QRATOR LABS

QRATOR.WAF

Solution's guide

qrator.net

Qrator Web Application Firewall

Effectively secure critical web resources against external attacks and gain complete control over application usage in the allowed scenarios with the cloud Qrator Web Application Firewall.

Qrator.WAF is an advanced next-generation tool that helps to prevent a wide range of threats to web applications during their operation.

A high level of protection against both simple and complex targeted attacks is achieved by using the most detailed models of the protected application along with signature-based and behavioral anomaly detection methods.

The distributed infrastructure of WAF filtering nodes within the perimeter of the Qrator Labs network allows you to protect even the most heavily loaded applications with minimal delay and guaranteed service availability.

Why web applications have to be protected

1

For many organizations, web applications are an important part of their business processes and they provide key competitive advantages

2

They are a weak link in the perimeter of the organisation and the main target of attackers

3

Web applications are subject to various threats, such as theft of confidential data, fraud, attacks on the web users

Advantages of Qrator.WAF

○ Provided as a distributed cloud solution

○ Fast connection

○ Charging only for the actually used bandwidth to ensure the optimal cost of ownership

○ A greater set of usage scenarios compared to similar solutions

○ Flexible configuration taking into account features of protected applications

○ Operation in the lock mode with minimal false positives

○ A wide range of professional services from the solution developer.

Unique functional features

1 High level of protection

A high level of protection against both simple and complex targeted attacks is achieved by using the most detailed models of the protected application along with signature-based and semantic anomaly detection methods.

2 Effective prevention of false positives

A mechanism of early suppression of false positives minimizes their influence on decision-making. It makes it possible for a WAF operator to focus on significant events.

3 Unique functions of business logic analysis

Defining users, their actions in the application, action parameters, and data, as well as sequences (chains) of logical actions. This information can be used to suppress false positives and create a positive application model, or it can be exported to other systems for further analysis.

4 Specific machine learning algorithms

They optimize WAF performance, detect false positives, automatically build application models, and effectively use the solution in the active development cycle (SDLC).

Main use cases

○ Protection against major classes of web threats, including OWASP Top 10

○ Protection against brute force attacks

○ Protection against attacks on identification and authorization mechanisms

○ API security

○ Corporate service security

Security mechanisms

Basic security mechanisms

○ HTTP protocol validation (request types, headers, and their parameters, etc.)

○ Automatic filtering of static resources: a separate mode for processing static resources (provides ease of data analysis in the control and monitoring subsystem)

○ Analysis of requests and responses using signature analysis (including those that detect OWASP Top 10 attacks)

○ The mechanism of "black" and "white" lists for basic types of sources (IP address, URLs)

○ Blocking sources when multiple anomalies are detected in the requests

Enhanced security capabilities

○ Limiting the rate of requests from one source (Rate Limiting) for the application as a whole.

○ Automatic detection of the performed logical actions and checking its parameters for compliance with the predetermined patterns

○ Controlling sequences of logical actions

○ Success measurement of the performed actions based on the analysis of responses, including nested data

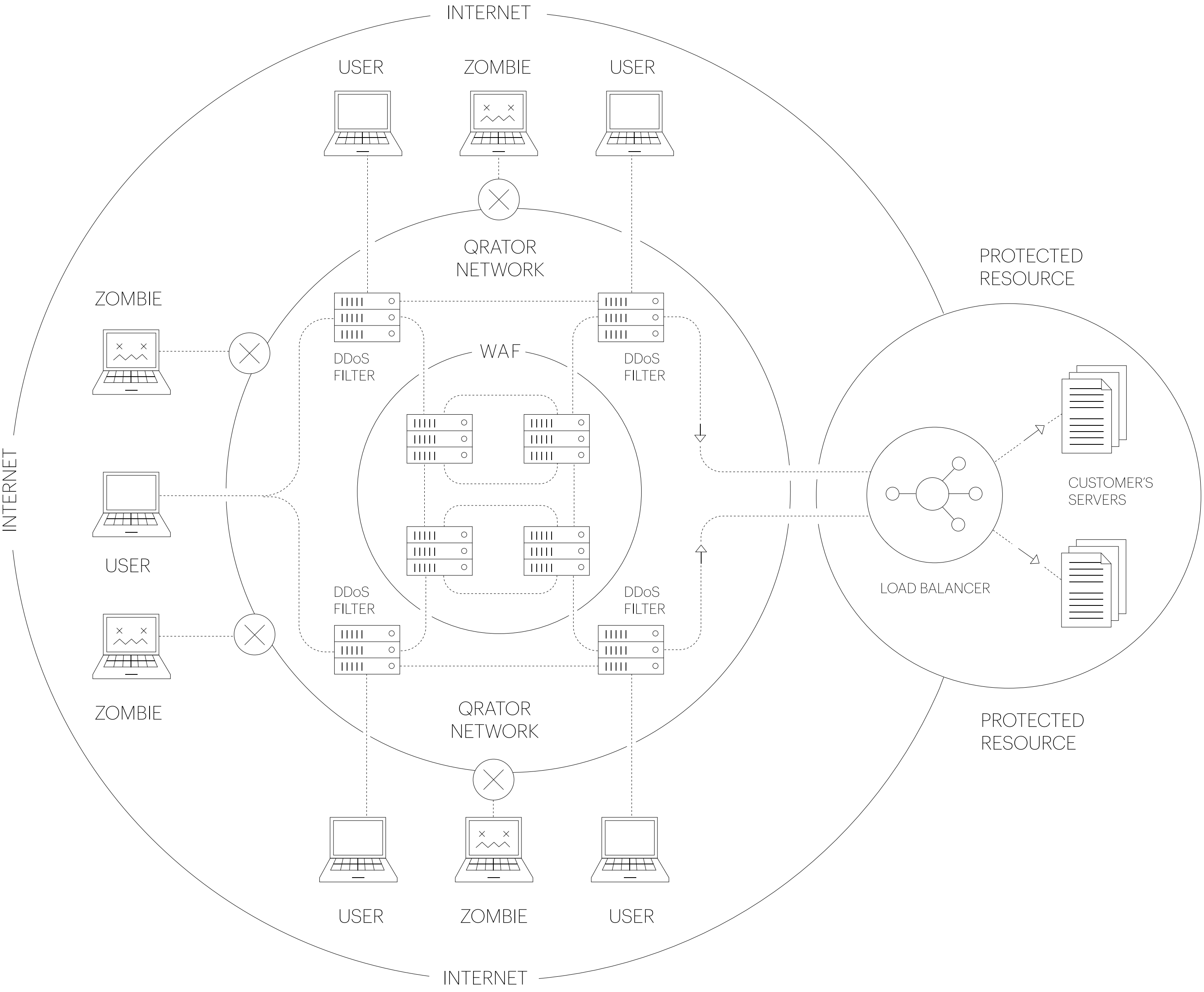
○ Defining sources that are arbitrary parameters of logical actions that characterize the request source (IP address, session ID, user name, certain cookie, etc.)

○ Controlling users and sessions, which define the key session parameters and the logical actions that are used as a framework to set, monitor, and disable these parameters)

○ Controlling user authorization at the level of sessions and performed logical actions

○ Controlling the rate of requests to individual logical actions depending on the parameters of the request source and other parameters (Rate Limiting).

How Qrator.WAF works



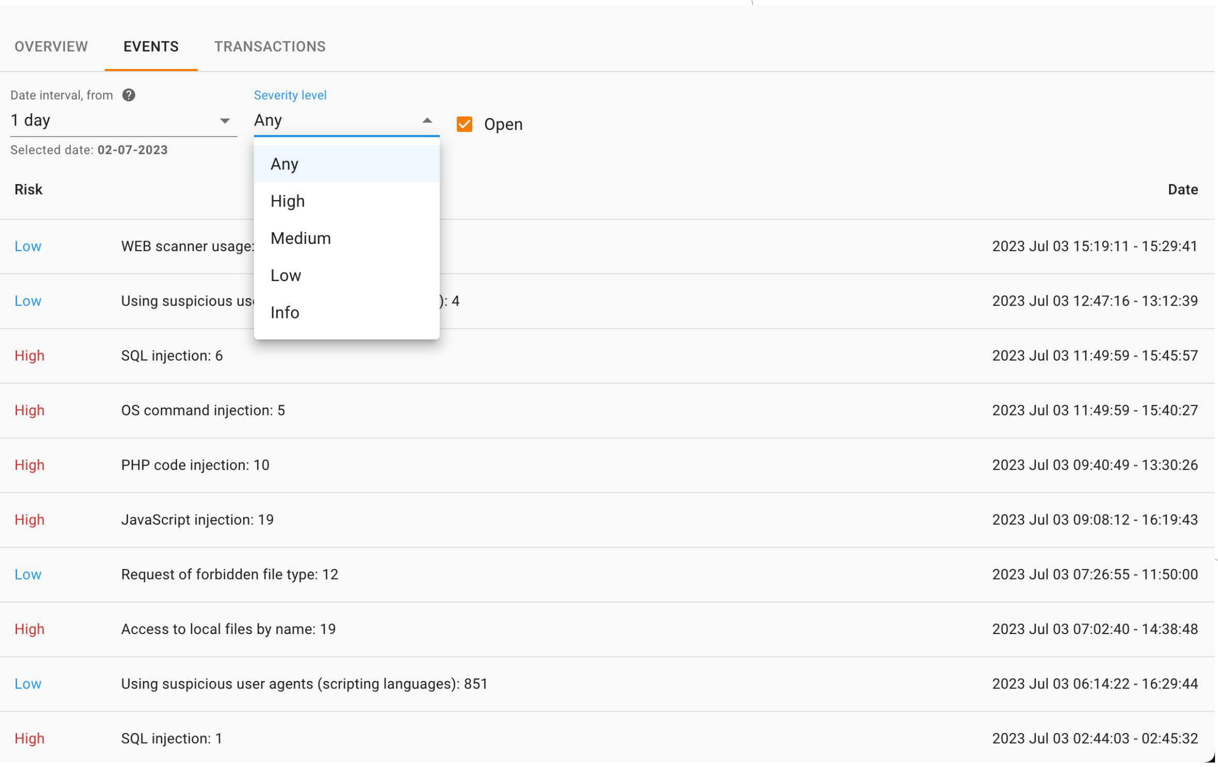
Monitoring interface

Customers are not required to have special expertise to make changes to the architecture of the protected application and configure cloud **WAF** rules.

We provide access to a ready-made solution based on the customer's wishes and provide round-the-clock monitoring of incidents in your personal account.

There is a separate WAF section in the customer account, where the following features are available:

EVENTS is a flexible tool for analyzing detected security events, grouped by type and threat level, with an option to view all the details of each individual transaction. It is also possible to manually suppress a false positive when a false positive lock is detected in the transactions.



Date interval, from: 1 day

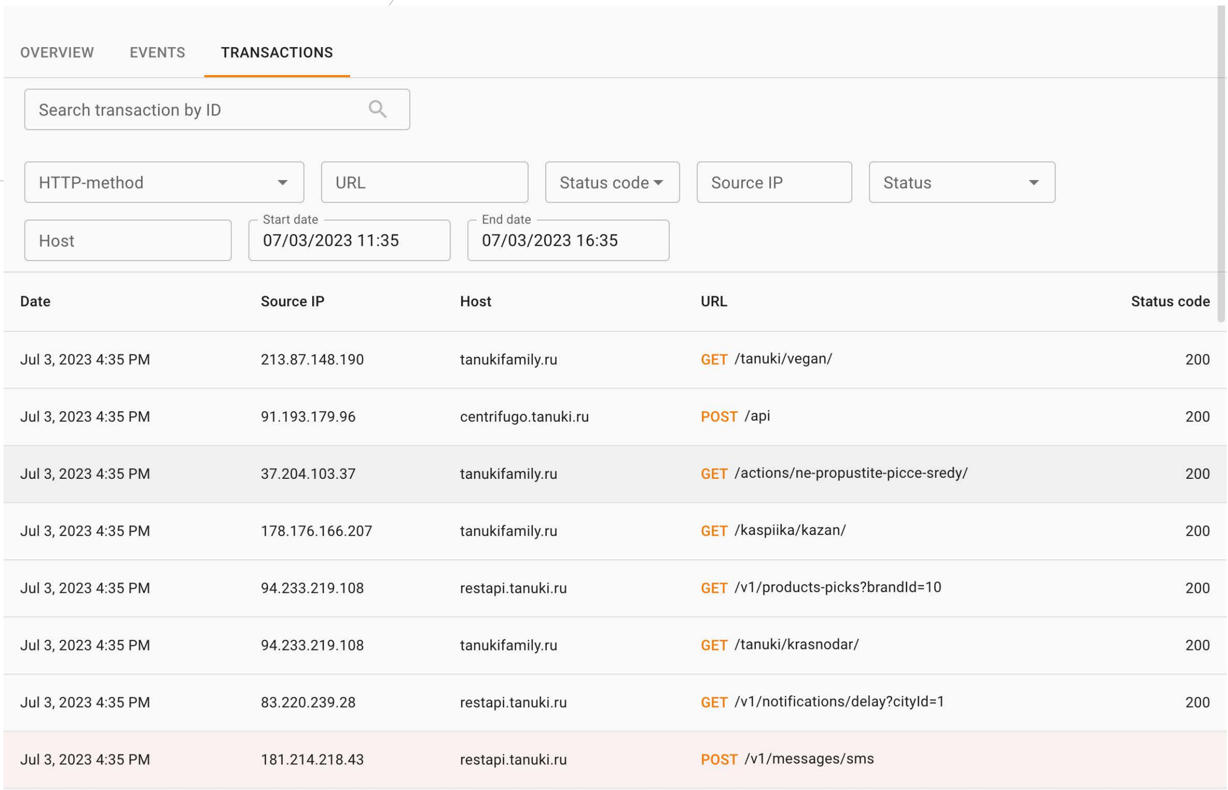
Selected date: **02-07-2023**

Severity level: Any

☑ Open

Risk		Date
Low	WEB scanner usage:	2023 Jul 03 15:19:11 - 15:29:41
Low	Using suspicious us): 4	2023 Jul 03 12:47:16 - 13:12:39
High	SQL injection: 6	2023 Jul 03 11:49:59 - 15:45:57
High	OS command injection: 5	2023 Jul 03 11:49:59 - 15:40:27
High	PHP code injection: 10	2023 Jul 03 09:40:49 - 13:30:26
High	JavaScript injection: 19	2023 Jul 03 09:08:12 - 16:19:43
Low	Request of forbidden file type: 12	2023 Jul 03 07:26:55 - 11:50:00
High	Access to local files by name: 19	2023 Jul 03 07:02:40 - 14:38:48
Low	Using suspicious user agents (scripting languages): 851	2023 Jul 03 06:14:22 - 16:29:44
High	SQL injection: 1	2023 Jul 03 02:44:03 - 02:45:32

TRANSACTIONS is a section where all transactions of the protected application are stored, offering the possibility to flexibly search for requests using various parameters.



OVERVIEW EVENTS **TRANSACTIONS**

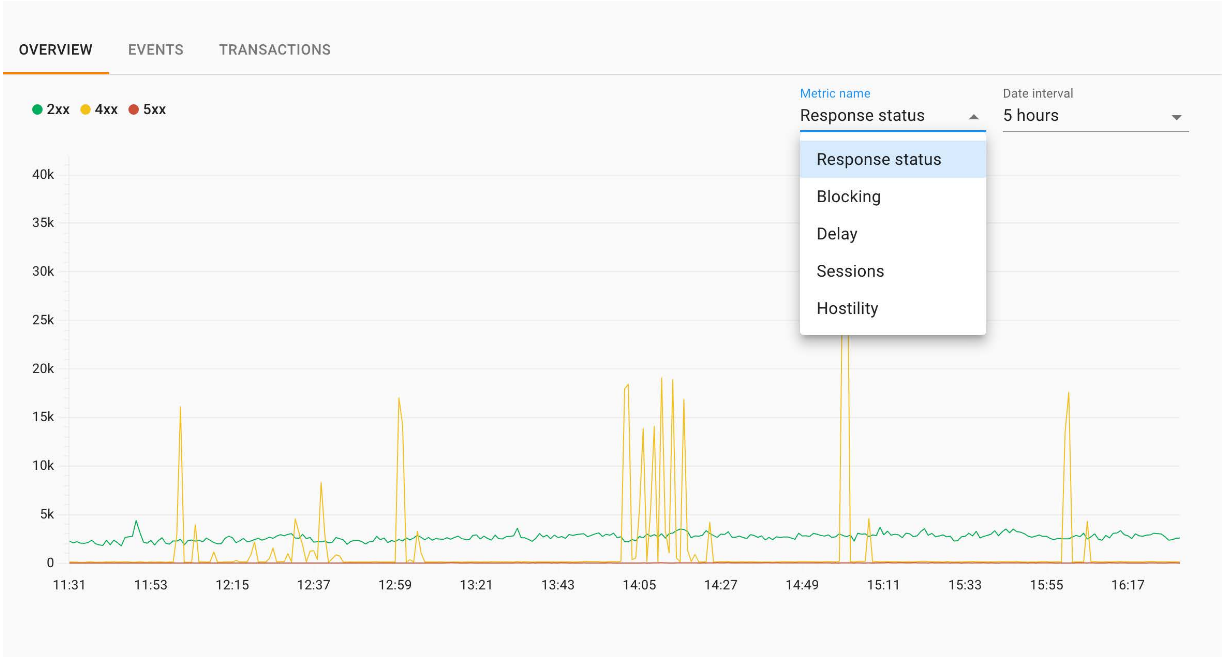
Search transaction by ID

HTTP-method | URL | Status code | Source IP | Status

Host | Start date 07/03/2023 11:35 | End date 07/03/2023 16:35

Date	Source IP	Host	URL	Status code
Jul 3, 2023 4:35 PM	213.87.148.190	tanukifamily.ru	GET /tanuki/vegan/	200
Jul 3, 2023 4:35 PM	91.193.179.96	centrifugo.tanuki.ru	POST /api	200
Jul 3, 2023 4:35 PM	37.204.103.37	tanukifamily.ru	GET /actions/ne-propustite-picce-sredy/	200
Jul 3, 2023 4:35 PM	178.176.166.207	tanukifamily.ru	GET /kaspiika/kazan/	200
Jul 3, 2023 4:35 PM	94.233.219.108	restapi.tanuki.ru	GET /v1/products-picks?brandId=10	200
Jul 3, 2023 4:35 PM	94.233.219.108	tanukifamily.ru	GET /tanuki/krasnodar/	200
Jul 3, 2023 4:35 PM	83.220.239.28	restapi.tanuki.ru	GET /v1/notifications/delay?cityId=1	200
Jul 3, 2023 4:35 PM	181.214.218.43	restapi.tanuki.ru	POST /v1/messages/sms	

OVERVIEW is a dashboard with different metrics of the traffic of the protected web applications (response code, locks, delay, sessions, hostility).



Metric name: Response status

Date interval: 5 hours

QRATOR LABS

qrator.net

sales@qrator.net

+420 602 558 144