

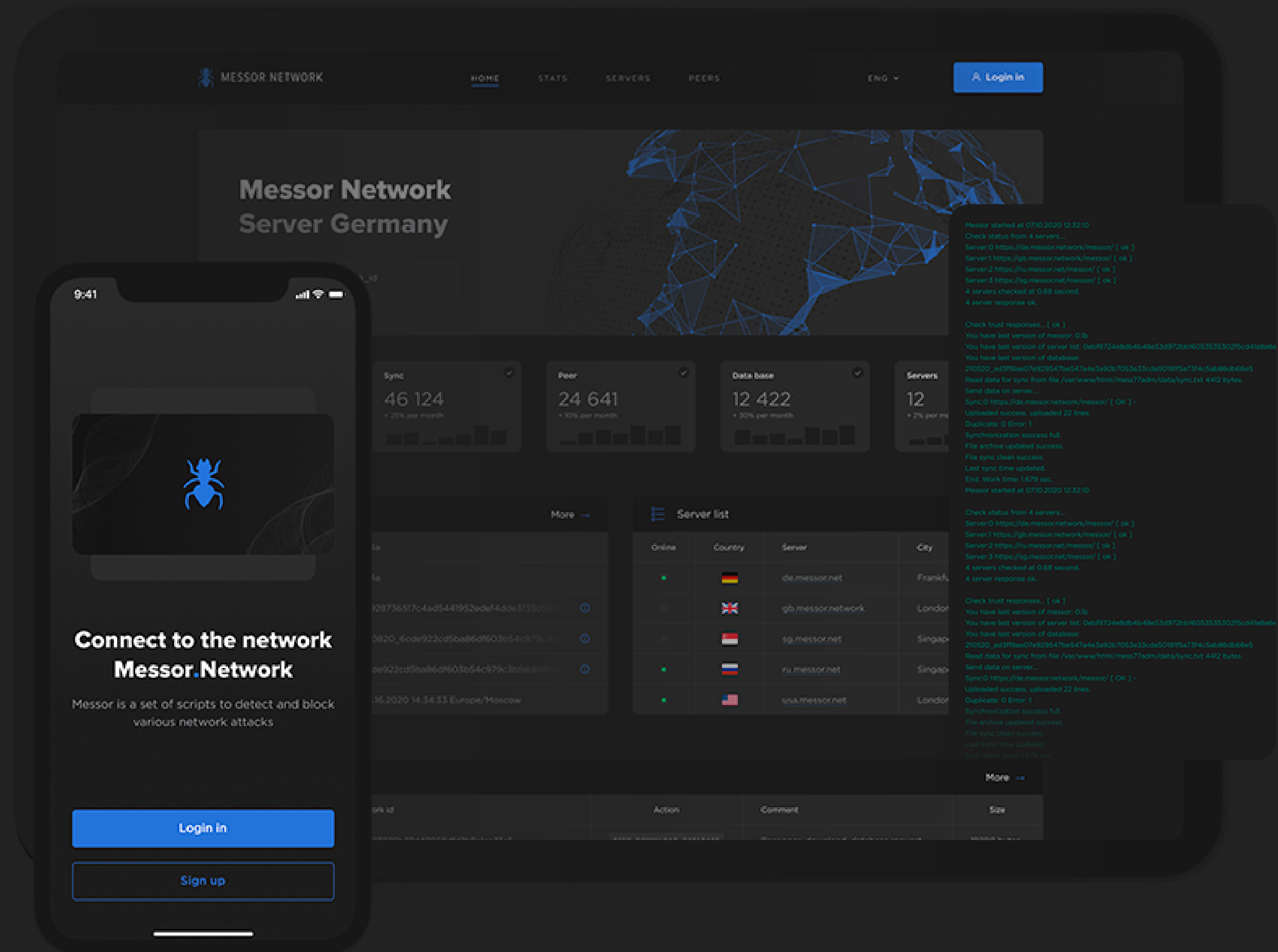
Created by Messor Limited

# Messor Network

an application for blocking  
network attacks and scanning

## Who can Messor help?

- ✔ If you keep a blog or a website on the Internet
- ✔ If you have a company that conducts online activities
- ✔ If you have a network of sites and servers



# Product



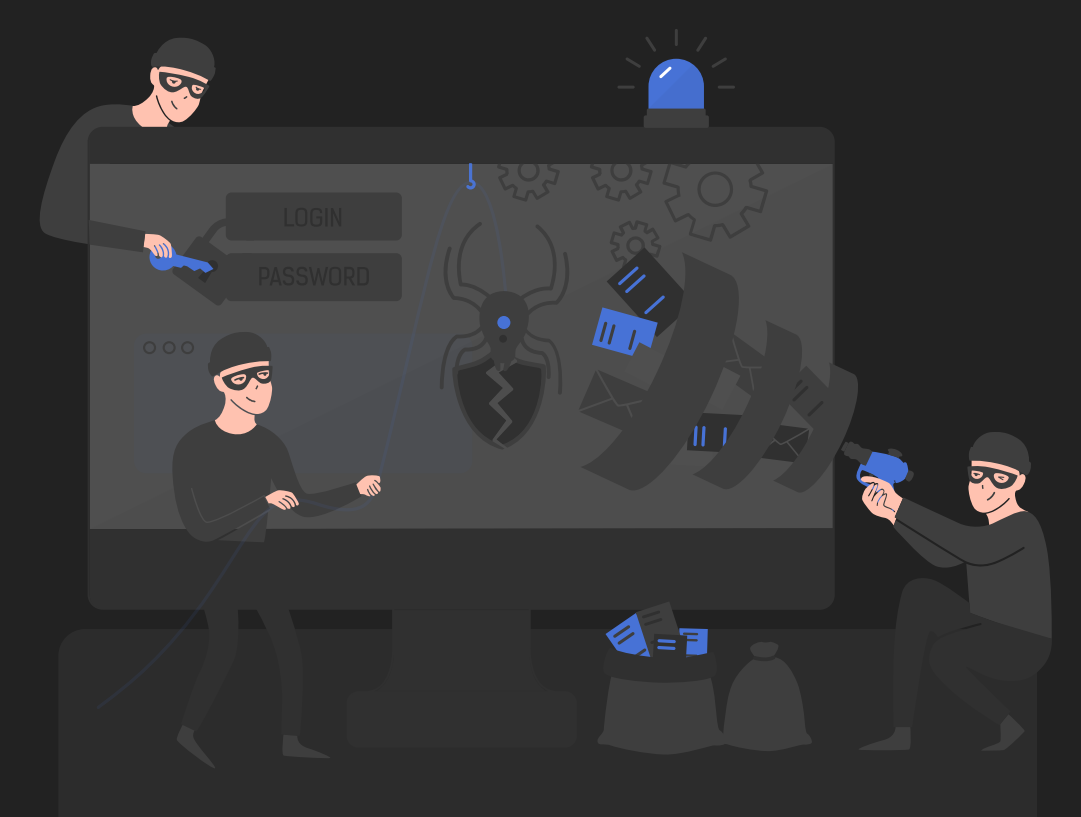
The Messor open-source app provided free of charge is designed to protect your data and online business



Messor is capable of preventing various network attacks. In addition, it contains several traps.



The flexible configuration gives you a great opportunity to add your own addresses and security filter settings



A daily updated blacklist based on scanning and attacks of all network members will prevent attacks and protect your business

# Messor Will Help You:

1

Monitor the security of sites and servers

2

Protect your personal data on the Internet

3

Reduce network security costs

4

Protect your business from network attacks and scanning

5

Block those who try to bypass your security filters



# Blocking WAF/IPS Attacks



A system for detecting and preventing attacks and prohibited activities. It includes sensors and traps designed for attempted attacks.



Messor is capable of analyzing your traffic and detecting anomalies using the signature database. Analysis of data from GET, POST, and COOKIE USER\_AGENT.



In addition to traffic analysis, Messor has a set of trap signatures that hackers and automated scanners quickly fall for, thanks to which Messor detects attempted attacks in real-time and blocks them. You can set a blocking level of the attackers and take the necessary actions yourself.



All recorded for attempted attacks will be sent to Messor.Network servers for analyzing the neural network. After that, all the participants of the Messor.Network will block the attackers' addresses.

## Main settings

### Ip firewall ⓘ

Block ip from messor database and black lists. [Lock settings](#)

Add IP attackers to a temporary blacklist after  attempts

### User Agent firewall ⓘ

Block users by useragent block string from messor database.

Block attacks through user agent

Block search engines bots (google/msn/yandex/...)

Block tools (wget/curl/python/...)

Block ALL (tools/bots/search engines)

### Traffic analyzer ⓘ

Block users by GET/POST block string from messor database.

GET- Analyze GET data and block dangerous requests

POST - Analyze submitted form data and block dangerous requests

COOKIE - Analyze cookie and block dangerous requests

### Bot | DDoS Protection ⓘ

DDoS mitigation is a set of tools for resisting or mitigating the impact of distributed denial-of-service attacks on networks attached to the Internet.

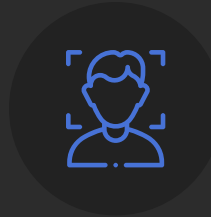
[Reset all settings](#)

[Save](#)

# Protection from DDoS attacks



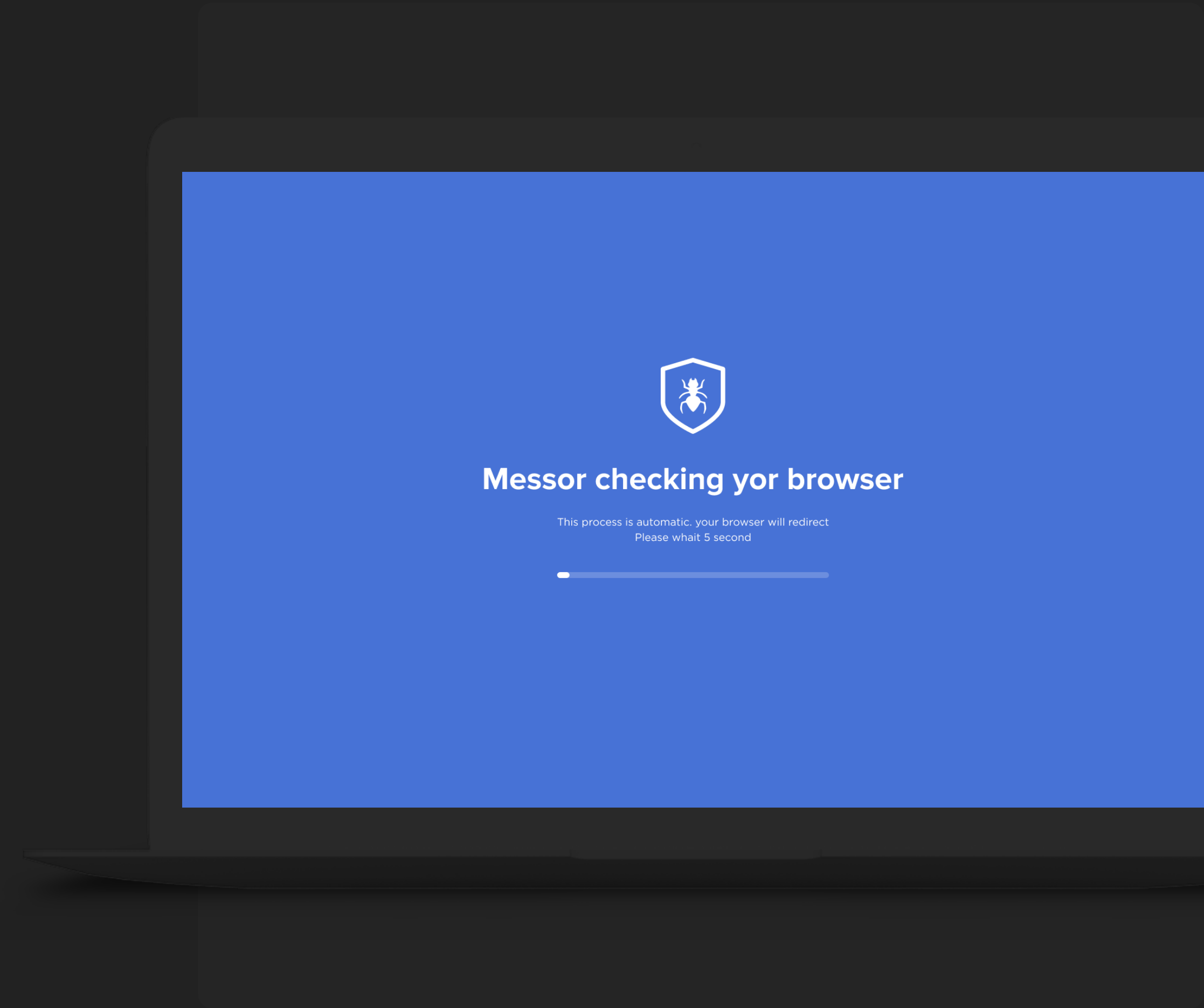
The DDoS Protection feature helps you detect and block automatic scanners and DDoS bots. Blocking SPAM bots will reduce the amount of malicious traffic to your site/server thereby reducing the load and costs.



When the DDoS Protection feature is enabled, all users will be scanned for automatic actions. If a user is recognized as a bot, the system will block him/her.



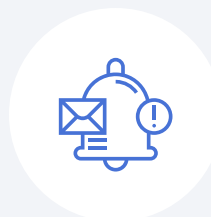
Our unique algorithm does not require a user to perform such actions as entering the text from a picture, etc. – everything happens completely automatically.



# Virus Scanner



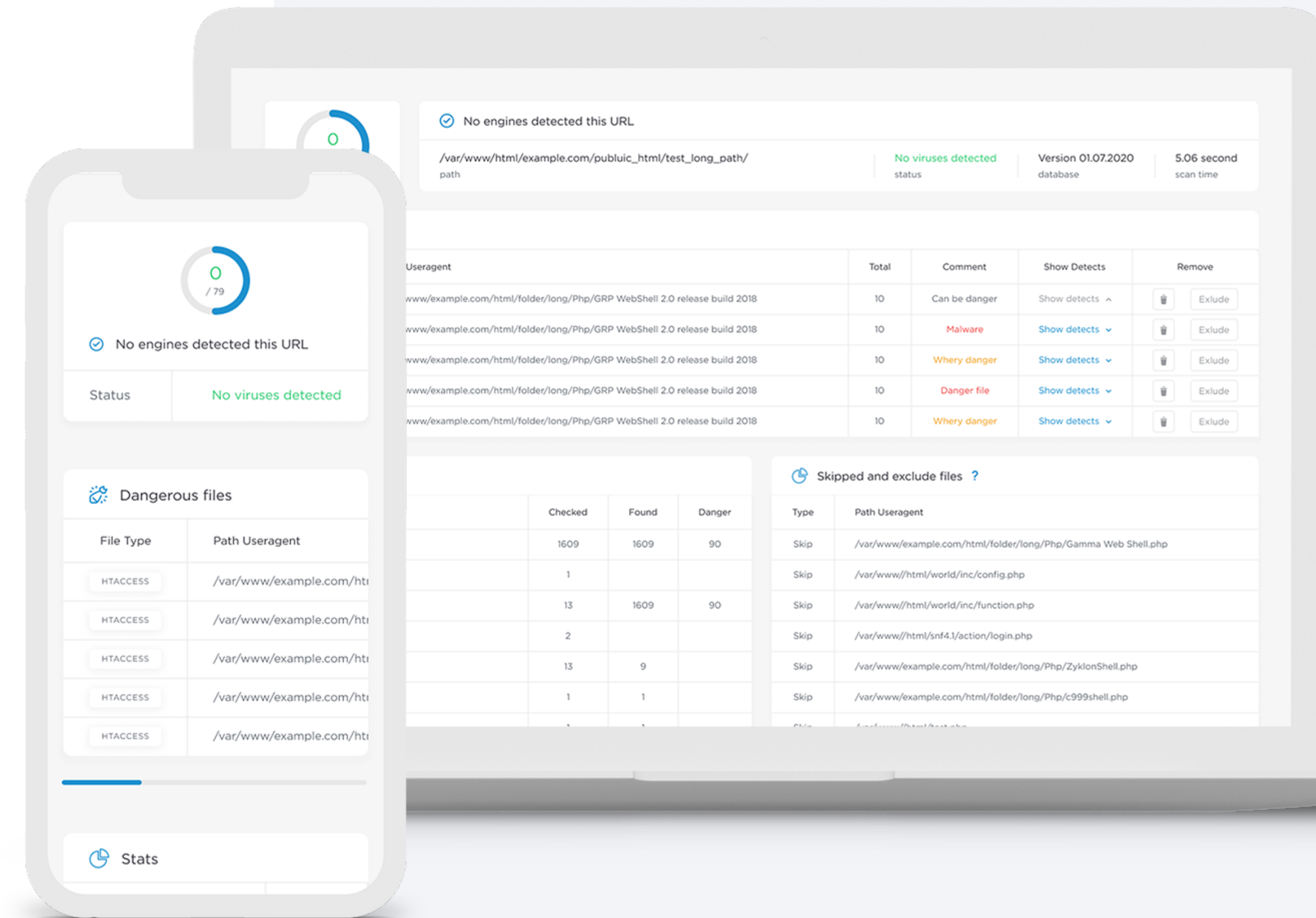
The Virus Scanner feature helps you find and remove malicious code and files on your server/website. It is possible to set up daily automatic scanning of your server or website to search for infected files and automatic removal of malicious code.



Sending reports to Messor.Network servers and instant notifications by email/SMS/phone are also possible if viruses are detected.







Our scanner is fundamentally different from conventional antiviruses. We do not search against signature databases – our algorithm detects dangerous functions in files. In such a way, we can find malicious code without examining and entering it into the database. This approach allows us to find any malicious code with high accuracy.



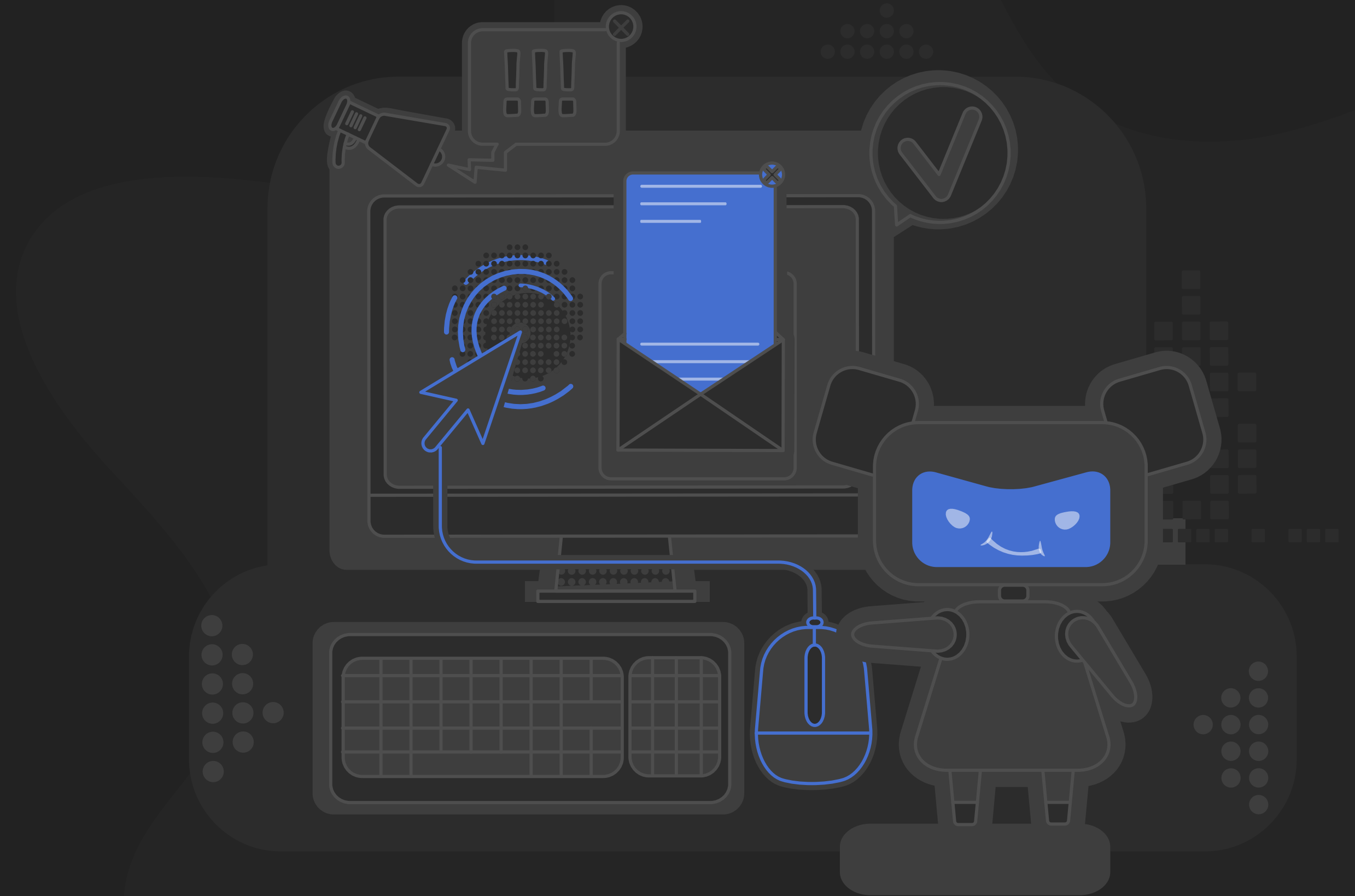
# Blocking Bots

The Blocking Bot feature helps you block different types of bots. You can choose the level of blocking from dangerous network bots to search robots, or you can make the site inaccessible to all types of bots.

## Types of blocking

-  Blocking attacks through UserAgent and blocking utilities for vulnerability scanning.
-  Blocking utilities for downloading bot websites for automatic activities on your website.
-  Blocking all kinds of bots and search engines (human-only access)
-  Blocking search engines

*Blocking is carried out by analyzing the UserAgent string, IP address, and JavaScript - checking the user's browser.*



# Block by IP Allow/Blocklist



The IP blocking feature includes the ability to block specific IP addresses, address lists, or specific countries



And most importantly, the Blocklist is collected based on data from all participants of the Messor.Network. You receive a daily updated database of malicious IPs.



You can also add exclusion addresses to the Allow list, and these addresses will never be blocked.





# Backup



The feature of backing up your files and database can guarantee the safety of your data in case of server failure, data loss, encryption of your data, and hacking.



You can save your backups on your server or send them to you by e-mail, or use secure storage in our repositories on our servers.



# File System Control

By using the File System Control feature, no change in files on your server or website goes unnoticed.



You are provided with full control of changes to your files

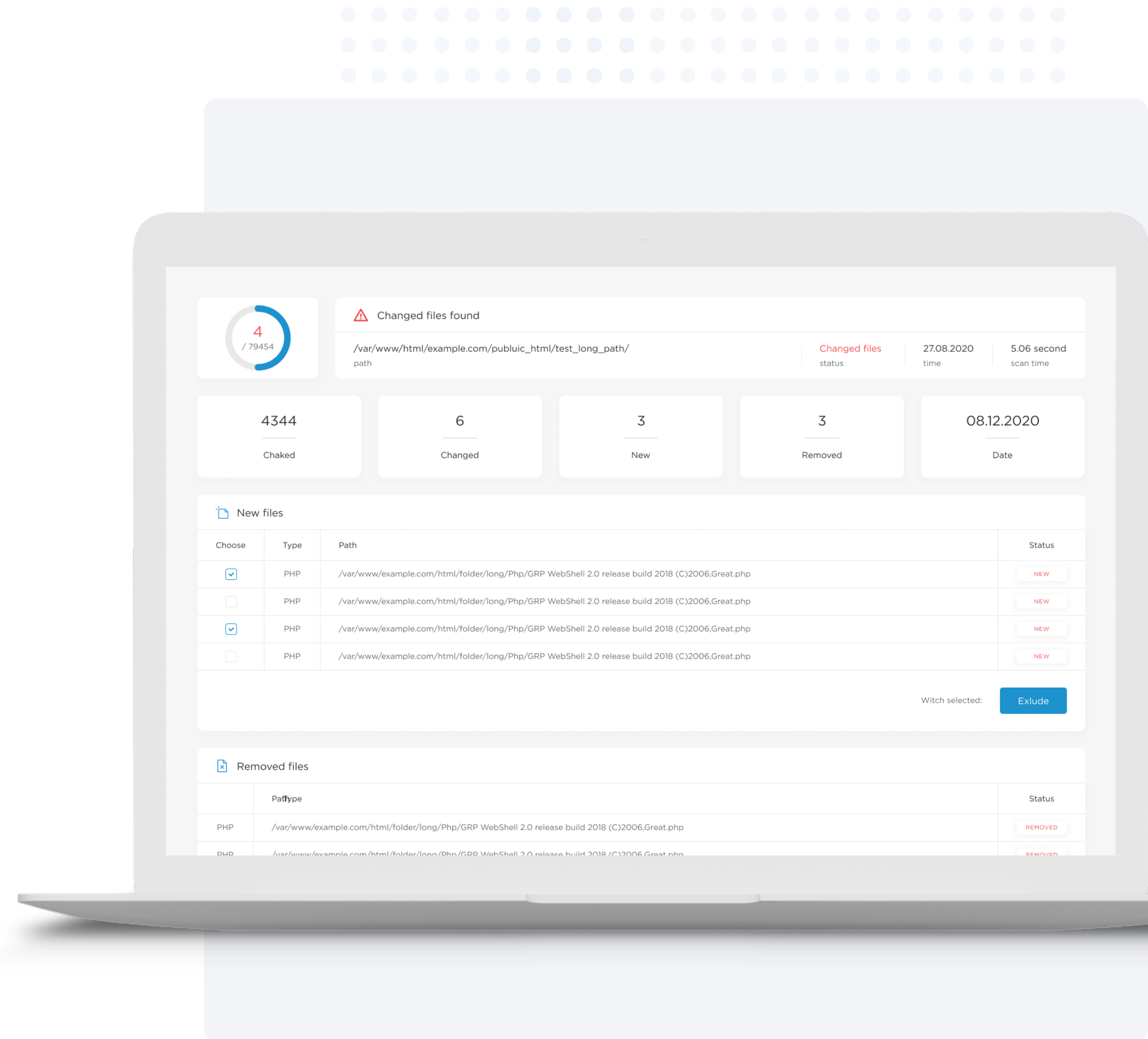


You can configure notifications about changes of critical files



This will help protect the integrity of your system. In case of hacking or other attacks on files, you will be quickly and easily aware of it

*How it works: The system takes a snapshot of the file system, then repeats this operation and compares it with the previous snapshot. If there is a difference in the hash sum of files (a change has occurred), the system sees this and records it in the report.*



# Notifications/Monitoring



The Notification and Monitoring features will help you to always be aware of the situation with your website/server.



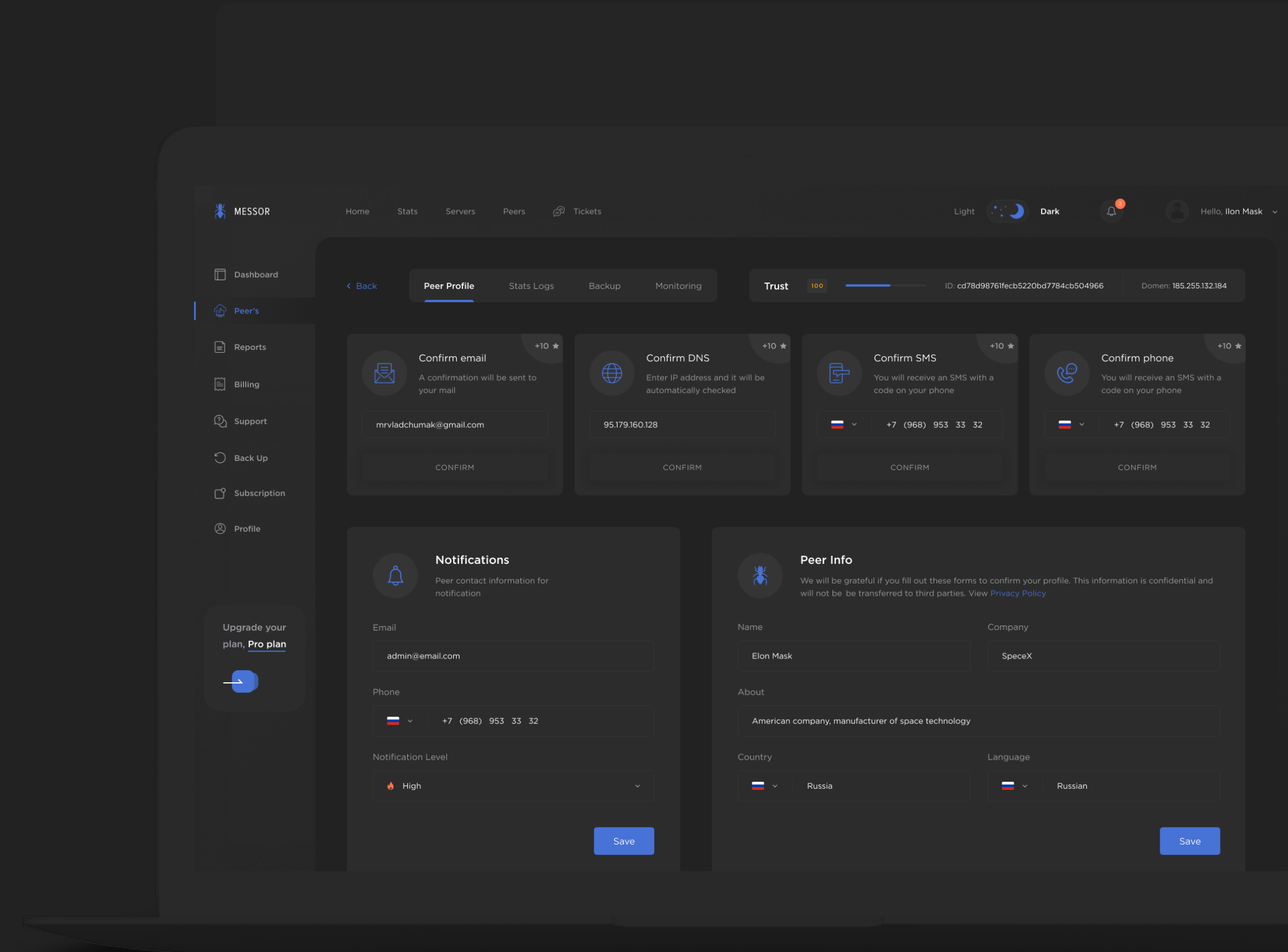
The settings of the notification system will help you be quickly aware of security incidents. It is possible to check your website/server daily for malicious code and the presence of your domain in virus lists.



Daily or even hourly check of your website/server for availability and response speed.



Notifications can be sent either by email or by SMS or even by phone through your personal SecurityOfficer.

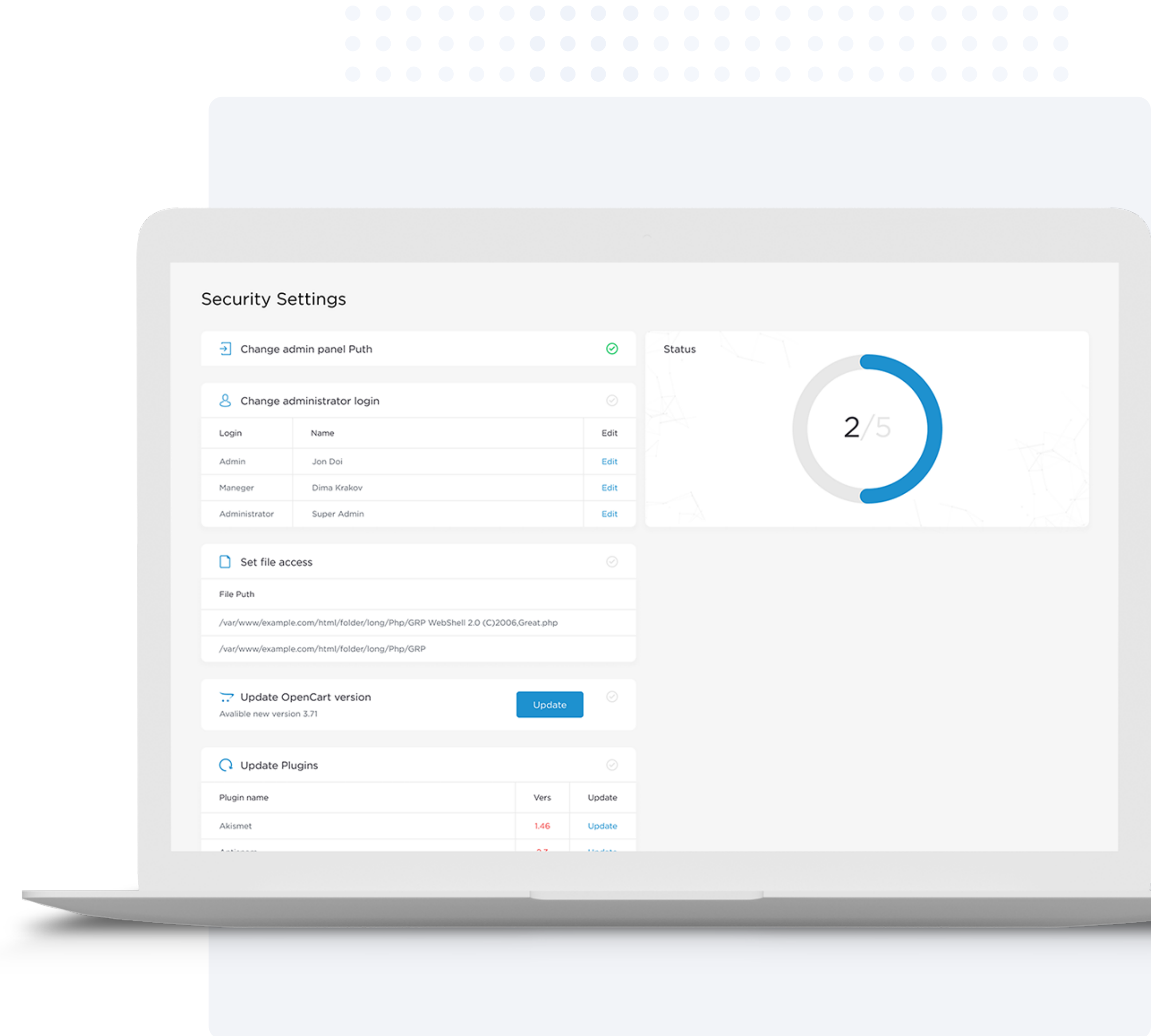


# Security Settings

The Security Settings feature will help even an inexperienced user to safely configure his/her management system and server.

## Messor will check your CMS security settings

It will identify vulnerabilities, and will also give you detailed instructions and recommendations for the correct setup. This function will help you perform such actions as hiding the admin panel, checking the security of your accounts, checking for your software updates, and much more. The specific list of features depends on the specific CMS.



# Contacts

Messor Limited

An International Business Company registered Seychelles under No. 222758

Dated 18th of August 2020

Registered Office : House Of Francis, Room 303, Ile Du Port, Mahe, Seychelles



To become a member of the Messor network, please write to us at [support@messor.network](mailto:support@messor.network) or [manager@wwood.dev](mailto:manager@wwood.dev)

## Follow the project news

 [blog.messor.network](https://blog.messor.network)

 [twitter.com/MessorNetwork](https://twitter.com/MessorNetwork)

 [www.facebook.com](https://www.facebook.com)

 [github.com/messor-network](https://github.com/messor-network)

