QRATOR LABS

QRATOR.ANTIBOT

Solution's Guide

qrator.net

Qrator.AntiBot

Intelligent protection against automated bot attacks for web, mobile applications and APIs without affecting the UX.

23%

Bot traffic on a website

9,2%

The average business loss of website scraping

4 196 806 693

Monthly blocked bot requests

SECURING YOUR BUSINESS RESOURCES

Malicious bots drive your business to loss by brute-force hacking, identity theft, creating useless traffic and competitive parsing on websites.

Click fraud, content scraping, SEO manipulation, and other bot attacks can dramatically impact business revenue not talking about excessive abuse of application resources that power fraudulent activity, such as account takeover or application DDoS.

Stopping malicious bots helps maintain brand reputation and customers' trust especially when it comes to credentials security.

Protects Against

- Account Takeover
- Parsing
- Credential stuffing
- Server overloading

Why Qrator.AntiBot

Qrator.AntiBot distinguishes good and bad bot traffic without posing inconvenience for legitimate users and bringing comprehensive protection against automated content search, data scraping, brute-force attacks, and DDoS attacks.

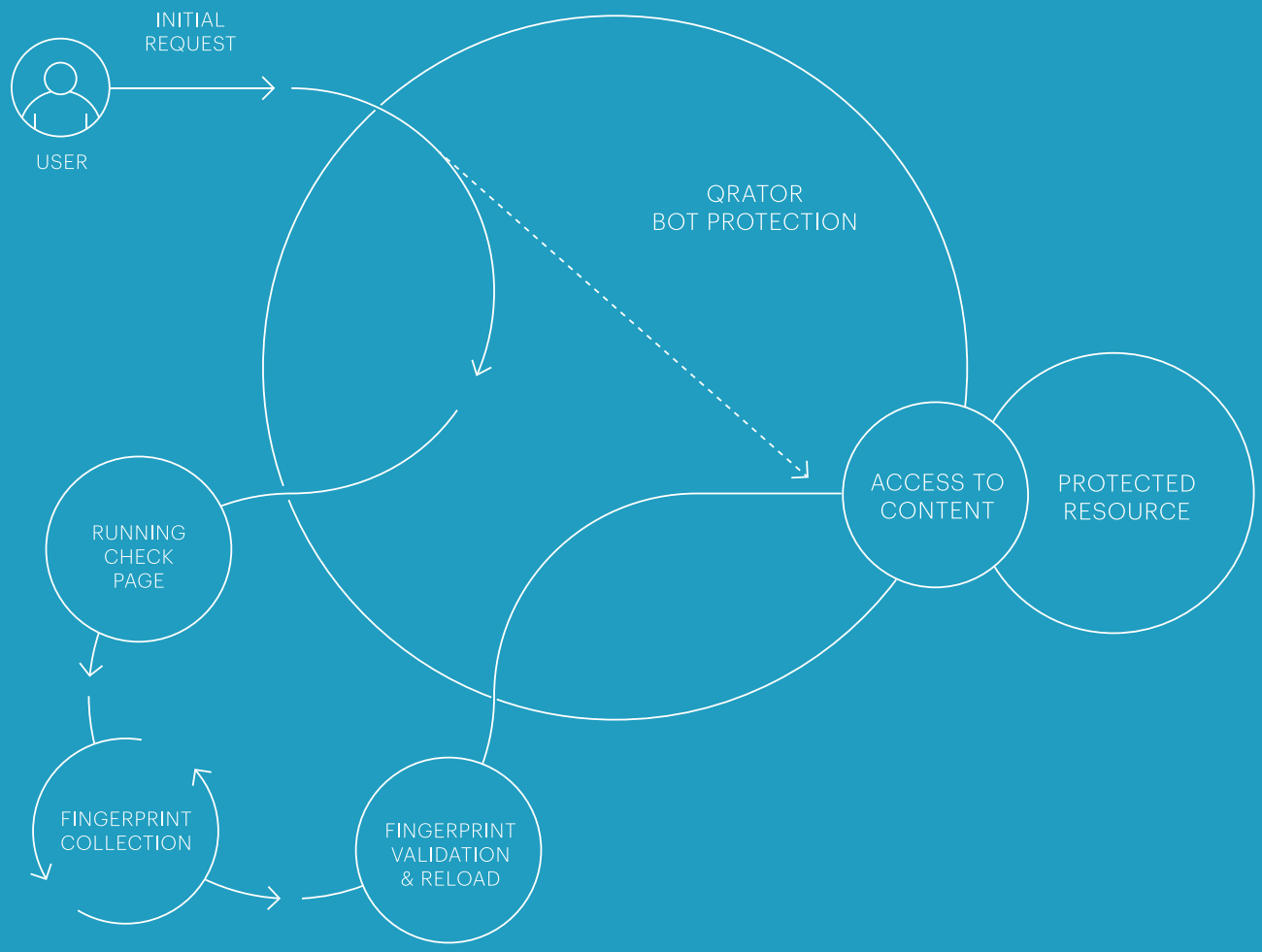
- built-in element of the Qrator Labs DDoS Mitigation Solution
- takes minutes to deploy and enables flexible configuration of user-defined rules
- protects websites, mobile apps and APIs
- No CAPTCHA

World Renowned Bot Detection Technologies

- DOM Inspection
- Javascript Fingerprinting
- Behavioral Analysis
- Search for Tampering
- Scoring against Valid Users
- Measuring Likeness to Known Bots

How Qrator.AntiBot works

Qrator.AntiBot is included in the delivery set of the Qrator Labs DDoS Mitigation platform and can be turned on and set in a special section of the Qrator UI.



Web-based locations

For the locations where web-based users are expected by the protected location, Qrator.AntiBot checks the environment of a browser addressing a protected resource and generates a tracking cookie for browsers considered as trusted. At the same time, Qrator.AntiBot restricts access to the resource for visitors who run script-based bots and/or utilize web scraping software suites, including full-stack browser-based solutions.

APIs protection

For the APIs used by native mobile app users (iOS & Android) Qrator.AntiBot supports several protection methods:

- enabling browser-based authentication (BBA) for app users on the login stage, checking the environment and the OS-defined browser used to perform BBA;
- validating security tokens with which the users have to sign their requests;
- filtering out the attempts to access the API directly.

Four Easy Steps of Customization for Your Business

Qrator.AntiBot checks can be set up and customized in the following steps:

1. Define the locations of your website where the users should confirm their authenticity by processing the check page: the entry points for your legitimate visitors.
2. Specify the locations of your website available only for validated users – crucial API calls, credentials fill-in forms, search methods etc.
3. Outline your trusted users and friendly bots by using header-based, IP/CIDR-based and geo-based exceptions
4. Choose the percentage of your user base affected by the set rules to conduct A/B tests and smoothly onboard the feature

Two operation modes

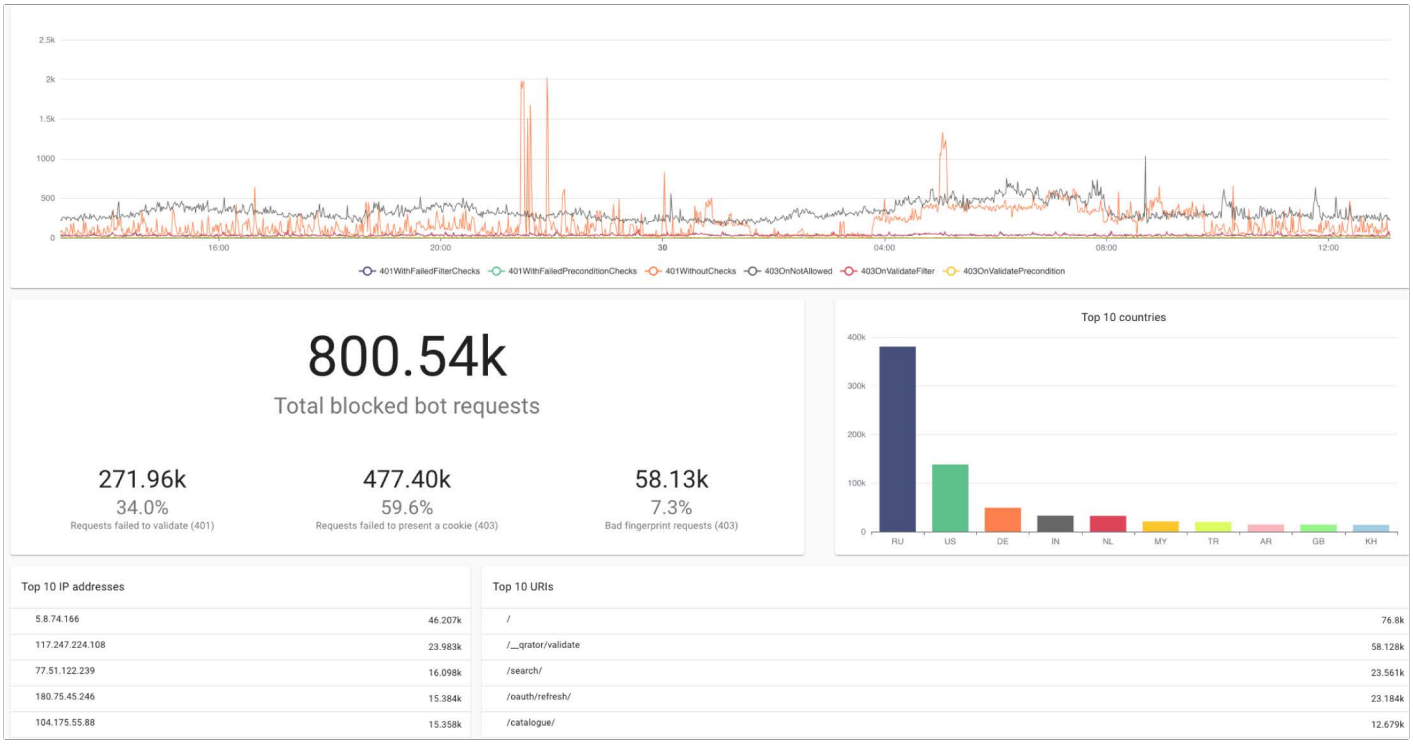
Monitoring mode

Qrator.AntiBot proxies a user's request further in case of any validation result. If a browser sends any response to Qrator.AntiBot, it will not receive an error code, but validation details will be recorded in the event log. The event log can be viewed anytime by a Qrator.AntiBot operator.

Blocking mode

Badly fingerprinted browsers or applications without JS support (including scrapers without the usage of browsers) will receive a customizable block page. A legitimate user will briefly see the check page first (a blank or a customized 401 page), and after validation will get the requested page.

The product's interface supports permissions for good bots, QA and other cases requiring bypassing the checks. Trusted IP addresses, CIDR lists, geozones and header rules can be specified to set up these scenarios.



QRATORLABS

qrator.net
sales@qrator.net
+420 602 558 144