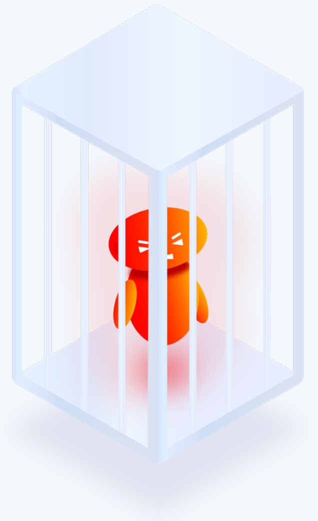

Bot Protection

Bots are a necessary and integral aspect of running virtually any service or hosting material on the internet. Not all bots represent a threat to legitimate users and their data. Many bots perform valuable functions such as indexing and monitoring. However, bots - in conjunction with scrapers - are also frequently used for nefarious purposes such as competitive intelligence gathering, data mash-ups, establishing fraudulent websites, probing system vulnerabilities, analyzing financial information, location tracking, and the theft of valuable or sensitive information.

Bad bots and scrapers typically swamp websites with thousands of requests per second, thereby reducing their speed, capacity or even availability for legitimate users.

Key Benefits

- Secure your web assets against unwanted Bot Traffic
- Allow desirable bots such as search engines
- Protect your APIs against abuse
- Regain lost capacity due to unwanted traffic

How we combat bad bots?

The most effective way of combating unauthorized bot behaviour is by reducing their efficiency - slowing them down and restricting the amount of content they are able to scrape. It is, however, not always desirable to simply block bots, some of which perform tasks that support commercial or other organizational functions. The Bot Protection Module is able to identify and classify bots, allowing them access within specified thresholds before they are blocked or directed to a “waiting room”, leaving legitimate access unaffected. We combat bot and scraper threats in nine separate steps (1-9) in the four phases - all in a matter of seconds.

Firstly, a series of static measures is utilized in our Threat Protection Centers™ (TPC™), then dynamically outside our TPCs, dynamically within our TPCs, and finally using a reCAPTCHA Challenge. This is performed quickly to minimize disruption for legitimate users. These steps, and their component parts, are outlined in more detail below.

→

Phase 1: Static measures run by our TPCs

1. Incoming traffic is matched against known bad bot sources (IP address reputation) and discarded.

2. Analysis of the origin of source IPs, only allowing traffic from known good sources.

3. User-agent identification against known unwanted bot families.

Phase 2: Dynamic measures conducted outside our TPCs

4. Using a JavaScript challenge, modern browsers can return answers in a series of different challenges. This requires no user intervention, and is automatically completed by any modern browser.

5. A cookie challenge is issued which forces the browser to accept a cookie which is expected in each subsequent request. This is a highly effective way of identifying fake browsers, scripts and automated tools.

6. Leveraging "deception techniques" on the client by injecting inception end-points -- for example images or JavaScript files -- which trick links produced on the client side to follow a pathway that would not normally be used. A legitimate browser would not respond to such end-points, but a script or tool is more likely to hit a deception end-point. We monitor our deception end-points, and identify illegitimate connections that reach them.

Phase 3: Dynamic measures handled by our TPCs

7. Inside the TPC™, we use several dynamic measures as well. Over a given period of time we monitor the number of requests made, the number of sessions, and the frequency of http error status codes. Statistical analyses of these and other figures is performed to identify abnormal or unauthorized activity.

8. We also run a large number of machine learning algorithms to identify and mitigate identified threats. This step is the Cloud Risk Engine component of Baffin Bay Networks' bot and scraper defenses, and its most dynamic

Phase 4: reCAPTCHA Challenge

9. Finally, if anomalies are still identified after all the above methods, a reCAPTCHA challenge can be presented to users. Because this measure requires users to input information, it is only used as the last in our sequence of anti-bot measures.
   If users are returned to pages other than those they expected, or if we identify abnormal activity from an IP address, we inject code fingerprinting, collect data from a suspect browser, and combine this with data gathered during the previous steps to identify unauthorized activity.

➞

Optimal user experience

All the mentioned measures are conducted in a matter of seconds, thereby minimizing disruption to user experience while keeping users - individuals, businesses and other organizations - and their data secure.

Threat Protection Centers™ (TPC)

Amsterdam, New York, Los Angeles, Singapore, Frankfurt & Stockholm (2).

Threat Protection Portal

Our portal monitors attacks in real-time. It provides statistics on all traffic and attempted attacks and a comprehensive reporting function allows clients to create daily, weekly and monthly reports.

You receive the best possible protection from fresh attacks with our Security Operation Center which monitors the constantly evolving threat landscape around the clock.

Regardless of where your assets are located – on premises, in cloud-based platforms, third party hosts – our Threat Protection Platform is equipped to provide multi-vector threat protection to all deployed assets.