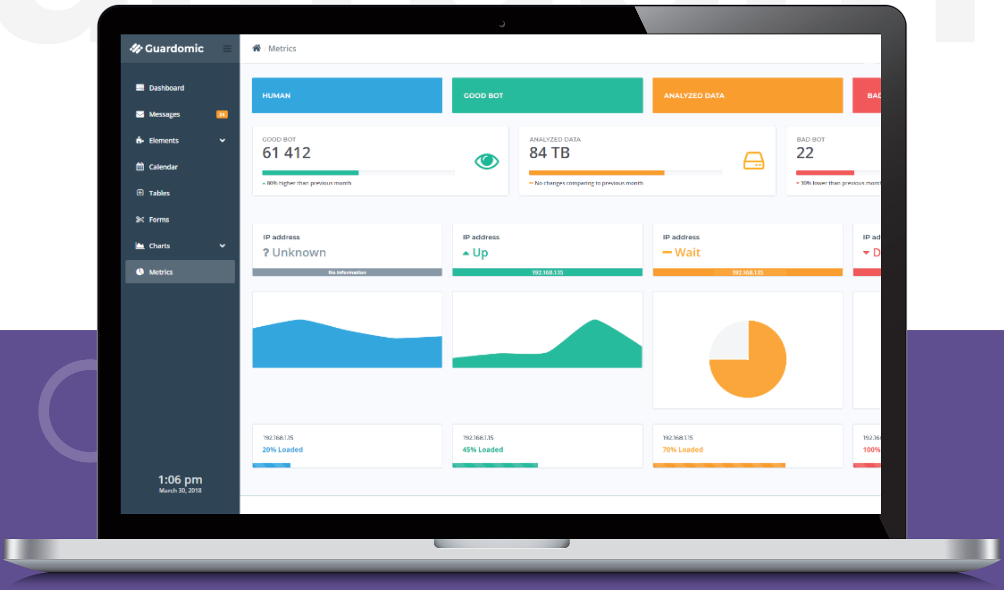
# Guardomic

Protection From Bot Attacks



GOOD BOT
61 412
80% higher than previous month

ANALYZED DATA
84 TB
No changes comparing to previous month

BAD BOT
22
10% lower than previous mont

IP address
? Unknown
No information

IP address
Up
192.168.1.15

IP address
Wait
192.168.1.15

IP ad
D

192.168.1.15
20% Loaded

192.168.1.15
45% Loaded

192.168.1.15
70% Loaded

192.16
100%

1:06 pm
March 30, 2018

see how it works

**www.guardomic.eu**

## Introducing the bot mitigation engine

Bot traffic, crooked display ads, and cryptocurrency web mining are the digital plague of the 21st Century. It is time to protect your online business and your users. Guardomic engine comes in as a powerful solution. Our system relies on in-depth statistics allowing you to secure your website traffic.

## Bots = Billion Dollar Losses

The scale of a problem is epidemic. The global network suffers from bot attacks huge. Only the online advertising business in 2016 alone, have experienced a bot-based waste at the estimated level of $7.2 BILLION!

To be more specific, only one botneck attack named Methbot was able to generate a loss in video advertising on a level of $3 to $5 million a day. To get a full picture of this disaster, let's take a look at the table below:

*Table 1 – Examples of wastes generated by bots*

| Bot Operation | Type | Focus | Estimated Losses Per Day |
|---|---|---|---|
| **Methbot** | Bot Farm | Programmatic video advertising | $3,000,000 |
| **ZeroAccess** | Malware | Ad fraud and bitcoin mining | $900,000 |
| **Chameleon** | Malware | Ad fraud | $200,000 |
| **Avalanche** | Malware | Identity theft, access control | $39,139 |
| **Ponmocup** | Malware | Theft | $27,778 |

## It has escalated – Problem overview

- Bots have infected the Internet and this problem is on the rise.
- Web attacks cause financial losses that damage the online business.
- All web-based services are an easy target for all kinds of attacks set up by bot networks. Online business has to face it and do what it takes to prevent those attacks.
- There is a gap in the market. Online business desperately needs a tool to detect bots on websites and threats they cause. A tool that will be a shield protecting them from bot attacks.

## Who needs a bot mitigation engine?

- E-commerce marketplaces, online shops, internet service providers.
- Banks and other financial institutions.
- Government agencies.
- Flight lines (aiming at protecting against web scraping).
- Every customer that cares about online security.

# What is Guardomic?

Guardomic is an answer to this problem. It's an innovative solution designed to protect online services from botnet attacks such as:

- Web Scraping
- Online Fraud
- Digital Ad Fraud
- Web Application Security
- SPAM

**Guardomic** consists of several key components that interface with each other:

**That's not all.** Armed with Guardomic, you are able to block unwanted traffic on your website. It means that you can decide to stop the traffic coming from a specific country, specific ISP, or IP range.

Typically, the system runs in a protected mode. It analyzes and blocks unwanted traffic according to your policy set. However, you can also narrow it down to only-monitor mode, which means it will only analyze the traffic, but without blocking. This mode will enable you to view detailed reports about what kind of traffic goes through your web service.

**There are two ways to implement Guardomic:** as a SaaS (Software as a Service) or as a set of virtual appliances installed on-premise. Regardless, whether it operates in the cloud or on-premise, the system behaves like a filter between global network and your online services.

The solution works apart from the hardware infrastructure. In real-time, Guardomic changes the allocation of the required resources and use them according to the actual need.

**Why this feature is so important?**
Because, when the botnet attack reaches your web service, the system rapidly increases efficiency to ensure undisturbed access to protected online service.

### Guardomic Web

– this is your main dashboard – a place where you log in to manage your domains, change your settings and watch the statistics.

### Guardomic API

– to correctly determine whether a certain request should be filtered or not, the Gateway asks our API and receives the answer within tens of milliseconds. The API makes the decision based on multiple factors.

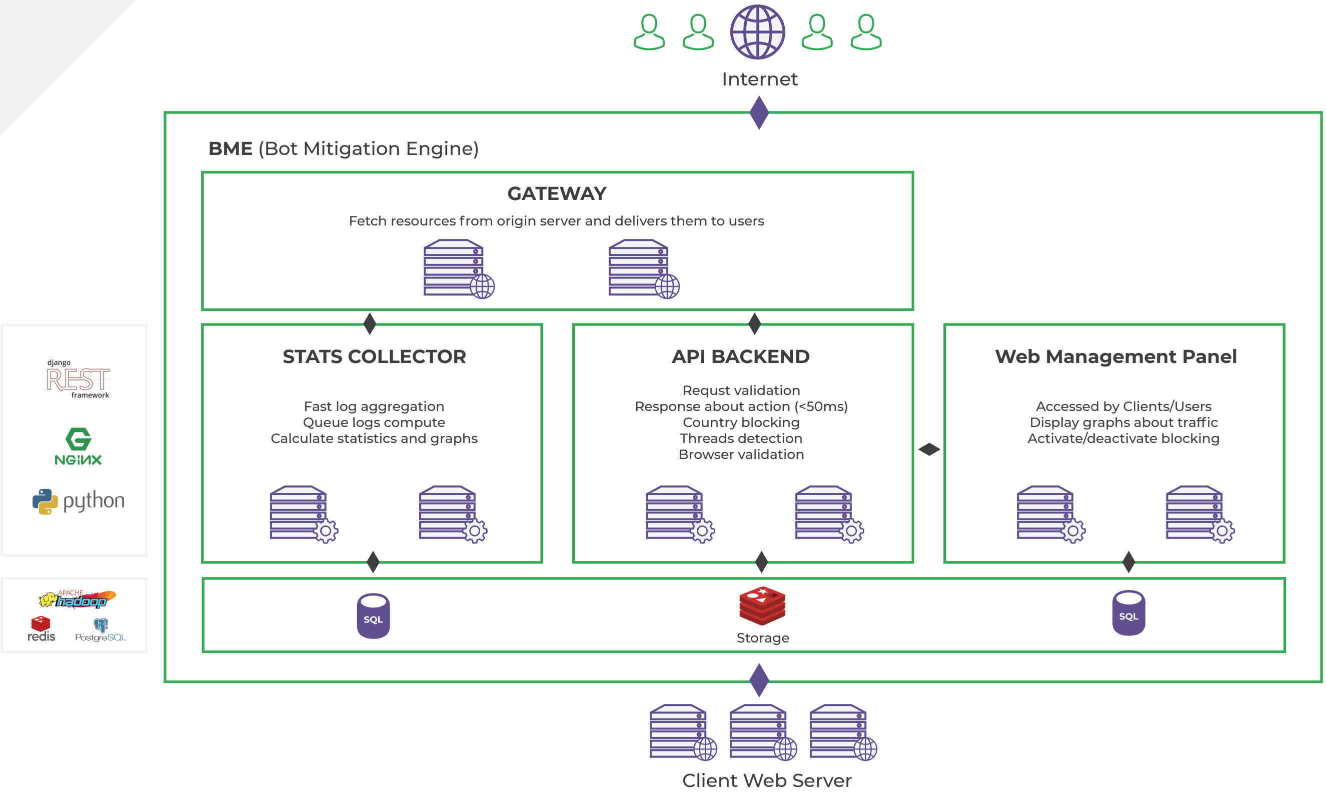
### Guardomic statistics

– the goal of our system is to deliver you near real-time statistics. To be able to achieve it, we created an autonomic system that will calculate per-domain statistics based on every request going through our Gateway.

### Guardomic Gateway

– that's a relief for your servers. After registering your domain in Guardomic, all requests to that domain will flow through our gateway. This means that the system won't put any strain to your servers, but it will also go unnoticed to your website's users. To recognize more sophisticated bots, we can use the Gateway to add some content such as a JavaScript code or a hidden link to your website's body.

## Check our infographic to get the best picture of our solution:



Internet

**BME** (Bot Mitigation Engine)

GATEWAY
Fetch resources from origin server and delivers them to users

STATS COLLECTOR
Fast log aggregation
Queue logs compute
Calculate statistics and graphs

API BACKEND
Requst validation
Response about action (<50ms)
Country blocking
Threads detection
Browser validation

Web Management Panel
Accessed by Clients/Users
Display graphs about traffic
Activate/deactivate blocking

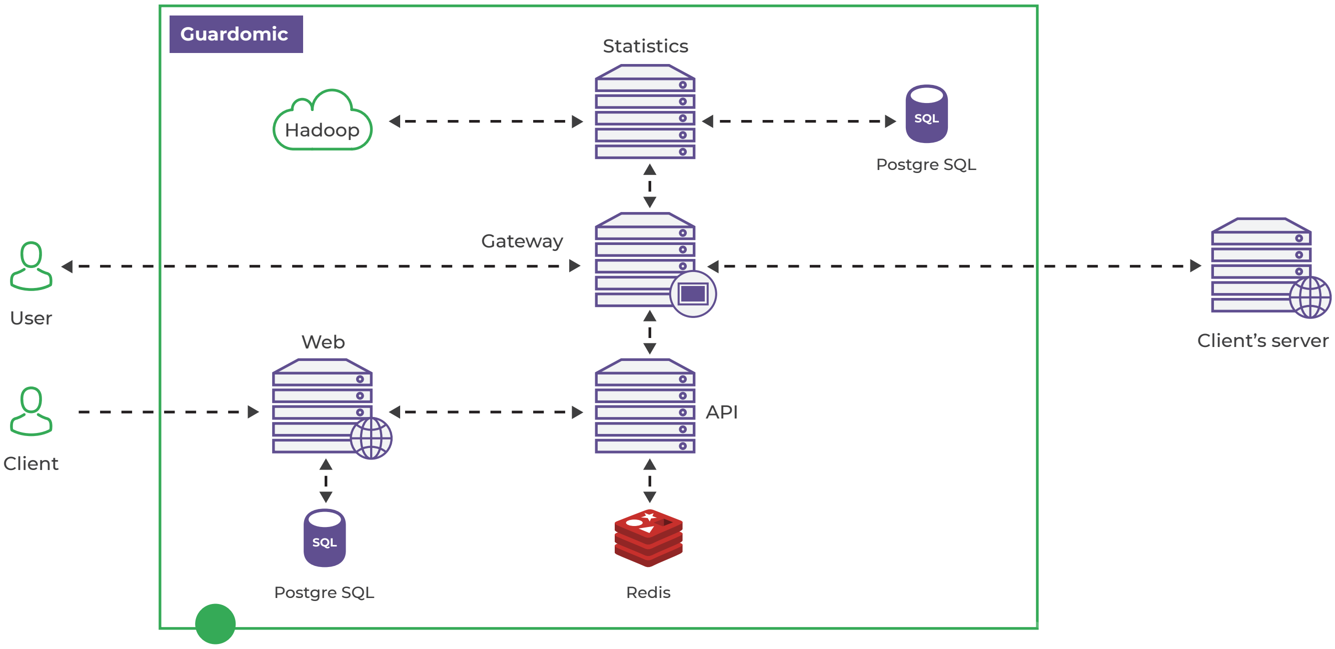
Storage

Client Web Server

*Fig.2 - The general overview of the solution*

Botnet attacks are viciously premeditated and planned. They can hit a whole infrastructure that consists of multiple data centers scattered all over the globe. To be on the safe side, the Guardomic service should be implemented within the entire organization, in each data center at the same time.

For better performance and efficiency the system can make the most of Artificial Intelligence and Neural Networks – this will ensure a high detection of unusual bot attacks.



## Contact

Koma Nord Sp. z o.o.
Łużycka 2 Str.
Gdynia 81-537, Poland

☎ +48 58 621 11 00

✉ guardomic@komanord.pl