CORE

Web application protection against DDoS attacks, bots, and hacking in real time

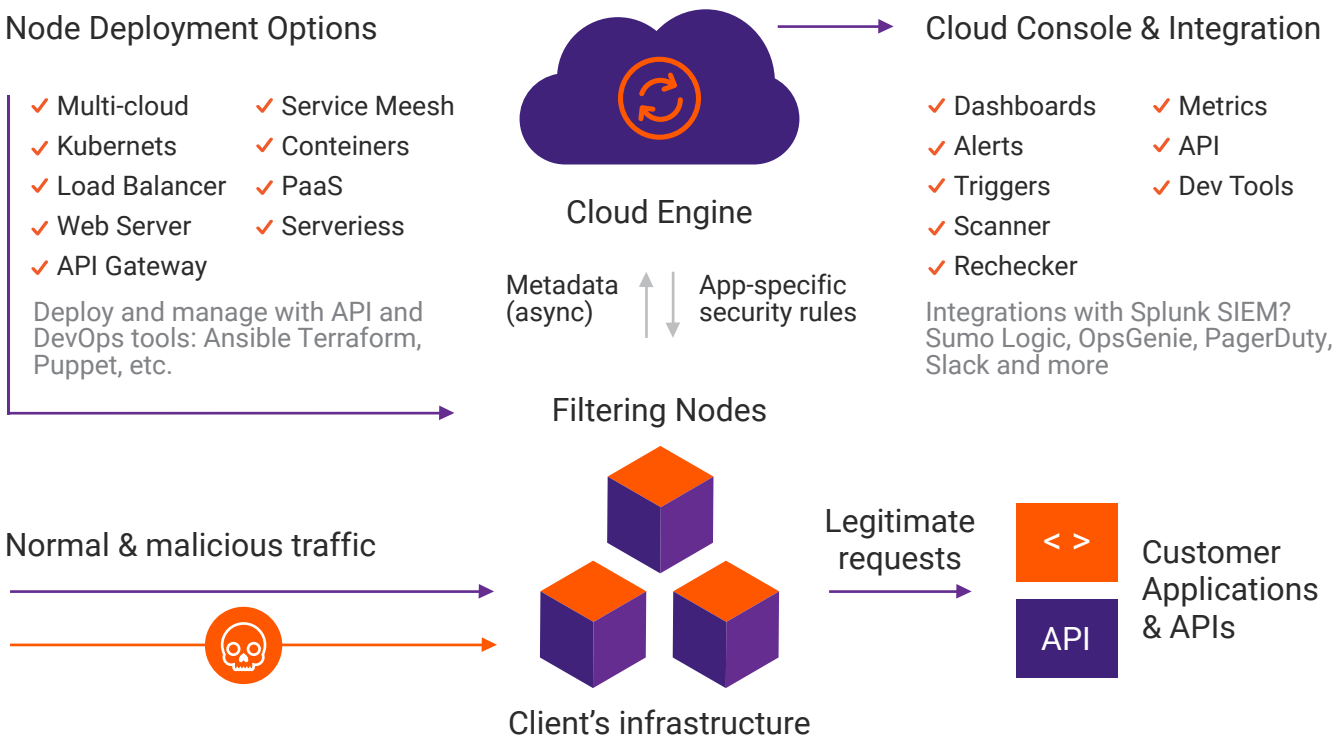
Introducing a comprehensive solution for protecting web applications, APIs, and microservices against DDoS attacks at L7 and the primary threats of the OWASP Top 10.

We will detect and prevent any attacks—even low-frequency attacks on your web resource — in good time, as well as eliminate the possibility of its vulnerabilities being exploited.

About the traffic cleaning platform

The cloud platform consists of our own traffic filtering centers in Europe.

Each node processes at least 160 Gbps of active traffic. This makes the total effective filtering bandwidth more than 1.5 Tbps. The nodes are connected to several service providers and they have backup copies of all systems, such as cleaning servers, managing servers, data storage systems, and network equipment.



How DDoS protection at L7 works

✓ Resource analysis

Resource load is analyzed in real time for 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 period of time, then the client's behavior on the website is analyzed (for example, the time between queries and subqueries).

✓ Query check

The query is checked against suspicious signatures currently relevant for the resource. Both coincidence and "proximity" can be checked.

✓ Query validity conclusion

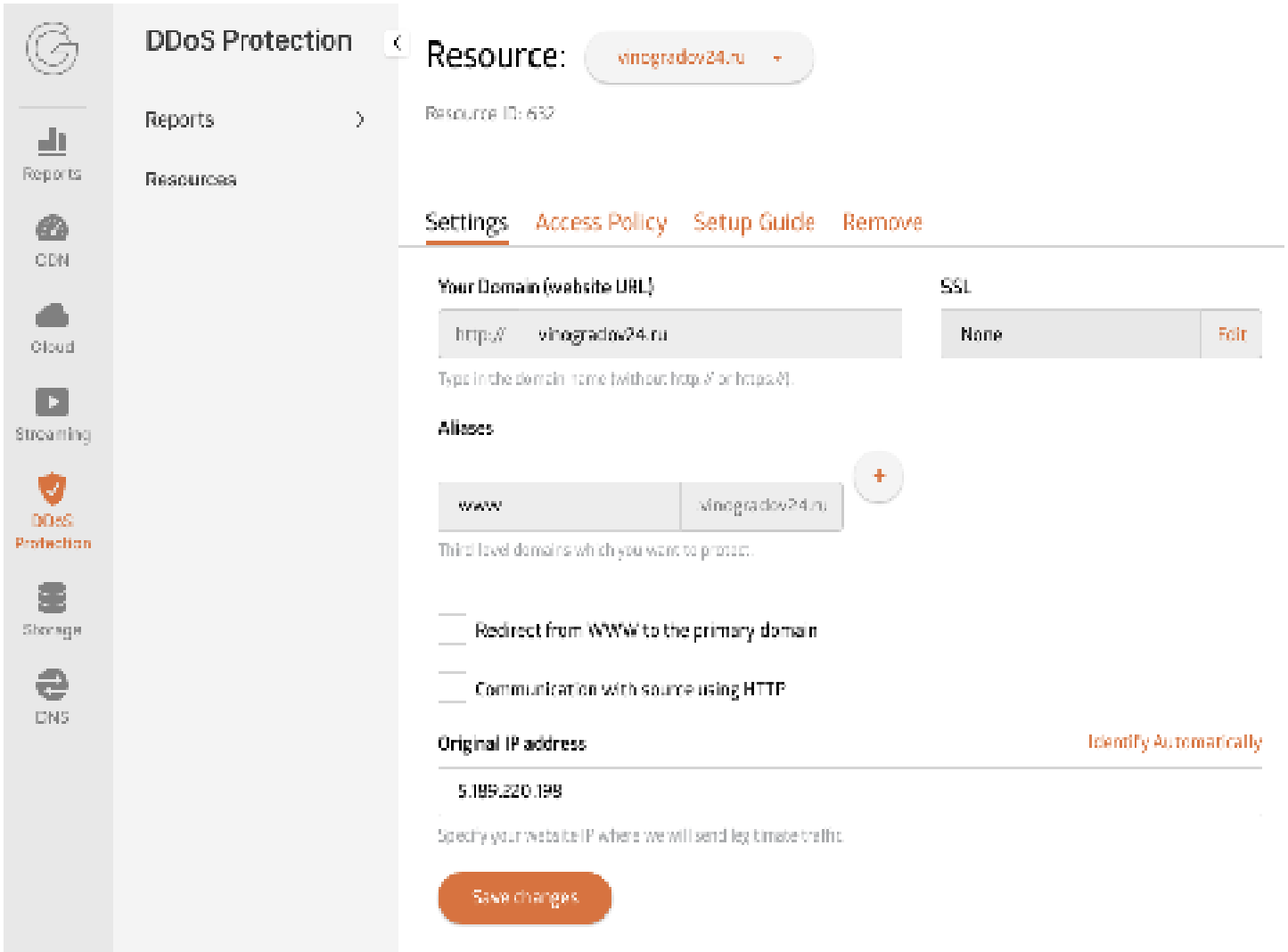
As a result, the information is combined into a factor vector that is used to calculate query validity.

Technological advantages

- ✓ We protect you against low-frequency attacks starting with the first query
- ✓ We block sessions, not IP addresses
- ✓ We support whitelists and blacklists of IP addresses
- ✓ We support HTTP/2, IPv6, and web sockets
- ✓ We support HTTPS with and without disclosing SSL certificates
- ✓ We provide load balancing, including Round Robin, Weighted Round Robin, and IP hash
- ✓ We provide statistics in your personal account

How DDoS protection at L7 works

Web protection control panel interface



How a WAF works

Blocks the majority of attacks on web applications. Can work with large amounts of traffic.
The unsupervised training algorithm helps prevent false positives.

Proactive filter

- ✓ Blocks the majority of attacks on web applications. Can work with large amounts of traffic.
- ✓ The unsupervised training algorithm helps prevent false positives.

Vulnerability detection system

- ✓ Detects existing safety errors within web applications.
- ✓ Provides information about detected vulnerabilities and detailed recommendations on how to eliminate them.

Virtual Patching system

- ✓ Protects applications from vulnerabilities by detecting and blocking attacks and hacking attempts in real time.

Technological advantages

- ✓ Non-signature (statistical) analysis methods don't affect legitimate traffic
- ✓ Detection of new types of attacks whose signatures are not in the knowledge base
- ✓ Support for applications in Ruby, PHP, .NET, Perl, Python, and other languages
- ✓ Automatic monitoring of vulnerabilities until they are fixed
- ✓ Vulnerability elimination quality control
- ✓ Doesn't require any additional equipment, software, or changes in the application code
- ✓ No resource downtime required

CORE

Our guarantees

- The guaranteed availability of your resources is no less than 99.5%. If we can't protect you, we return your money.
- Traffic is calculated based on the 95th percentile We don't take into account 5% of peak traffic surges for your resource (you won't have to pay for traffic surges during specials and in emergency situations).
- The false positive rate is less than 0.01%
- Competent technical support 24/7

We are trusted

WARGAMING.NET

RedFox Games

BANDAI NAMCO

Albion ONLINE

avast

SANDBOX INTERACTIVE

G-Core is a global provider of strong solutions for online business for storing, delivering, and protecting any web content, as well as cloud computing.

We provide companies with a global low-latency cloud infrastructure and a unified control panel for services built on its basis.

We also provide custom software development, IT infrastructure management, game testing, and colocation services.

You don't need your own infrastructure for web-based protection against DDoS attacks, bots, or hacking. Your business processes won't stop, and your users and customers won't even notice that your resource has been attacked.

Would you like to test our web application protection for free?
Just contact us.

352 208 80 507

sales@gcore.com

CORE