All-in-one Web Application Security Solution

- DDoS Protection ✦
- Web Application Firewall (WAF) ✦
- Bot Protection ✦
- API Protection ✦

Introducing Gcore's comprehensive Web Application Security solution. We protect your web applications and services against DDoS attacks (L3, L4, L7,) OWASP Top-10 threats, zero-day vulnerabilities, and malicious bots.

SLA 99.99%	Zero-day attack detection	Block malicious sessions, not IPs

Key benefits

→ **Keep your service available** even under the strongest attacks

→ **Stay focused on your primary business** and let us handle web security fortifications

→ **Protect your application** from different attack vectors while maintaining performance

→ **Save money** by avoiding costly web filtering and network appliances

Why businesses need web security

Growing attack surface

As the prevalence of doing business online expands globally, the prevalence of web attacks grows, requiring companies to stay one step ahead of attackers.

Sensitive data protection

Data security is paramount in safeguarding customers' personal, financial, and health information, demanding a diligent approach from companies.

Sophisticated threats

To counter the escalating OWASP Top-10 risks and other sophisticated threats, organizations must employ a modern WAF to mitigate potential harm.

API abuse prevention

Automated behavioral attacks are on the rise, including malicious bots and application layer (L7) DDoS attacks, causing disruptions to end-user experience and posing significant risks to essential business services and making API abuse prevention essential.

The average cost of a data breach varies across sectors, with the highest average cost in the healthcare industry at a staggering average of over $10 million.

The financial industry ranked second, at almost $6 million per breach.

The public sector ranked last, still costing an average of $2 million for each attack.

Keep your customers' data in safe hands with Gcore, regardless of your industry.

WAAP

The **PCI DSS (Payment Card Industry Data Security Standard)** mandates the use of a WAF for organizations handling payment card data. Any company dealing with sensitive financial information must employ a WAF, regardless of industry.

However, the ever-evolving digital landscape has given rise to increasingly sophisticated intruder attacks. In today's environment, API security requires more comprehensive protection beyond what a traditional WAF can offer. Instead, you need WAF and API Protection, now available from Gcore's WAAP in one ready-to-use, powerful solution.

How WAAP works

WAAP is a universal solution for protecting all web resources and API types, thanks to its flexibility and vast number of precise settings. This results in near-zero false positives. Here's how WAAP works:

Scans incoming traffic in real time

Verifies traffic according to an existing rule set

Scores request features based on the set weights

Blocks requests if their total score exceeds the threshold

Scans web resources to detect and prevent potential vulnerabilities and zero-day attacks

Gcore WAAP guarantees

Safeguard sensitive data to meet GDPR, PCI DSS and other data protection requirements. Meet compliance requirements by tracking and protecting sensitive data usage, such as personally identifiable information (PII), financial data, and healthcare data.

Protect against the OWASP Top 10 to avoid current major security threats.

Stop zero-day attacks in their tracks.

Protect against unpatched vulnerabilities, as well as malicious programs against which no specific protection mechanisms have yet been developed, eliminating the risks of malicious exposure to zero-day attacks.

Guard against API-specific attacks. Don't worry about organizational risks — your API endpoints are securely protected.

Protect against credential stuffing, account takeover (ATO), and brute-force attacks. Stop behavior-based attacks by checking and matching query sequences. Intelligent rate limiting prevents botnets from overloading your resources.

Deploy rate limiting to ensure botnets don't overload your resources.
Use virtual patching to eliminate the risks of malicious exposure to zero-day attacks by patching found vulnerabilities.

Use virtual patching to eliminate the risks of malicious exposure to zero-day attacks by patching found vulnerabilities.

DDoS Protection

Our DDoS protection layer guarantees continuous application operation, even during massive attacks at the network (L3,) transport (L4,) and application (L7) layers.

Protect against numerous DDoS attack vectors:

- UDP/ICM/TLS flood
- ACK/RST/SYN flood
- TCP/amplification attacks
- IP/ICMP fragmentation
- Ping of death
- HTTP/HTTPS flood

How our protection algorithm works

Resource analysis
The resource load is analyzed in real time to identify any statistical abnormalities.

Technical analysis
Each new query undergoes a basic technical analysis of the client who sent it. For example, the median size of network packets is analyzed.

Behavioral factor recognition
If a client has sent more than one query within the monitored time period, then the client’s behavior on the website is analyzed. For example, the time between queries and subqueries is checked.

Query check
The query is checked against suspicious signatures currently relevant to the resource. Both coincidence and “proximity” can be checked.

Query validity conclusion
The information from these various factors is combined into a factor vector that is used to calculate query validity.

What’s unique about Gcore DDoS protection?

- Over 1 Tbps total filtering capacity
- Near-zero false positives
- SLA 99.99%
- Real-time statistics
- Easy deployment
- GDPR compliance
- Low-frequency attacks detection from the first query
- 24/7 expert technical support

Bot Protection

All online enterprises face a significant threat from bots, encompassing APIs, websites, mobile applications, and payment systems. Bots can be programmed to overwhelm resources, engage in website parsing, hack user profiles, send spam, and perform other malicious actions, posing potential financial and reputational losses for companies.

As the number of smart devices used globally increases exponentially, the number of devices with potential for being hacked also increases. Every internet-connected device can potentially be used by hackers, including to form botnets. Bot Protection is essential to stop new and sophisticated bot attacks, essential to safeguarding clients' data and upholding every company's reputation.

The detrimental impact of malicious bots on your business

Account hacking and bank card fraud

Malicious bots can exploit stolen login and password databases to gain unauthorized access to user accounts, potentially leading to leaks of both customer personal data and payment information.

Content theft

Bots can unlawfully copy and steal your valuable digital content — including product and service descriptions, infographics, and expertise — for competitive intelligence, resale, or fraudulent resource aggregation.

Scalping

In various markets, such as concert ticket sales, bots engage in scalping. By purchasing items and reselling them at inflated prices, bots can negatively affect your company's reputation.

Corrupted analytics

Malicious bots can distort your metrics, compromising your ability to optimize conversion rates and enhance user interface efficiency. Ensuring clean data is crucial for making informed decisions.

Advertising fraud

Launching advertising campaigns can attract bot traffic, resulting in wasted expenses and advertising fraud. Safeguarding your resources is essential to obtaining genuine leads.

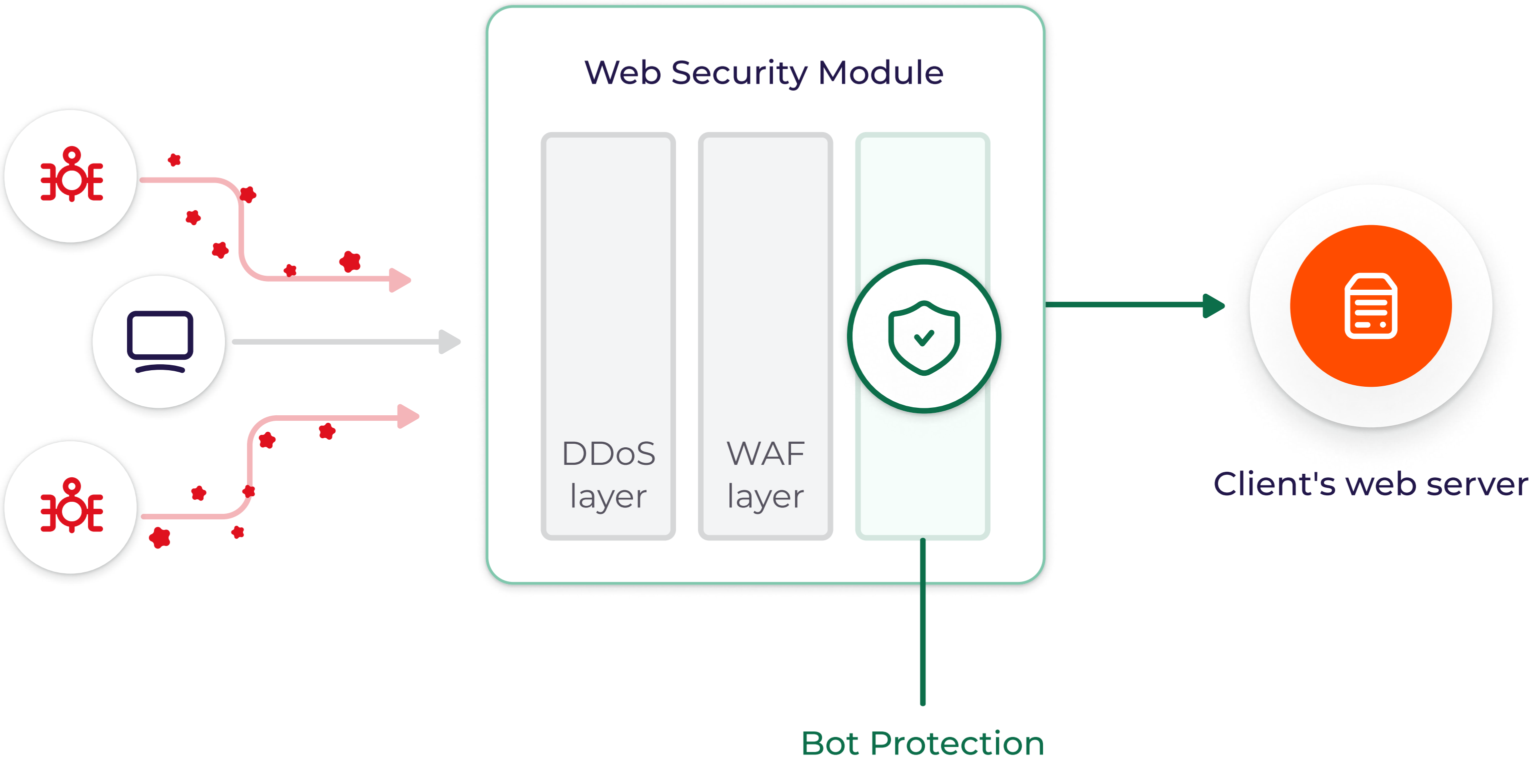
Parsing for the competition

Bots can collect price quotes from your website, providing valuable information to your competitors for competitive advantage.

Bots mimic user activity to perform inappropriate operations

Bot Protection module detects robotic activities and drops the connections

Client's workflow communicates only with real users



Web Security Module

DDoS layer

WAF layer

Client's web server

Bot Protection

Gcore Web Security guarantees

- SLA of 99.99%, with a money-back guarantee.
- Traffic is calculated based on the 95th percentile. We don't take into account the top 5% peak traffic surges for your resource, meaning you won't have to pay for traffic surges during specials and in emergency situations.
- The false positive rate is less than 0.01%.
- Expert technical support is available 24/7.

Using Gcore's Web Application Security services save your time and money. Even under an active attack, your business processes will continue as normal, and your users and customers won't notice anything is happening.

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.

Trusted by

WARGAMING.NET LET'S BATTLE

RedFox Games

Albion ONLINE

Want to test our Web Application Security for free?

Reach out. Stay safe with Gcore.

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