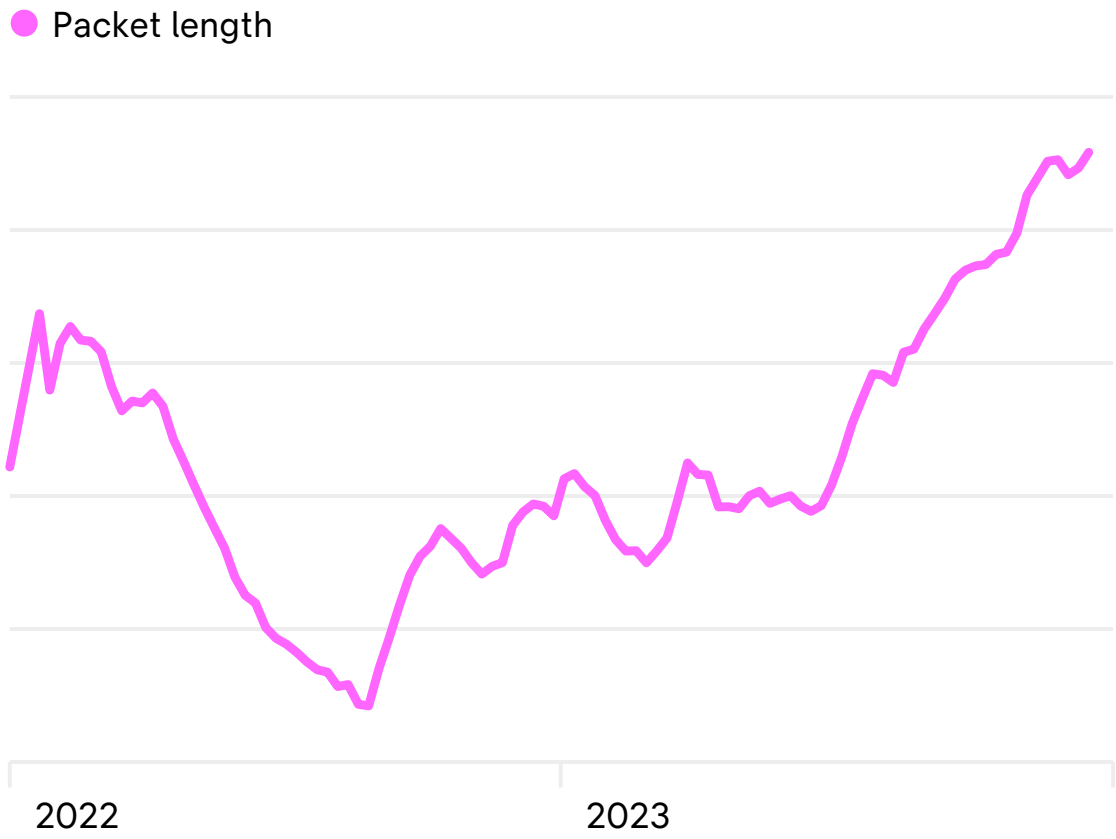
Average packet length and amplification

With improved DNS amplification, attackers are achieving **larger and more effective** responses with the reflection packet. There is a growing trend towards more **multi-vector amplification** attacks, where different reflection UDP services are combined within the same attack.

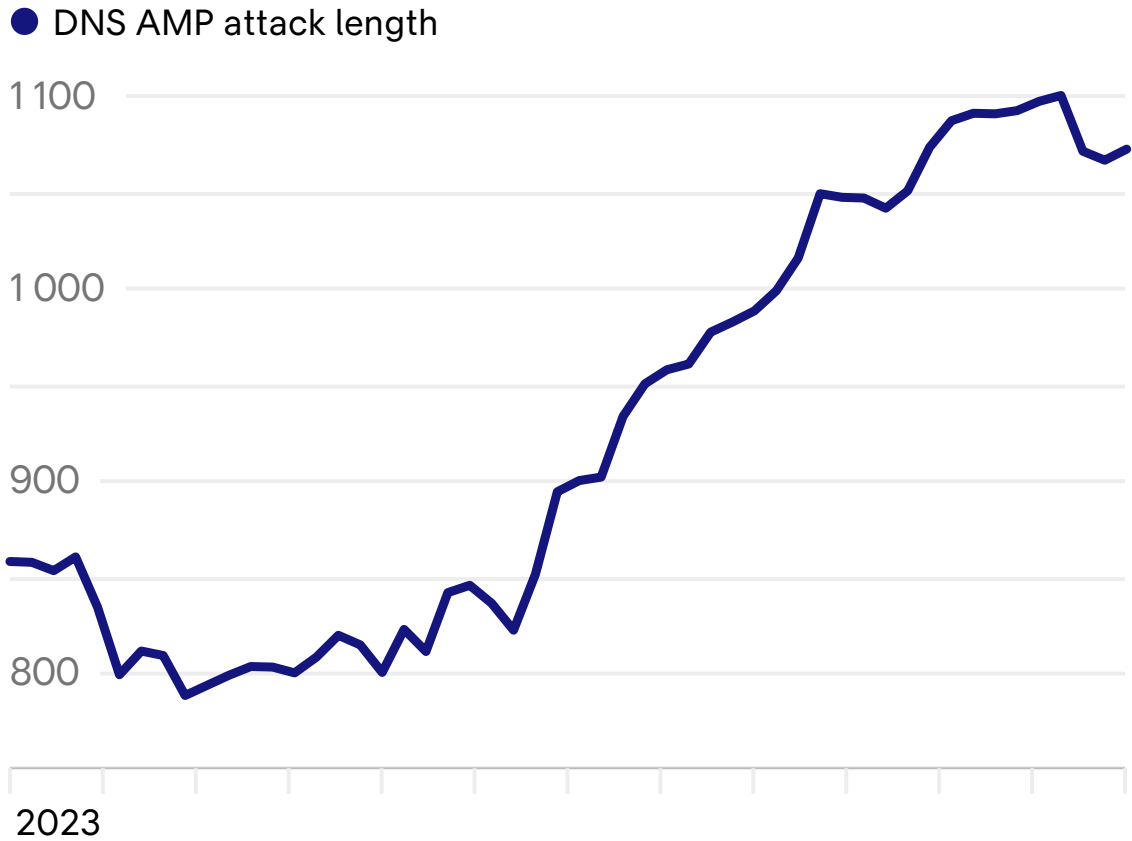
Attackers are constantly evolving their tactics - often changing their vectors mid-attack

The cat-and-mouse game continues, and attacks continue to evolve with advanced DDoS vectors such as TCP/Syn in combination with mixed UDP amplification. We've also observed attackers adapting and changing vectors more frequently, even during ongoing attacks.

Attack average packet length



DNS AMP attack average packet length



Geographical distribution





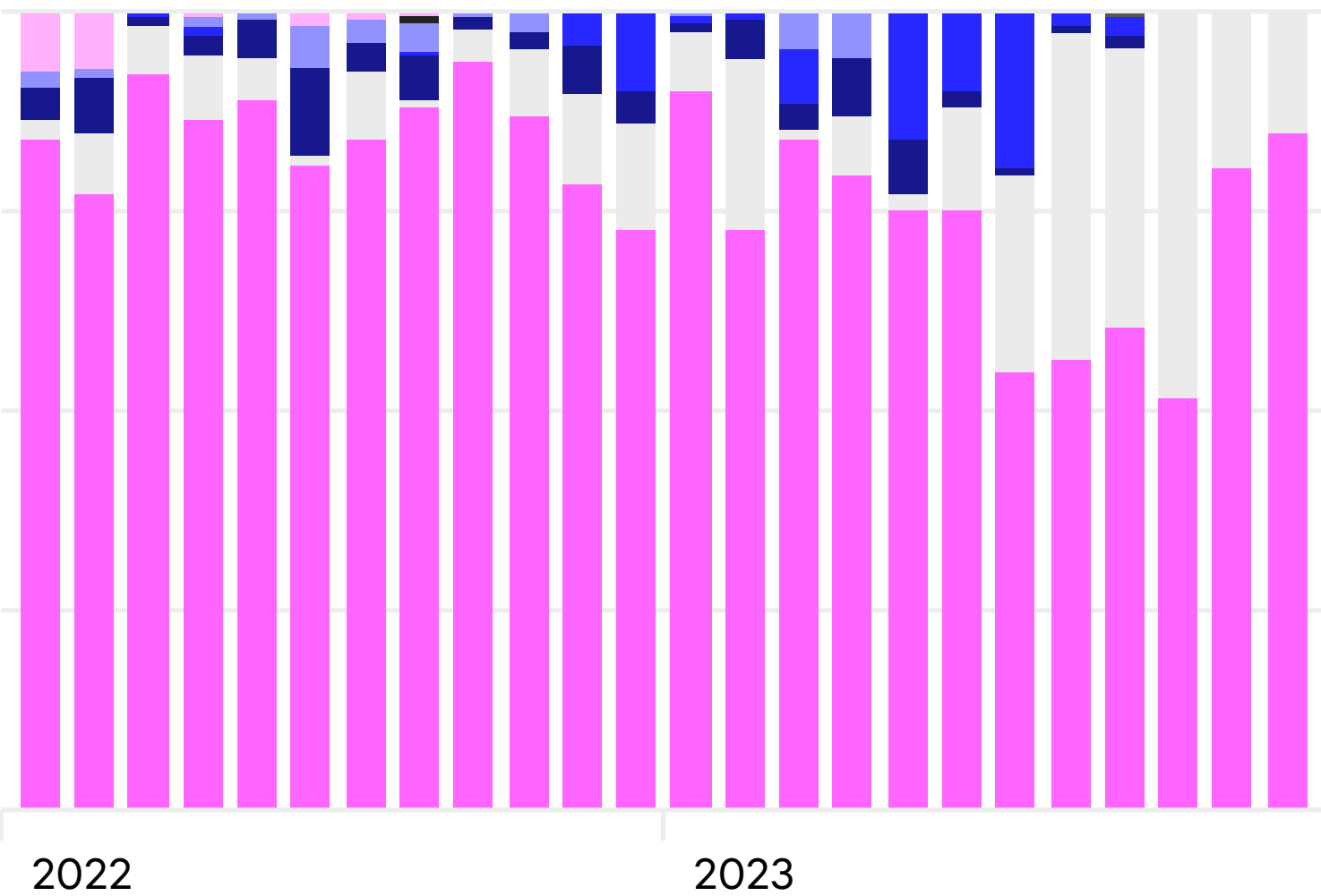
DDoS attack patterns around the world

As with last year, heightened geopolitical tensions continue to manifest themselves in the digital ecosystem as hotspots of DDoS activity.

Globally, there has been an increase in HTTP application-layer attacks. Prominent DDoS attacks have included those by pro-Russian groups like REvil, Killnet, and Anonymous Sudan, with some high-profile attacks against websites in Europe and the US.

Attack type (percentage & total numbers)

- TCP SYN
- UDP
- NTP Amp
- SSDP Amp
- CLDAP Amp
- DNS Amp
- DVR_DHCPDiscover Amp
- SNMP Amp

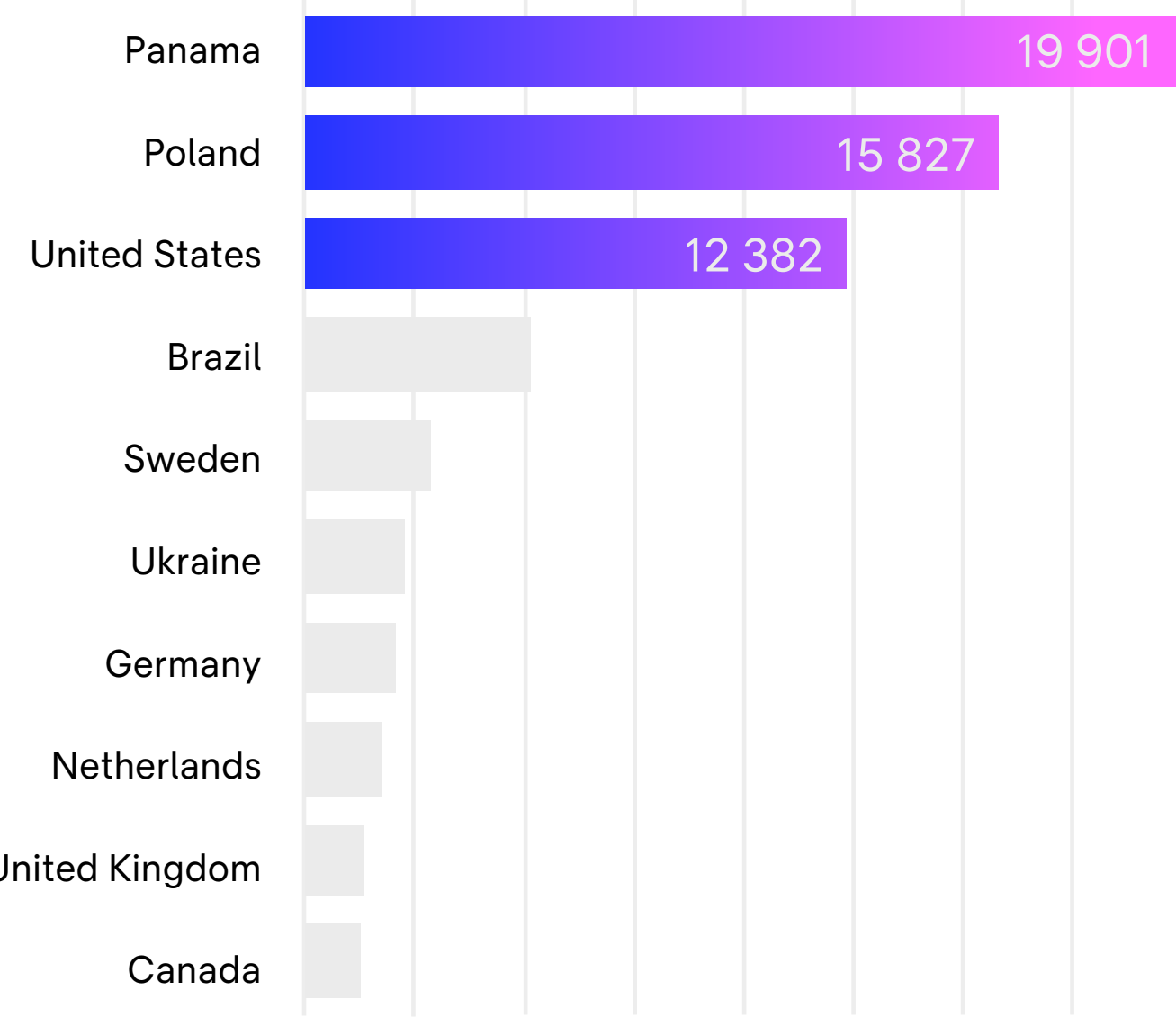




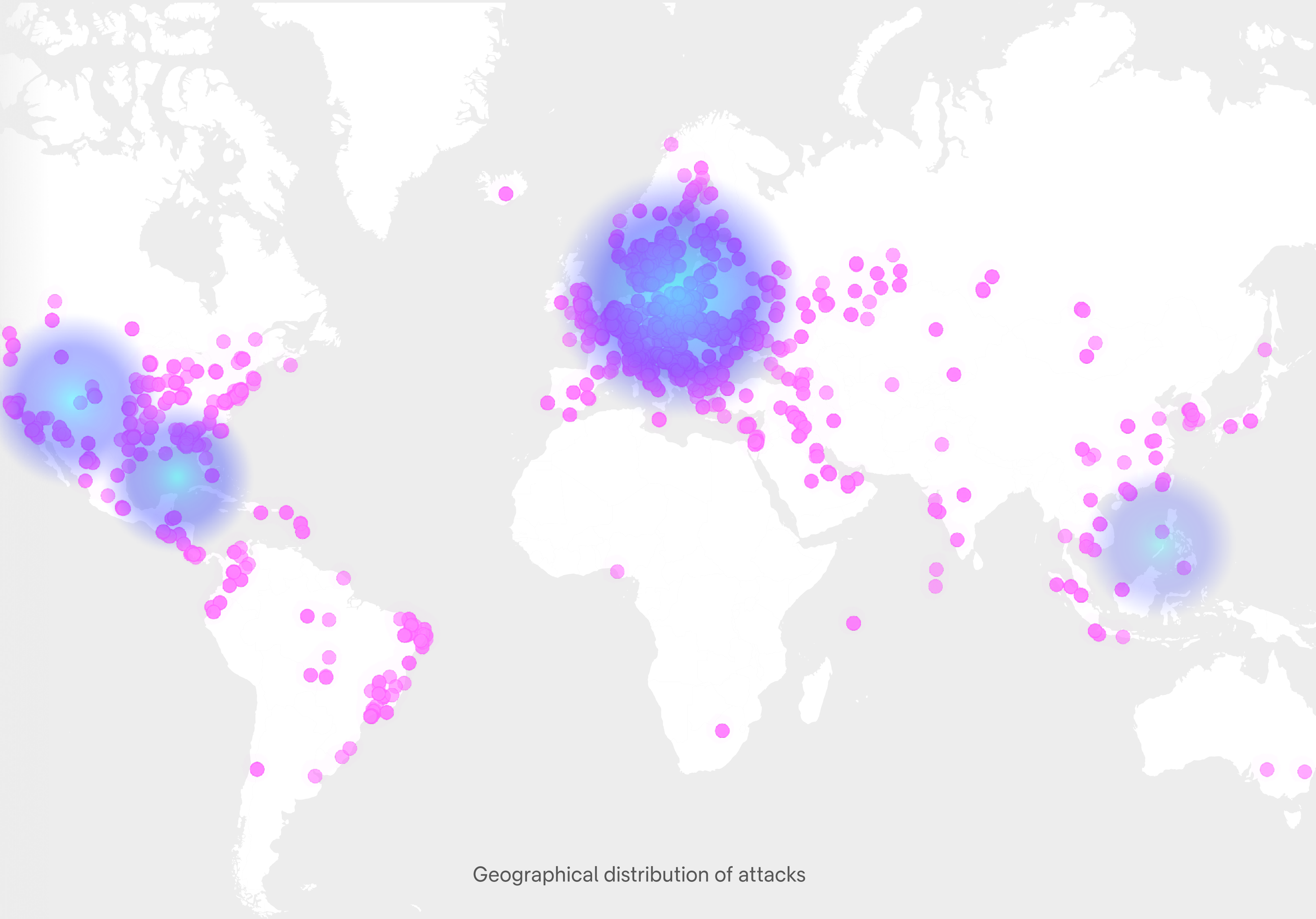
The global picture in AS1299

An overview of attack distribution in our
global IP backbone

Top 20 attacked countries



11. Colombia | 12. France | 13. Bulgaria | 14. Norway | 15. Czechia
| 16. Italy | 17. Austria | 18. Iraq | 19. Russia | 20. Costa Rica



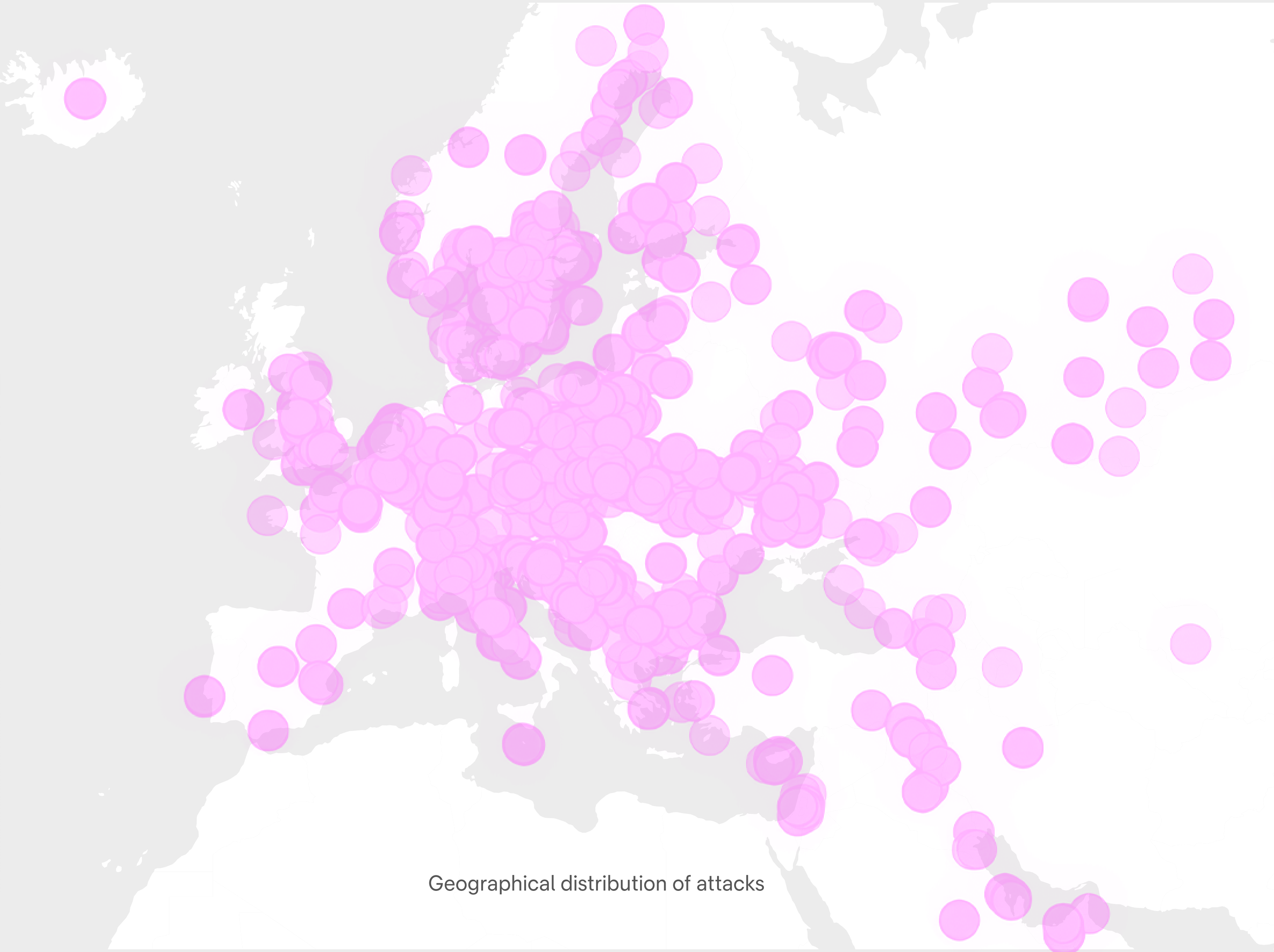
Geographical distribution of attacks



Global conflicts and their impact on cyber-attacks

Europe stands out, with Poland being the second most attacked country globally and Ukraine in sixth place. This is most likely a consequence of the ongoing hybrid attacks against NATO countries and allies of Ukraine in Europe.

So far, we haven't seen evidence of the Gaza conflict in a DDoS context.



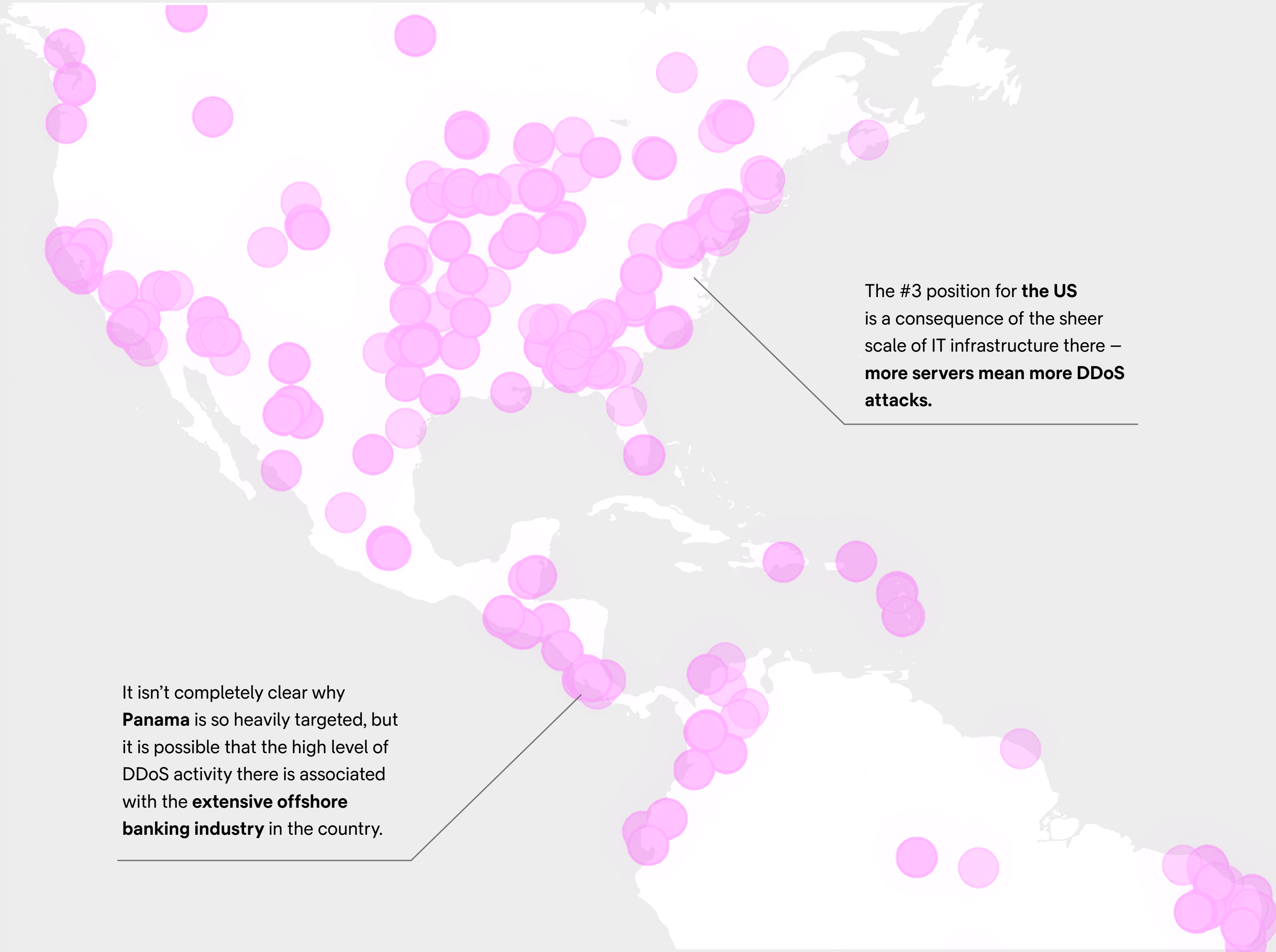
Geographical distribution of attacks



A shift in attack types

When it comes to our DDoS protection customers, **DNS amplification** attacks tend to dominate, but looking at our global network overall, **TCP SYN** attacks and **UDP attacks** in different flavors are more prevalent. Furthermore, the focus of these global attacks has **shifted from Europe to a more even worldwide distribution**, with a slightly disproportionate increase in attacks targeting the US. We believe this is a result of **a shift in focus towards bigger companies or government entities**.

The larger, higher profile targets tend to face more sophisticated attacks aimed at circumventing stronger/more elaborate mitigation systems and they require significantly more attack resources to succeed.





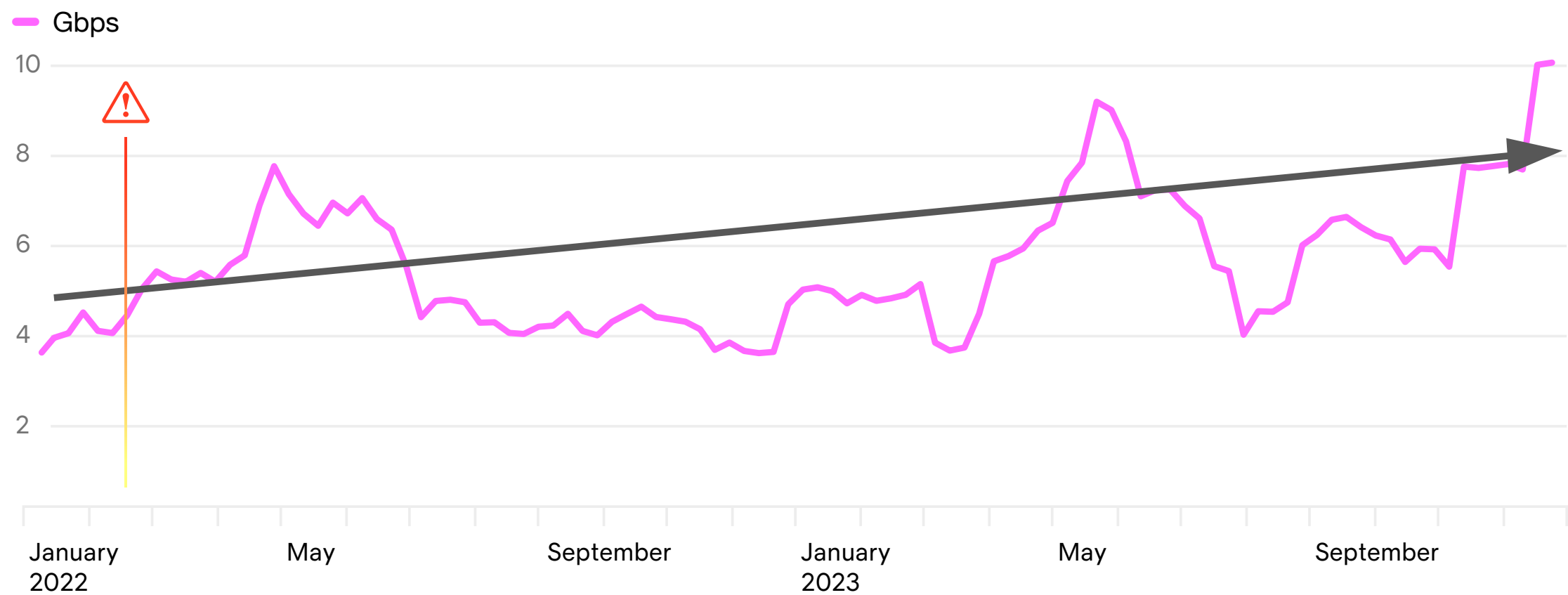
DDoS and the war in Ukraine

Average bps has been continuously increasing since the conflict started in February 2022. It is clear that **DDoS is a significant weapon in the hybrid warfare arsenal** – there is a direct correlation between DDoS activity during Nov-Dec 2023 and the intensity of the ground war.

During late 2023 and the beginning of 2024, we observed a **significant increase in DDoS attacks towards Poland**. The average attack strength (Gbps) rose nearly fivefold over the year, and the actual number of attacks skyrocketed. Most of these attacks used the DNS amplification vector and targeted data communications service providers and network infrastructure.

This development is closely tied to the conflict in Ukraine, and various hacking groups have **singled out Poland as a target**.

Average Gbps per week

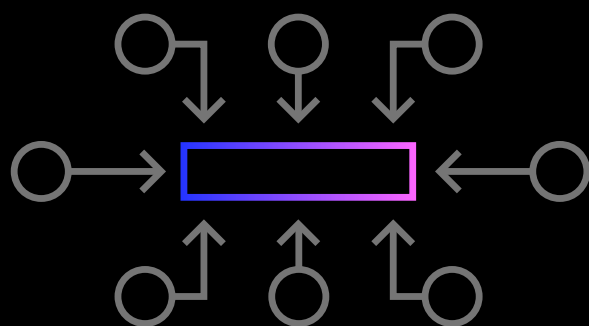


Total attacks per week





Glossary and terminology



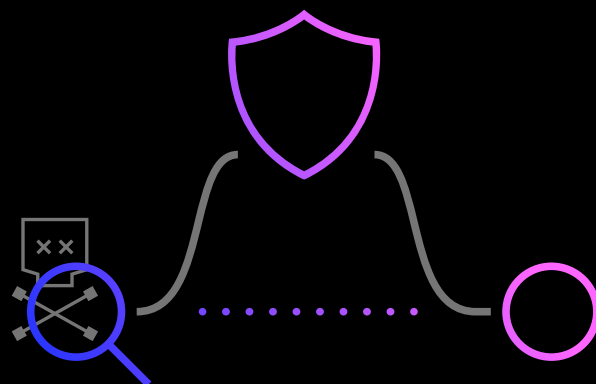
Attack-vector

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.



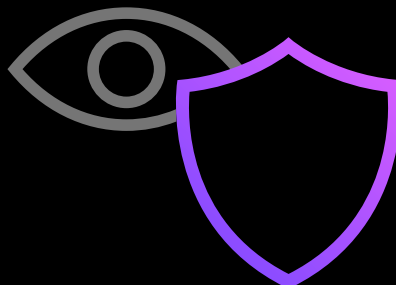
DNS amplification

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.



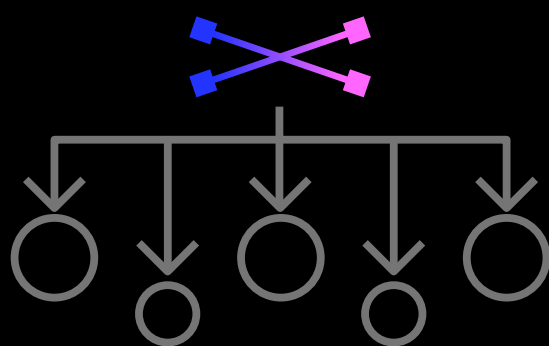
Auto-mitigation

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.



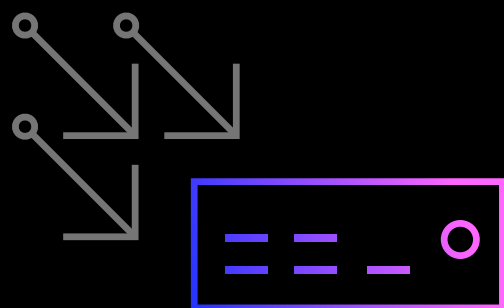
Carpet bombing

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.



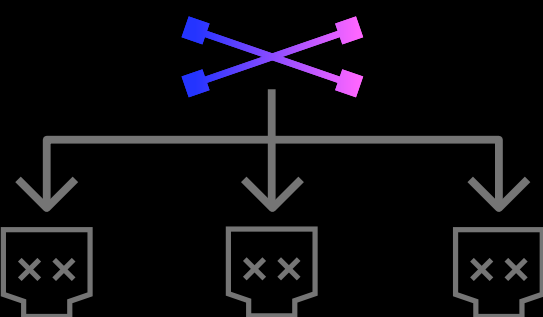
NTP amplification

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.



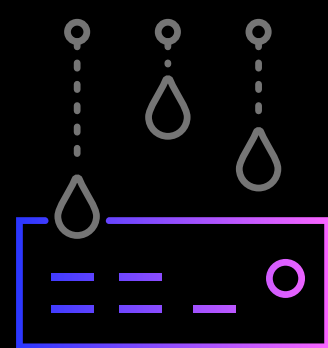
SYN attacks

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.



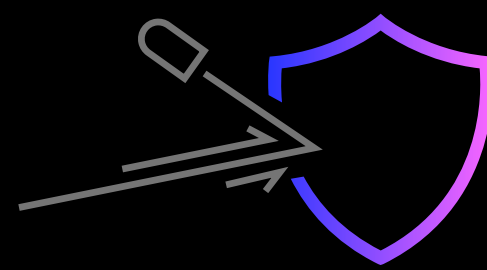
DDoS-as-service / Botnets

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.



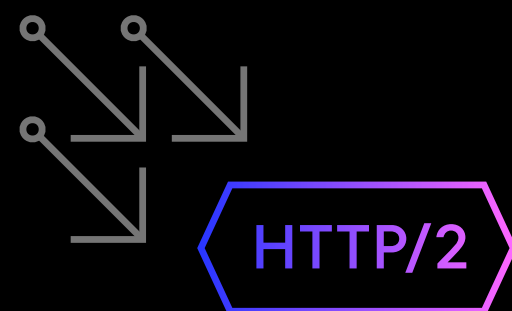
DNS Water Torture attack

Like 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 surrounding infrastructure.



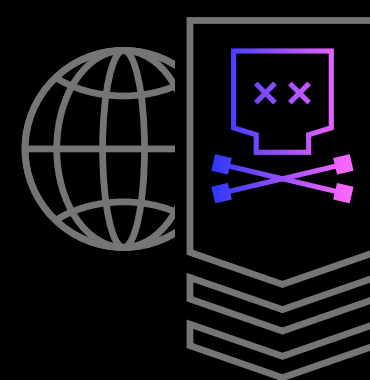
Bulletproof hosting

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 and 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 75,000 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 [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. 2024. All Rights Reserved.