Real-time DDoS Protection against complex attacks

Protect your infrastructure against the most complex and powerful DDoS attacks with Gcore. Introducing a comprehensive protection solution for the network (L3,) transport (L4,) and application (L7) layers, operating in data centers around the world.

DDoS attacks are growing in complexity every year and can result in significant financial losses for businesses across all industries — potentially amounting to millions of dollars. Don't let your company become a victim. Prepare now and ensure the protection of your reputation, revenue, and customer base.

Our solution

Over 1 Tbps total filtering capacity | **SLA 99.99%** | **Global coverage across 6 continents**

Twice yearly, we publish Gcore Radar. This report presents the current state of the DDoS protection market based on Gcore's statistics. In 2023, we've seen figures indicating the increasing importance of DDoS protection.

Key Highlights from 2023 Q1–Q2

- The maximum attack power rose from **600 to 800 Gbps.**
- The most-attacked business sectors are **gaming, telecom, and financial.**
- The longest attack duration in the year's first half was **seven days, sixteen hours, and 22 minutes.**
- Most attacks lasted less than **four hours.**

As the number of IoT and 5G devices continues to grow, so does the volume and risk of attacks globally. Every one of these devices has potential to be hacked and become part of a botnet.

Protection against all types of DDoS attacks

Volumetric attacks

This form of attack targets and overloads the entire available bandwidth of clients, and in some instances, the entire data center. By employing a variety of methods, such as UDP and ICMP flows, and attacks aimed at amplifying traffic, it obstructs legitimate users' access to servers and applications. Common subtypes include:

- **UDP flood**
- **ICMP flood**
- **IP/ICMP fragmentation**
- **IPSec flood**
- **Amplification attacks**
- **Ping of death**

Connection attacks

In a connection attack, network devices or systems utilize internal tables with finite resources or features to track ongoing connections. When these tables are flooded with excessive connections, new users are prevented from establishing a link. In extreme cases, such overwhelming can cause device crashes, leading to a loss of connection for all active users. Specific methods include:

- **SYN flood**
- **SYN+ACK flood**
- **ACK flood**
- **RST flood**
- **TCP attacks**

Application attacks

Application attacks occur when servers are inundated with complex requests, leading to the consumption of all available CPU and memory resources. This type of assault can severely impact server performance. Examples of these malicious attacks include:

- **HTTP**
- **HTTP get/post flood**
- **Slow attacks like slowloris**
- **Game server attacks**
- **DNS cache poisoning**
- **L7 UDP flood**
- **L7 TCP flood**

Technological advantages

- **Proprietary DDoS protection solution**
- **Over 1 Tbps total filtering capacity**
- **Near-zero false positives**
- **Protection against L3, L4, and L7 attacks**
- **SLA 99.99%**
- **Easy deployment and high degree of customization**
- **High- and low-frequency attack detection from the first query**
- **GDPR compliance**
- **24/7 highly-skilled technical support**

We provide 3 types of remote DDoS protection integration

Protected servers

Purchase servers equipped with proprietary, inbuilt DDoS protection. Deploy instances across 16 global locations, safeguarding your resources against attacks at the L3, L4, and L7 layers. With over 1 Tbps attack filtering capacity and 99.9% guaranteed availability (SLA), you can rely on Gcore's secure cloud servers.

GRE tunneling

Defend your infrastructure by implementing GRE tunneling within your data center to protect your server anywhere in the world.

White Label

Resell our comprehensive, fully customizable White Label solutions. Ideal for ISPs, IIGs, CSPs, and partners aiming to extend their brand and enhance business scalability.

Protection algorithm

Step 1: **Resource analysis**

The system analyzes resource load in real time to detect any statistical anomalies that may indicate malicious activity.

Step 2: **Technical analysis**

Every new query is subjected to an initial technical examination. This includes, for example, analyzing the median size of network packets sent by the client.

Step 3: **Behavioral factor recognition**

If multiple queries are sent by a client within a monitored time frame, the system evaluates the client's behavior on the website, such as the time intervals between queries and subqueries.

Step 4: **Query check**

Queries are scrutinized against current suspicious signatures relevant to the resource, with both exact matches and near matches ("proximity") being evaluated.

Step 5: **Query validity conclusion**

The data collected from the previous steps is synthesized into a factor vector. This composite information is then used to determine the validity of the query, helping to ensure accurate and robust protection.

Games we protect

- **Wargaming games**
- **All HL1/HL2 games and mods**
- **GTA V: SA**
- **GTA V: FiveM**
- **RUST**
- **Counter-Strike 1.6**
- **Team Fortress 2**
- **Left 4 Dead 2**
- **Counter-Strike: Global Offensive**
- **Rag Doll Kung Fu**
- **The Ship**
- **Garry’s Mod**
- **Nuclear Dawn**
- **Dino D-Day**
- **Arma 3**
- **Call of Duty: Modern Warfare 3**
- **Starbound**
- **Space Engineers**
- **7 Days to Die**
- **Quake Live**
- **ARK: Survival Evolved**
- **Minecraft**
- **Battlefield 4**
- **TeamSpeak 3**

Trust in Gcore for your protection: **secure your company's future by entrusting infrastructure protection to an experienced provider. As a hosting and cloud provider, Gcore has years of expertise in server protection.**

Outstanding protection at an outstanding price

- We use the 95th percentile to charge for traffic. 5% of peak traffic is not taken into account when billed.
- We offer SLA 99.99%. In case of security failure, we refund you.
- We save you time and money. You don't need to maintain costly on-premises infrastructure.

Trusted by

WARGAMING.NET LET'S BATTLE

RedFox Games

Albion ONLINE

Gcore is an international leader in public cloud and edge computing, content delivery, hosting, and security solutions.

We manage a global infrastructure designed to provide enterprise-level businesses with first-class edge and cloud-based services.

Gcore is headquartered in Luxembourg with ten offices worldwide.

Want to test our DDoS Protection for free?

Just reach out. Stay safe with Gcore.

gcore.com +352 208 80 507 sales@gcore.com