Q3 & Q4 2024

zayo®

Protecting Your Business from Cyber Attacks

The State of DDoS Attacks

DDoS Insights

Executive Summary

That's a wrap on 2024, and the numbers are in: DDoS attacks are surging like never before, with a greater distribution across all industries. This makes secure and reliable network infrastructure even more paramount for healthy operations. We're a quarter of the way through this century, and, simply put, **your data and network uptime are too critical to leave exposed.**

Read on to explore our insights and gain a thorough understanding of how cybercrime is evolving and what steps you can take to protect your organization.

The Big Picture

As we predicted in our mid-year report, 2024 has brought a higher baseline for the frequency and severity of DDoS attacks – a new normal, if you will. We noted a large spike in attack frequency and sustained growth in the size of attacks.

Well, that trend has continued through the remainder of 2024. Experts at Zayo and thought leaders across the industry agree that **we're now at a more extreme baseline when it comes to DDoS attacks**.

Heightened Attack Frequency

Comparing 2024 to 2023, **DDoS attack frequency grew by a whopping 81.7%**. Where we previously detected just over 90,000 attacks in 2023, this year we observed nearly 165,000 attacks.

Interestingly enough, the first half of last year yielded more attacks (largely due to a surge of attacks in Q2), but the second half of this year saw attack volume grow by 60% compared to Q1 & Q2, with October and November showing the greatest number of attacks – likely due to the United States Presidential election.

All Industries and Business Types

Telecommunications is an easy target for these attacks because a successful DDoS attack targeting a network provider can cause a major ripple effect, impacting countless additional businesses. However, year-over-year the telecommunications industry shares less of the total attack volume, which ultimately means **other industries are facing a greater threat than in years past**.

The cost of a DDoS attack is **$6,000 per minute**.
What's your cybersecurity strategy?

Methodology

This report analyzed more than 160,000 threat detections experienced by Zayo DDoS Protection customers throughout 2024. Of those attacks, over 101,000 attacks occurred in the second half of this year. The data spans 17 industries dispersed across North America and Western Europe.

DDoS 101

Unfamiliar with DDoS attacks? Let’s get you up to speed.

A Distributed Denial of Service (DDoS) attack is a deliberate, targeted cyberattack that aims to wreak havoc on an organization’s online operations. While DDoS attacks come in various forms, they all share a common objective: overwhelming the target’s Internet circuit with excessive, illegitimate traffic to cause significant disruption.

In many cases, **attackers use DDoS attacks to probe an organization’s security defenses, identifying weaknesses for potential future cyber threats** – more to come on that in the “duration” section of this report. Though the specifics of each attack may differ, their fundamental purpose remains the same – to inflict harm and compromise system availability.

Cybercriminals are successful because they continually **optimize their attack techniques and technologies**. Cybersecurity solutions, including DDoS Protection, aim to stay two steps ahead of them by **predicting trends, learning from global traffic patterns, and fortifying networks** with a dedicated team of cybersecurity professionals.

> “Experts anticipate that the DDoS attack landscape will undergo significant changes, paralleling the advancements seen in AI-driven attack methods. As technology progresses, **attackers will devise increasingly sophisticated techniques that exploit digital vulnerabilities and incorporate physical threats.**”
>
> **- Tyler Burke,** Product Manager, Network Connectivity at Zayo

Why "Distributed" Denial of Service?

DDoS attacks vary from DoS (Denial of Service) attacks because they are distributed, meaning they come from multiple – often thousands – of devices. **Hackers seek devices with weak security to form an array of infected Internet-connected machines that can perform DDoS attacks on their behalf**: networks of these devices are called botnets.

The Internet of Things (IoT) is fundamental to our accelerating digital age, but its pervasiveness is bringing forth added security risks, too. There's even a chance one of your personal Internet-connected devices, **like your Smart TV**, has inadvertently joined a botnet.

DDoS 202: A peek behind the scenes

DDoS attacks come in three main types:

1. **Volumetric attacks**, which flood a network with excessive traffic to overwhelm its bandwidth
2. **Protocol attacks**, which exploit vulnerabilities in network protocols to exhaust server resources, making services unavailable
3. **Application layer attacks**, which target specific applications by overwhelming them with seemingly legitimate requests, making them difficult to detect

The End of Year Pulse

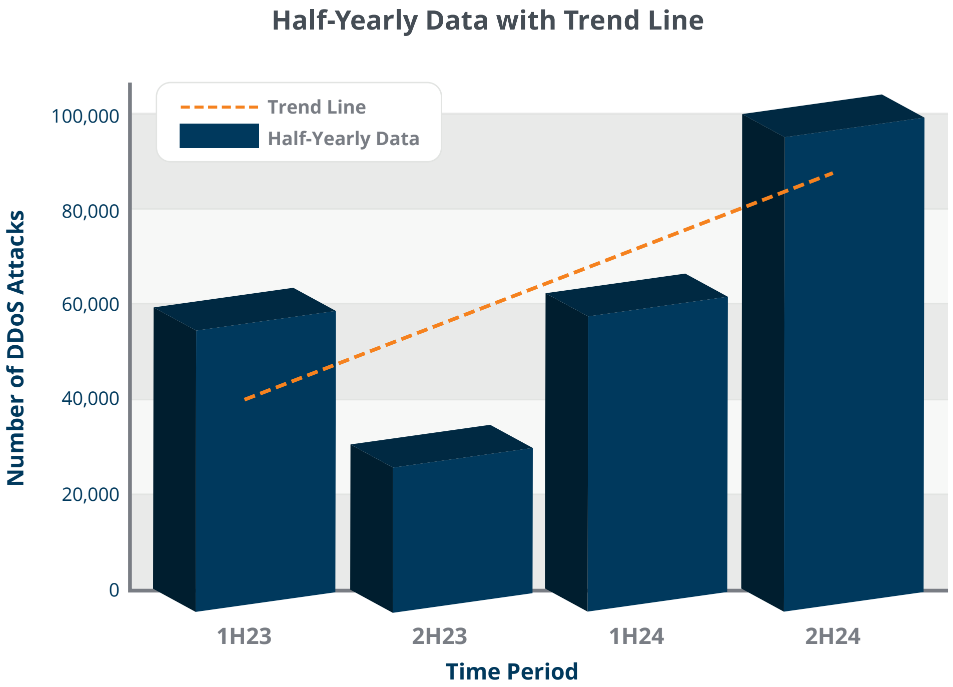
The shift to a hybrid workforce and distributed business environments resulted in a multitude of new digital assets, widening the attack surface and creating greater exposure weakness.

In a way, much like the attack severity of DDoS attacks has reached a new baseline, the state of how organizations connect and operate is also reaching a new equilibrium: even more disbursed and complex.

With that in mind, it's no surprise that **2H 2024 yielded the highest number of DDoS attacks we've ever recorded across two quarters**, driving the entirety of 2024 to reach a heightened level of attack frequency, sophistication, and impact. Large organizations must consider that while they have rapidly evolved into this new age, so have cybercriminals. That's why a comprehensive cybersecurity solution, including **DDoS Protection**, **SASE**, and **Firewall solutions is absolutely necessary**.

Key trends to highlight across 2024:

- **Quarter-over-quarter attack growth**, making 2023 pale in comparison – a trend that is likely to continue through 2025
- **A steady increase in attack size**, so your organization may not just be hit more often, but also harder
- Telecom as an industry passing the torch to the cloud and SaaS space for **the largest share of our top 10% observed attack size**
- **A burst in attack volume compared to 2023**, targeting critical industries including education, healthcare, and finance



All gas, no brakes

The foot is always on the gas: it's unlikely DDoS attacks will go away, let alone slow their acceleration. Just look at the information in this report, insights shared in previous Zayo reports, and even data from others like NETSCOUT and Cloudflare.

When we factor in the powerhouse accelerator that is Artificial Intelligence (AI), the proliferation of devices and network complexity will create an even larger playing field for digital crime. We're prepared – and eager – to tackle these burgeoning challenges.

A good defense is a good defense

Disarm this ever-growing threat with the industry's only **comprehensive, network-based DDoS Protection solution** capable of protecting all your network traffic without impacting latency. Get protected today.

The Frequency of DDoS Attacks

Show me the numbers!

Okay, we hear you – you're here for the rich data, and we're here to deliver, beginning with the **frequency** of attacks: the big, behemoth number that keeps growing every year. DDoS attacks are a monster that feeds off chaos and delicious, stolen data – and the reality is the frenetic pace of today's digital world has created an all-you-can-eat buffet for it.

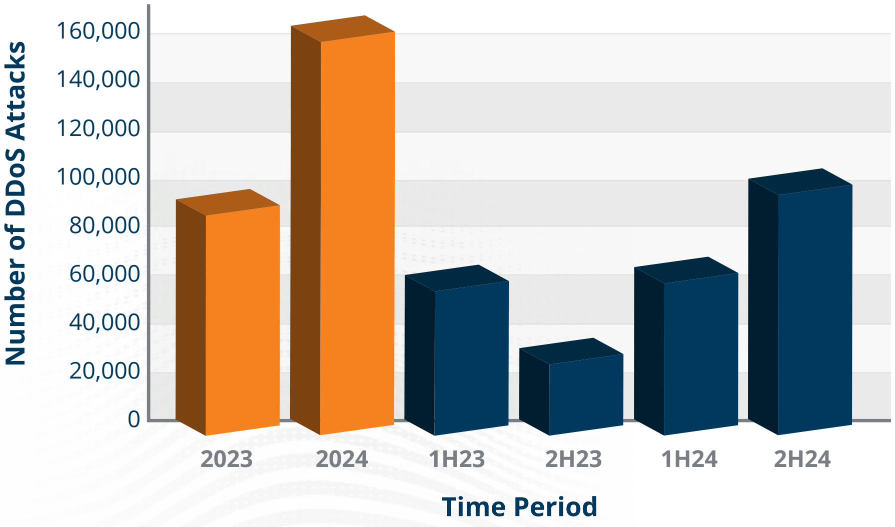
The numbers you were looking for

In 2024, we detected a total of 164,996 DDoS attacks; 101,683 of which took place in the second half of the year. As said above, that DDoS monster is feasting.

To put it in perspective...

- 2H 2024 was **60.6% greater** in volume than 1H 2024
- 2H 2024 was **231% greater** in volume than 2H 2023
- All of 2024 was **81.7% greater** in volume than all of 2023

Yearly and Half-Yearly Data Comparison



Remember, as detailed in our methodology section, these were attacks observed targeting existing Zayo DDoS Protection customers. Because they already had protection in place, their organizations could continue operating without interruption.

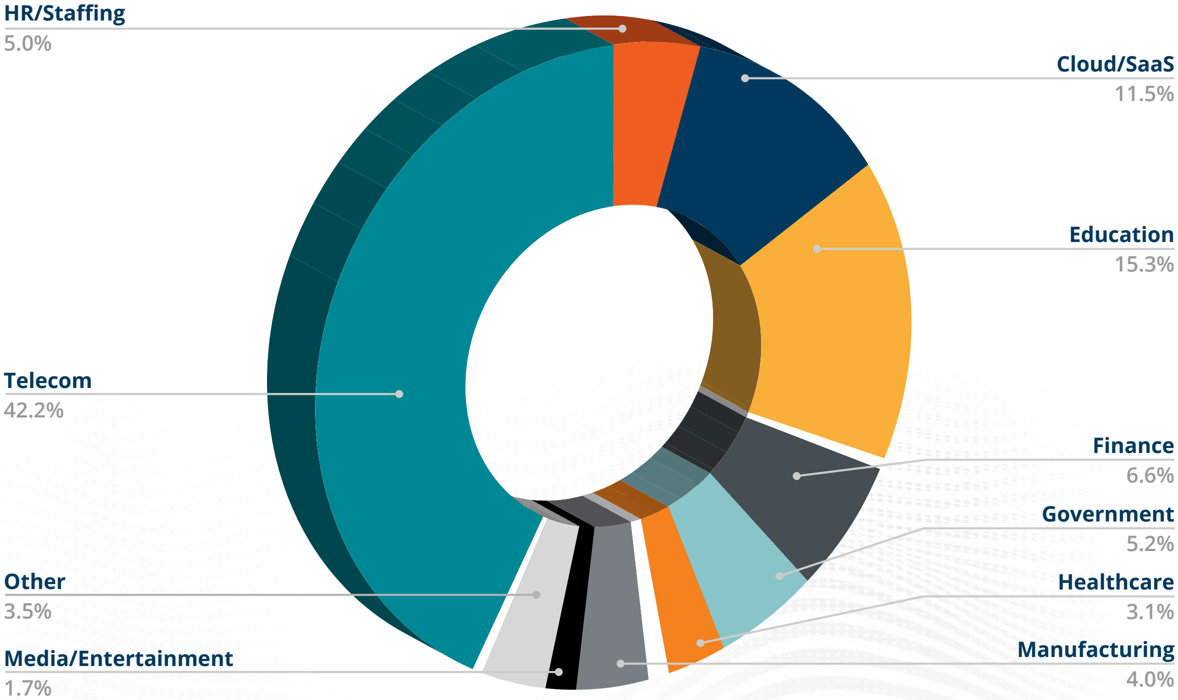
Seeing the **bigger picture**

NETSCOUT reports roughly **43,750 DDoS attacks per day**, according to their 1H 2024 insights. They also detail that **more than 75% of newly established businesses are involved in DDoS activities within just 42 days of coming online**. Indeed, the online world is swift to bring a business into all its opportunities – and its dangers.

The numbers, by noteworthy industries

But the growth in attack volume isn't the only thing that's noteworthy about 2024. As referenced in the introduction of this report, the spread of attacks has widened to target a greater range of industries, which we'll dive into shortly. While the telecommunications industry still shares the plurality of these attacks, the number of attacks this industry faces is down to **42% of all observed attacks in 2024** vs. 48% in 2023.

2024's Most Attacked Industries by % of All Attacks



Telecommunications

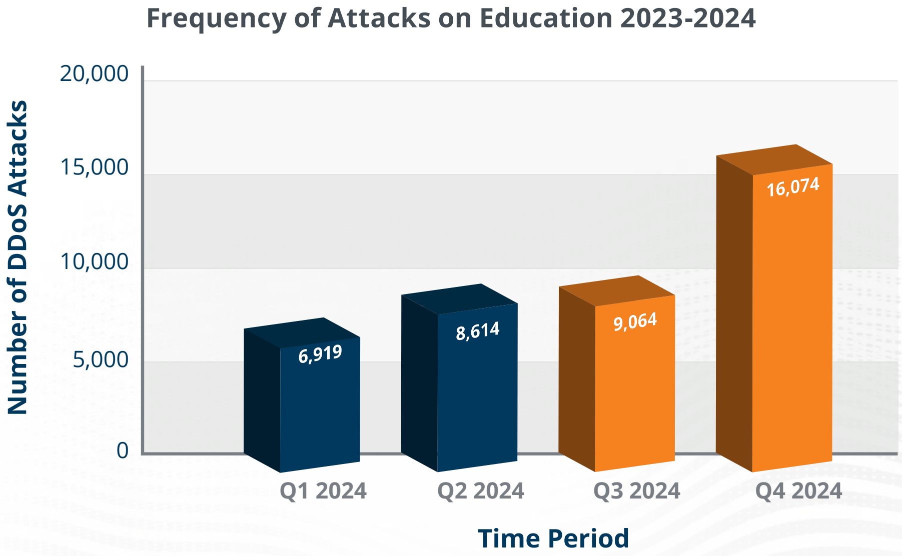
When you want the most impact, why not go straight to the source? That's the mindset driving attacks aimed at the telecommunications industry, which is why it's the reigning champion, year-over-year, as the **#1 most attacked** (as seen above).

A successful attack on a telecom provider can impact entire networks, causing widespread outages. Network is a critical part of a country's infrastructure, and consequences from a disruption cause not just financial impact, but social and even public security impacts, too. Further, due to the large attack surface area (varying complexities of infrastructure, multiple targets with multiple points of entry), telecoms also strangely serve as test subjects for attackers seeking to refine new DDoS methods before targeting other industries.

Education

Our runner-up, DDoS attacks targeting education comprised 15% of all attacks this year – down slightly from 17% but still 62% more frequently than in 2023. Unsurprisingly, these attacks peaked just before exam time: April, October, and November saw a significantly greater volume of attacks than other months. For example, November had 5,571 attacks while there were 97 in June and 679 in July. It's no wonder the FCC introduced its Cybersecurity Pilot Program in 2024 - a widely popular program necessary to address this quickly-growing problem.

Checkpoint Research's recent blog on cybercrime targeting educational organizations points out a key reason why cybercriminals target these institutions: they contain a wealth of personally identifiable information that can be used for financial gain, drastically amplified by a digital infrastructure that hasn't had the resources to keep up with modern cyberattacks.



Cloud and SaaS

This industry nudged upward from 10% of all attacks in 2023 to 11% in 2024. That's still nearly 19,000 attacks throughout the year – 15,470 of which occurred in the second half.

We'll talk more about this industry in the size section of this report, but there's no surprise the share of attacks here is growing. More and more organizations rely on cloud and multi-cloud solutions: taking one of these providers offline can cause major downstream impacts. And if a critical cloud provider is down long or frequently enough, well, one might take their business elsewhere.

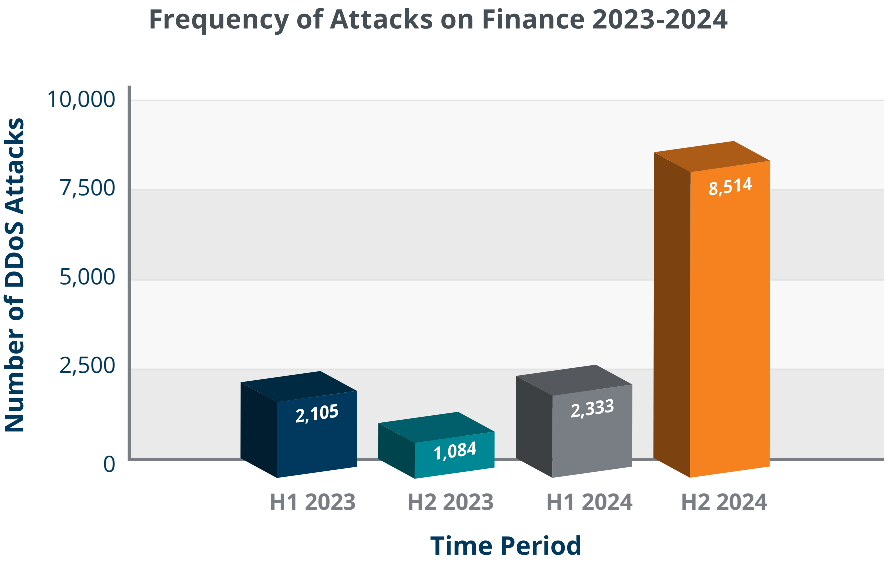
Know your enemies

Let's face it: it's a cutthroat world out there, and the truth is DDoS attacks are not just conducted by lone wolf hackers; businesses have been known to target competitors with these attacks as well. Research by Cloudflare shows that among those surveyed who *did* know where their attacks were coming from, 59% said they were from a competitor. The retail industry is especially rife with these attacks, noting major DDoS spikes during sales seasons (we saw a +300% burst in retail attack volume in October and November).

Finance

When it comes to the "biggest leap," finance takes 1st prize. In 2023, we observed just 3,189 total attacks on this industry (3.5% of all attacks). This year, the attack volume tripled to 10,847 attacks, comprising 7% of all attacks.

Not only do financial institutions rely on continuous, uninterrupted operations for their employees and their customers, but they are a wealth – no pun intended – of highly sensitive, highly ***valuable*** data should a hacker get their mitts on it. Beyond competitors working on taking each other down, you're also dealing with geopolitical forces and those looking to score a big ransomware payout.



Government

Spanning local, state, and federal government (as well as government institutions), this group of our customers comprised 8% of attacks in 2H 2024 and 5% of total attacks across all of 2024 – roughly the same as in 2023, which was also 5%. This still puts it in our Top 5 Attacked Industries leaderboard.

There are *endless* reasons why cybercriminals target government entities, sharing some commonalities with the other Top 5 Industries, such as the high volume of valuable and sensitive data these entities have access to. And with softer defenses due to varied levels of network sophistication and security solutions, this sector is certainly a magnet for deliberate, hard-hitting attacks.

What really sets it apart is these attacks tend to be more opportunistic, more motivated, and originating from a wider geographical footprint than others.

- **Opportunistic:** the timing of American politics is well publicized and easy to predict. With the November 2024 election, we clearly noticed a surge in attacks in September and October, among which 66% of all these attacks took place.
- **Motivated:** those seeking to send a message – or stop a message from being accessible – could target these institutions with perfectly timed attacks.
- **Broader:** whether state-sponsored attacks from other countries, coordination between multiple hacktivism groups, or anything in between, these attacks tend to originate from more distributed regions and botnets.

Healthcare

A participation trophy this industry probably isn't too pleased to receive, healthcare faced a 223% growth in the total number of attacks targeting it between 2023 and 2024. Though the healthcare industry has not yet reached the Top 5, this is a worrying trend that we should all keep an eye on.

The shift to digitization of records has been much-needed in the healthcare industry, but with that comes a more porous defense with more weak points than before. Zayo has been working closely with healthcare organizations of all sizes to shore up their defenses, with perfectly-built solutions for their needs including SD-WAN, which can feature a built-in firewall, SASE, and – of course – DDoS Protection.

The Timing Trend Continues

Those following our reports may notice the lack of a "timing" section in this report. We continue to monitor and analyze data on attack timing, and we will report on it if there are any changes in the trend. However, what we've seen in the past (and shared in past reports) continues to this day: DDoS attacks are timed intentionally to cause **maximum** chaos so, naturally, they predominantly take place during the work week across critical working hours: Monday-Friday, between noon and 5 pm Eastern.

The Duration of DDoS Attacks

Across all of 2024, an average DDoS attack lasted 39 minutes, and nearly 3,000 attacks lasted beyond 1 hour. In fact, 59 attacks this year lasted for more than 24 hours.

Despite massive growth in the frequency of attacks between 2H 2024 and 1H 2024, the average attack duration decreased in the second half of the year (from 45 minutes to 38 minutes).

A network outage of half an hour might seem like small potatoes at first glance, but it has a far greater impact than just inconvenience. First, experts still agree **the average financial cost of a DDoS attack is $6,000 per minute** (you can do the math here to see how all that adds up). Second, there's the exposure of your network to cybercriminals. Third, the reputational damage and poor customer and user experience can lead to lasting ramifications.

The **average financial cost** of a **DDoS attack** is **$6,000** per minute

The High Cost of Network Downtime

Imagine a bustling international airport at peak travel time. Flights are scheduled down to the minute, baggage is moving through conveyor belts, and thousands of passengers are checking in, going through security, and boarding planes. Suddenly, without warning, the entire airport's systems go offline.

The air traffic control tower loses communication with pilots, flights can't take off or land, and passengers are left stranded at gates, growing more impatient by the minute. Airlines start losing revenue as delays pile up, crew schedules get thrown into chaos, and missed connections create a domino effect of frustrated travelers.

Meanwhile, passengers scramble for alternatives – some book flights with competing airlines at nearby airports, while others cancel their trips altogether. Even after the systems are restored, the damage lingers – baggage is lost, customer trust is shaken, and flight schedules take hours or even days to return to normal.

This is what it's like when a business loses its network. Operations come to a standstill, customers look elsewhere, and even after recovery, **the ripple effects of downtime can last far longer than the outage itself.**

Industry Callouts

The average DDoS attack duration stayed relatively consistent for most industries this year, with a few noteworthy exceptions.

Government

Consistent with the nature of these attacks being opportunistic and motivated, the **average attack duration in 3Q'24 was 247 minutes**, dipping significantly to just 44 minutes in 4Q'24. The timing here is easily assumed to have the purpose of disorienting and discombobulating political groups' efforts approaching the November election.

Transportation

A bit of a sleeper in the first half of this year at an **average of 20 minutes per attack**, the duration of attacks on this industry grew quickly to 69 minutes on average in 3Q'24 and 134 minutes for 4Q'24. We predict attacks on this industry to continue to be volatile and unpredictable, and we'll provide more insight if consistent trends emerge.

Finance

In 2023, the duration of DDoS attacks targeting this industry soared – not so much in 2024. The **average attack time dwindled by about 50%**. However, it's important to contrast that to the massive increase in attack frequency we shared earlier. Will this trend of shorter burst attacks continue? We'll stay vigilant.

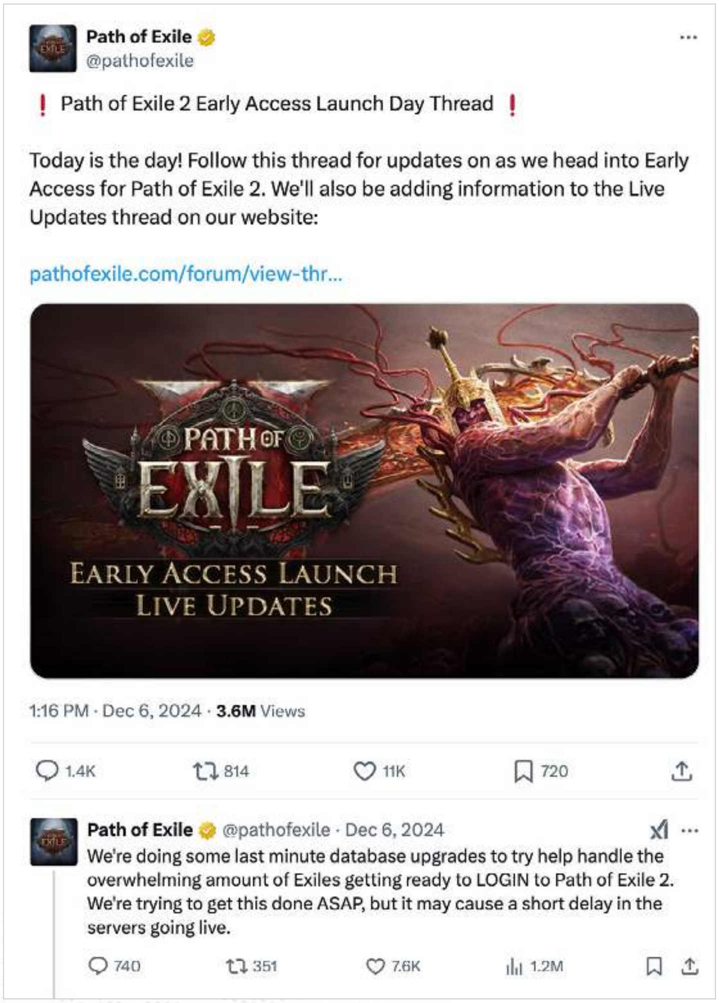
Not DDoSed, But Down – Sometimes It's Legitimate Traffic

When is a DDoS attack not actually a DDoS attack?

Well, quite often, actually. That's why it's vital for protection services like ours to be intelligent, targeted, and readily equipped with the most up-to-date traffic insights. **When choosing DDoS Protection, ensure you're getting a tool that equips you with the ability to easily configure your security thresholds and parameters.**

It's not uncommon for networks to receive a huge surge of traffic that ends up being legitimate. Perhaps it's a major news story, a topic that's trending on the front page of Reddit, or the highly anticipated launch of a new online video game. This exact thing happened in early December on the planned release day of Path of Exile 2 to a mid-sized New Zealand-based gaming company. Due to the massive hype around the release, more than a million anxiously-awaiting players overwhelmed the company's servers trying to log in at the same time.

Thankfully, in this case, the company and its network were prepared for this burst, and with just a bit of unexpected downtime and database work, they were up and running just about two hours later – which is a respectable feat in this industry.



Path of Exile
@pathofexile

❗ Path of Exile 2 Early Access Launch Day Thread ❗

Today is the day! Follow this thread for updates on as we head into Early Access for Path of Exile 2. We'll also be adding information to the Live Updates thread on our website:

pathofexile.com/forum/view-thr...

1:16 PM · Dec 6, 2024 · **3.6M** Views

Path of Exile @pathofexile · Dec 6, 2024
We're doing some last minute database upgrades to try help handle the overwhelming amount of Exiles getting ready to LOGIN to Path of Exile 2. We're trying to get this done ASAP, but it may cause a short delay in the servers going live.

A deep dive on burst attacks

In 2024, 86.78% of attacks lasted fewer than 10 minutes, and 10.26% of attacks were between 10 and 30 minutes. That means **97.04% of attacks lasted fewer than 30 minutes**.

A cause for celebration? Not quite.

Shorter duration attempts are often conducted intentionally, so defenders don't have time to manually analyze traffic and behaviors. This is why an automated protection system is necessary: attacks both large and small will **equally be protected without the need for manual intervention**, making all the posturing and strategy on an attacker's end completely irrelevant.

Remember, we're talking about the attack duration of DDoS attack **attempts** – despite Zayo quickly mitigating the attack (without impacting our customer), the attackers may choose to keep up their efforts, meaning the attack can go on for hours (and, therefore, mitigated for hours).

One reason you may see DDoS attack duration mitigated by Zayo as shorter than others is when the attackers realize they aren't breaking through our defenses, they stop their effort… giving up quicker than when they find a target with less security.

"Given the ever-growing rise of raw network capacity and the rapid expansion of intelligent tooling I expect we will see both **an increase in the volume of DDoS attack throughput** and **an increase in flexibility** as bad actors attempt to out-maneuver anti-DDoS measures that rely on sustained consistent attack patterns to detect and mitigate."

- Ed Loveless, Director, Product Management at Zayo

The Size of DDoS Attacks

The upward climb continues

The second half of 2024 continued the worrying trend of the first: DDoS attacks are only **getting larger across almost all industries observed**. We measure size by the amount of bandwidth used by the attack, impacting the amount of bandwidth needed to mitigate the attack.

Here's what we observed across individual industries from the first half of 2024 to the second half of 2024:

Change In Average Attack Size (in Gbps)

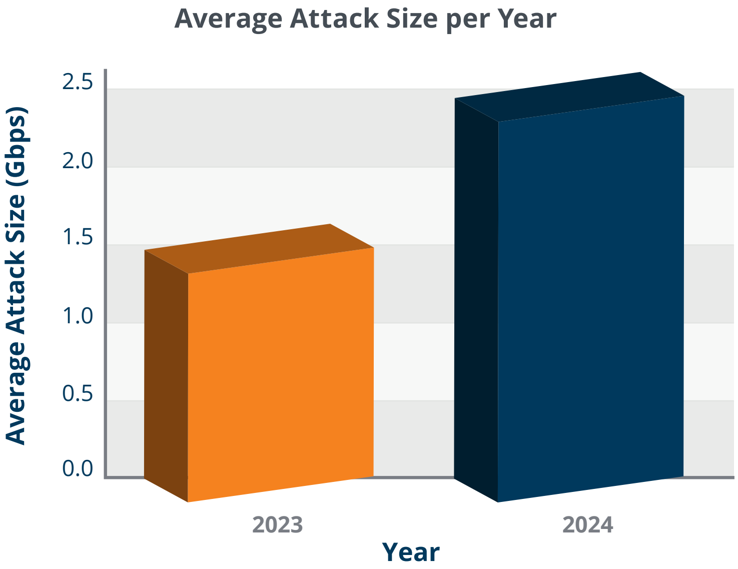
Industry	1H 2024	2H 2024	Δ
Cloud/SaaS	0.9	**4.0**	**▲318%**
Education	0.5	**0.3**	**▼-37%**
Energy, Utilities & Waste	1.2	**3.3**	**▲185%**
Finance	0.7	**2.0**	**▲201%**
Government	2.4	**2.6**	**▲10%**
Healthcare	4.3	**4.2**	**▼-2%**
Legal & Consulting	1.3	**2.5**	**▲101%**
Manufacturing	6.6	**8.5**	**▲28%**
Media and Entertainment	0.4	**0.5**	**▲19%**
Other	0.6	**1.5**	**▲159%**
Retail	1.1	**2.4**	**▲123%**
Telecom	1.5	**2.3**	**▲56%**
Transportation	1.2	**1.1**	**▼-9%**
HR and Staffing	3.5	**7.3**	**▲111%**

Let's take a look at some of the industries facing the largest attacks in the second half of 2024:

Cloud and SaaS: Increasingly on attackers' hit lists

With a market size projected to nearly triple in the next seven years, cloud and software-as-a-service (SaaS) companies are increasingly valuable targets for cybercriminals.

In fact, cloud and SaaS companies accounted for **half of all attacks by volume** recorded in the third quarter of 2024. Here's how the average attack size grew between 2023 and 2024:



Cyberattackers clearly have their sights set on companies in the cloud and SaaS space. But why are cloud and SaaS companies facing larger attacks? It could be for a few reasons, including:

- **The criticality of cloud and SaaS services:** As companies continue to digitize, cloud and SaaS services become even more vital to everyday operations. This means it's even more devastating when they're down due to a DDoS attack.
- **The sheer amount of bandwidth needed to overwhelm these targets:** Cloud and SaaS providers typically use massive amounts of bandwidth and resources to operate, meaning attackers must launch larger-scale attacks using more powerful techniques to make an impact.
- **The ripple effect of a DDoS attack on other companies:** Think of the impact a downed point-of-sale system software has on its retail customers, or an electronic health record outage for millions of patients, doctors, and hospital staff. The results of downed software or cloud systems can have catastrophic implications.
- **Multiple points of vulnerability in these companies' infrastructure:** The distributed nature and complexity of cloud services can mean more vulnerabilities for attackers to discover and exploit.

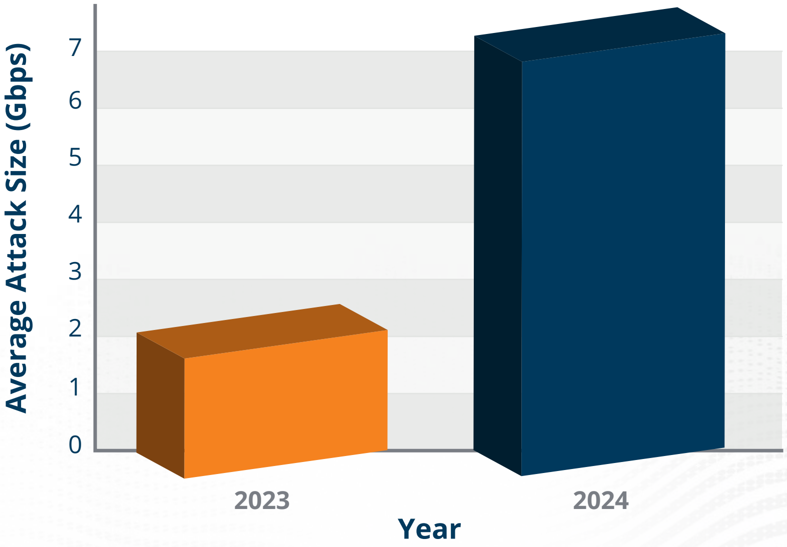
> “The increasing complexity and interconnectedness of networking environments open the door to new DDoS attack vectors. While it’s thrilling to see AI becoming a catalyst for growth and ingenuity, it presents an equally daunting platform for major disruptions”
>
> - **Noah Hagerty**, Product Director, Network Connectivity at Zayo

Manufacturing: A DDoS darling

Manufacturers continued to face a slew of large-scale attacks throughout 2024. With the **average attack size growing 257%** from 2023 to 2024, manufacturing companies made up almost 14% of DDoS attacks by volume in the second half of the year.

In the second half of the year, **the average attack size for a company in the manufacturing industry was around 8.5 Gbps**, suggesting that the average size of attack for these companies is only continuing to grow.

Updated Average Attack Size per Year



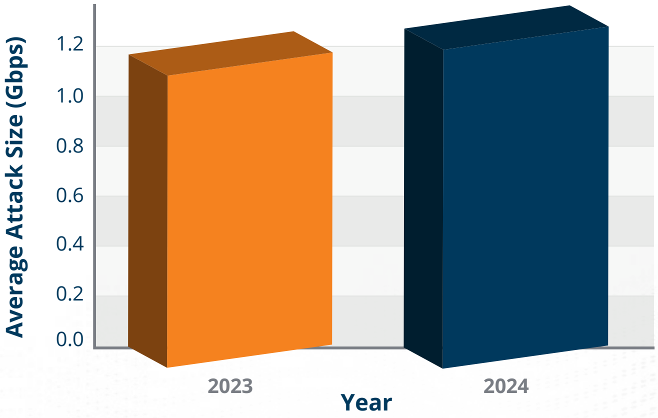
Manufacturers continue to be top targets for cybercriminals. Why is that? According to IBM X-Force's 2024 Threat Intelligence Report, there are a few key reasons:

- **Any downtime is extremely costly to manufacturers:** Aberdeen Research estimates that unplanned downtime can cost a manufacturer up to $260,000 an hour. Downtime halts production, crunches revenue, and leads to delays and a drop in customer satisfaction.
- **Manufacturing data is valuable:** While DDoS attacks won't directly result in stolen data or credentials, they can often act as a distraction for other types of attacks that will. They can also help attackers identify vulnerabilities that can aid them in stealing valuable data in a secondary attack.
- **Industrial Internet of Things (IIoT) adoption has widened the attack surface:** According to recent data, nearly two-thirds of manufacturers have adopted IoT in manufacturing or assembly processes. The plethora of IoT devices spread across distributed locations – many lacking strong endpoint security – across manufacturing operations creates more entry points for cybercriminals to exploit.

Finance: Following the money

Though the finance industry only saw slight growth in the average attack size between 2023 and 2024, we feel this industry is worth keeping an eye on. With **an average attack size of 2.0 Gbps in the second half of 2024** – a sharp increase from the previous half – financial sector companies must implement robust DDoS Protection to maintain an edge over cybercriminals.

Average Attack Size per Year



The largest attack Zayo mitigated in 2H 2024 was **443 Gbps** and targeted a French retailer.

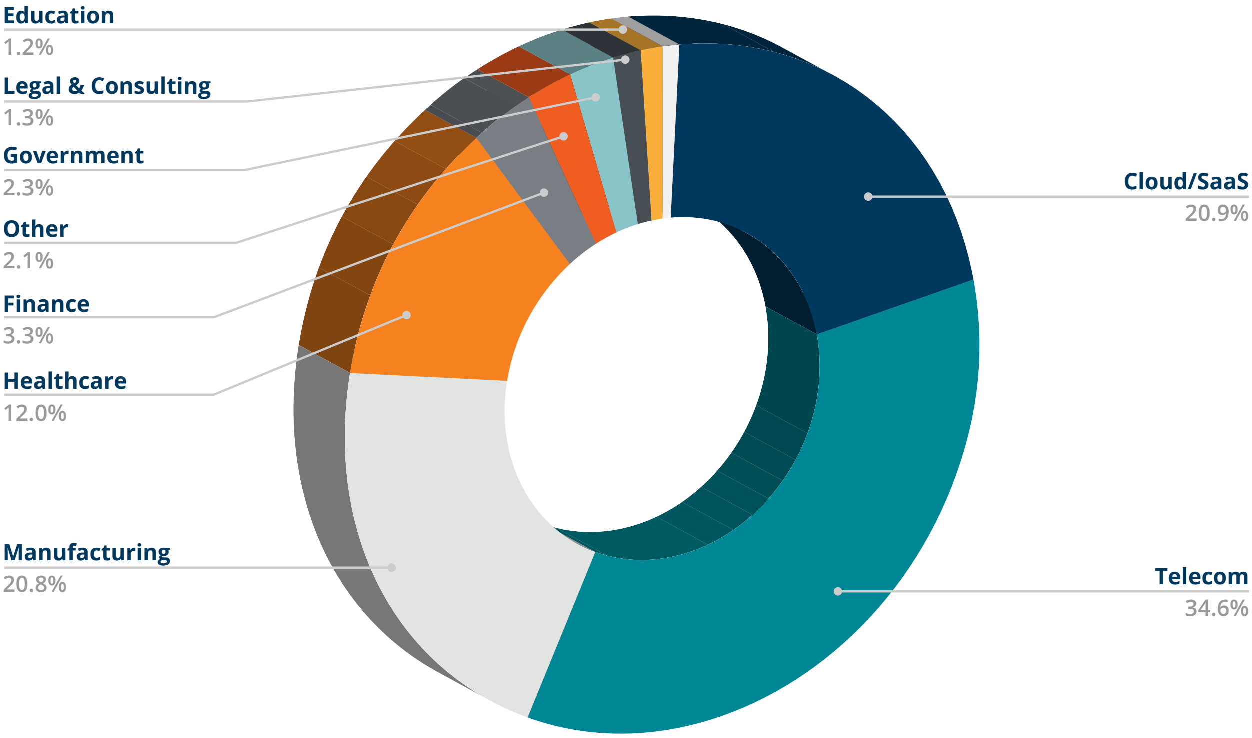
It's perhaps no surprise that financial firms – banks, investment firms, credit unions, you know, any business that deals primarily with money – find themselves the target of attackers. **With money, reputation, and sensitive data to lose**, why a financial institution *wouldn't* purchase DDoS Protection is anyone's guess.

And now, the winner's circle no one wants to be a part of... the top 10% of industries attacked by size!

Looking at only the top 10% of attacks by size in the second half of 2024, nearly 89% of the largest attacks targeted four industries: **cloud and SaaS, telecommunications, healthcare, and manufacturing**.

Of the largest 10% of attacks, here's who was targeted:

Top 10% of DDoS Attacks by Size



Telecommunications, healthcare, and manufacturing remain targets of some of the largest DDoS attacks. While the HR and staffing industry made the shortlist in our last report, the cloud and SaaS industry edged them out for a spot on the leaderboard this time around.

Once again absent from our leaderboard in this report are government entities. **Government entities made up just 2.16%** of the top 10% sized attacks in the second half of 2024, despite the industry being one of the most frequently attacked industries with some of the longest attacks during the same period. This tells us that attackers targeting government entities are opportunistic, targeting their victims with specific timing in mind to unpredictably cause maximum disruption.

Zayo mitigated a grand total of 793.4 TB of traffic in 2024

Tips on visualizing 800 Terabytes of malicious traffic:

1. Imagine an all-day Zoom call, then extend a little bit further: **2,500 years** should do it – with an average one-hour Zoom call being roughly 300Mb.
2. Get out the popcorn for **18 years** of binge-watching: at roughly 5 gigs per hour, that's about 160,000 hours of high-resolution video. Re-runs might be required.
3. Catch up on sleep by reading every "Terms & Conditions" document ever ignored; assuming each is 1 MB, that's **800 million** overly wordy agreements.
4. Just think to yourself: "That's a **really** big number," activate a DDoS Protection service, and set aside all that stress.

Why does the size of DDoS attacks continue to grow?

There are a few reasons we may be seeing larger average DDoS attack sizes in general:

1. Attackers are using **larger botnets**, or networks of compromised devices, to launch attacks. With more IoT devices coming online each year come more potential soldiers for an attacker's botnet army, increasing the potential size of attacks.
2. Cybercriminals are using advanced techniques like **amplification and reflection techniques** to increase the size of attacks. Both techniques involve tricking legitimate servers into sending large amounts of data to a target to overwhelm their systems.
3. DDoS attackers are constantly finding **new vulnerabilities** in software and network protocols to exploit. The proliferation of IoT devices, the deployment of 5G networks, and the introduction of new software tools to the market all offer new vulnerabilities for bad actors to take advantage of.
4. **Cloud services** provide new ways for cybercriminals to launch powerful, large-scale attacks. Misconfigured or compromised cloud environments can be used to launch attacks and generate large amounts of traffic.
5. **Higher bandwidth availability** also lends to larger DDoS attacks. With more bandwidth at their disposal, attackers can send even larger volumes of traffic to their targets.

The Future of DDoS (and Other Cyber) Attacks

DDoS attacks and other cyber attacks aren't going away anytime soon.

They will likely only become more sophisticated, more complex, and more damaging. We asked our experts to weigh in on this concerning trend – what do they anticipate will shape the future of cyber attacks and cybersecurity and how can we get ahead of looming threats?

Here's what Zayo's cybersecurity experts predict for 2025 and beyond:

AI-driven automation will make DDoS detection and mitigation more challenging

"Attackers will likely leverage **AI-driven automation to scale and refine multi-vector attacks in real-time**, making detection and mitigation more challenging. The exploitation of IoT devices and edge computing environments will further amplify these attacks, increasing their size and impact."

- Shawn Edwards, Chief Security Officer

While AI is being used to help detect and mitigate attacks with greater efficiency in real-time, it's also being used to perform them, making a bigger impact on attackers' targets.

Today, more **sophisticated attackers use AI to enhance the effectiveness of their botnets, making attacks harder to mitigate**. Tyler Burke explains how they work: "These AI-driven botnets could autonomously identify and exploit vulnerabilities, resulting in more effective and widespread attacks."

Zayo Product Director Ed Loveless adds, "Given the rise in AI agents and open tooling I expect to see DDoS extortion to ramp back up as malicious actors are able to automate a full pipeline to extort and interact with targets via AI tooling, and then leverage DDoS for hire services to enforce the threats. What was a manual process and very effective and destructive to many businesses at the start of the COVID lockdowns, now is easily orchestrated at scale today."

These evolving threats make robust cyber protection even more of a necessity. As artificial intelligence technologies continue to improve, the scale and complexity of these attacks will likely also improve.

Governments will impose stricter cybersecurity regulations

Regulations like the Digital Operational Resilience Act (DORA), which took effect in the European Union in January 2025 and applies to financial institutions, will impose cybersecurity mandates on targeted industries. Similar federal regulations like the PCI DSS 4.0 and National Institute for Standards and Technology (NIST) 800-171 are expected to tighten in the United States.

Organizations operating in affected industries must stay ahead of regulatory changes and think globally, as different standards apply in different regions of the world.

> "I suspect governments will impose stricter cybersecurity regulations, especially for critical infrastructure, driving compliance demands, but also **creating opportunities for organizations to stand out with advanced security measures.**"
>
> - **Shawn Edwards**, Chief Security Officer

Insider threats will continue to evolve

“Insider threats will continue to evolve as **attackers focus on planting operatives within companies or coercing outsiders**, making robust detection and a culture of security vigilance imperative.” – Shawn Edwards, Chief Security Officer

Cyber attackers may not look like the stereotypical masked, hooded, gloved cybercriminal hunched over a laptop surrounded by dozens of monitors typing code furiously. They may just look like Bob from IT.

Companies have a real problem on their hands when those with legitimate access within an organization use it to bypass security measures, steal data, halt operations, or deliberately launch cyber attacks. While we often think of weak passwords and sketchy email links as the origin of insider threats, sometimes insiders act deliberately to put their organization at risk.

It’s paramount that IT leaders stay alert, implement Zero Trust access, monitor suspicious behavior, and ensure proper training to minimize insider threats.

DDoS-as-a-service will continue to rise in popularity

It’s easier than ever for even the most unsophisticated cybercriminal to conduct a DDoS attack. DDoS-as-a-Service (DDoSaaS) providers reduce the barrier to entry for these low-budget, less technical cybercriminals by making it possible for attackers to leverage existing infrastructure to launch an attack instead of building their own.

Many DDoSaaS providers advertise their services on popular messaging applications, making launching a DDoS attack more accessible and available while increasing the anonymity of the attacker.

> “The availability of DDoS-as-a-Service and other cybercrime tools is expected to increase, enabling **even individuals with limited technical skills to conduct attacks**. This trend may result in a greater number of attackers and a wider variety of attack methods.”
>
> - **Tyler Burke**, Product Manager, Network Connectivity

Supply chain attacks will remain a key issue

By targeting upstream providers, attackers can make a larger impact, compromising downstream organizations that rely on the provider's services. What's more, nation-state actors often can conduct more advanced cyber attacks that allow them to easily gain access to intelligence and disrupt critical infrastructure.

Organizations and government entities must do their due diligence in evaluating third-party vendors' security measures. Implementing Zero-Trust security models and developing robust incident response plans can help organizations avoid and respond to these attacks.

"**Supply chain attacks will continue to grow**, with nation-states targeting upstream providers to infiltrate critical organizations through trusted relationships."

- Shawn Edwards, Chief Security Officer

What's Your Cybersecurity Strategy?

If you've made it this far, you know that operating without the proper DDoS protection in place is a massive risk.

This is the part where we tell you we have the solution.

Luckily, Zayo makes it easy to protect your business against costly DDoS attacks with a comprehensive, in-line, network-based DDoS Protection solution designed to ensure uninterrupted availability.

Zayo's DDoS Protection solution...

Safeguards every Zayo IP at the network level with a single subscription.

With network-level filtering, you can rest assured that our solution will detect and mitigate malicious traffic before it reaches individual devices or critical services.

Minimizes disruptive traffic flows without compromising latency.

Our DDoS Protection solution leverages Zayo's Tier-1 network backbone and over 35 Tb/s of peering capacity.

Is incredibly proactive.

Zayo's DDoS Protection just got even better. Our latest upgrade, the NETSCOUT® ATLAS® advanced intelligence feed (AIF), incorporates human intelligence and live traffic forensics to accurately and automatically detect and block inbound DDoS attacks and minimize false positives.

Doesn't use GRE tunnels.

Avoid the potential for additional latency, configuration complexity, and vulnerabilities introduced with GRE tunnels.

Is available to any Zayo Dedicated Internet Access (DIA) and IP Transit customers.

Our solution doesn't require any additional hardware – our solution seamlessly protects all IP services running on Zayo's network.

Can protect all of your network traffic.

Yes, even if you're using a competitor's network. We promise not to hold it against you. Our Multi-Carrier DDoS Protection solution protects Zayo and non-Zayo IP traffic from DDoS attacks.

Includes round-the-clock support.

Our Security Operations Center (SOC) and Network Operations Center (NOC) have your back, 24/7/365.

While the purpose of this report is to warn you against the risks associated with DDoS attacks, inform you about DDoS attack trends, and encourage you to protect your business, DDoS Protection is only one part of the solution.

Maintaining a robust cybersecurity posture means protecting your network, devices, users, locations, and applications at every level. Here at Zayo, **we don't just protect our customers from DDoS attacks – we offer additional cybersecurity solutions to keep your business safe** including:

Secure Access Service Edge (SASE): Zayo SASE is a cloud-based, end-to-end solution that provides comprehensive protection from edge to core to cloud leveraging SD-WAN, SASE PoPs, data center, and Tier-1 Internet connections. Zayo can deploy the solution using our customers' existing network infrastructure or as an upgrade to our massive infrastructure. Zayo's vendor-agnostic solution connects and protects distributed users, devices, and locations to applications and data, all while optimizing performance.

Managed Firewall: Zayo's Managed Firewall service protects network traffic at the core and edge from cyberattacks, viruses, malware, data leaks, and unauthorized users.

Moreover, security is baked into every solution at every layer of our network. Whether it's advanced monitoring features offered through our market-leading zInsights platform or designing our fiber network for maximum physical security and resilience, security is a key component of every Zayo solution.

As cyberattacks become more frequent and sophisticated, Zayo commits to remaining one step ahead of attackers, continually innovating and keeping a pulse on trends to ensure our customers remain secure.

Secure Your Organization With Zayo Today

Learn more about protecting your organization from a DDoS attack.

Contact us to get started.