Handle adversarial bots

Say you're dealing with adversarial bots or you have specific transactional endpoints you need to protect. For example, credential stuffing bots are attacking your login page. To stop attacks like this and combat the most sophisticated bots, turn to Bot Manager Premier, which you can add on to App & API Protector, or purchase alone.

1. Define resource to protect

To set up Bot Manager Premier, start by defining the transactional pages you want to protect, like your login and signup pages, for example. You define each as an API resource. Read how (login required).

2. Set expected traffic

Let Bot Manager know what client types make requests. When you do so, set an action for clients that you don't expect and make special allowances for those you do, like your own mobile app, for example. Use our special mobile SDK to protect your mobile requests.

3. Set your response strategy

You need information to craft an effective response to bots. The best way to get it, is to implement Bot Manager in monitor mode and see what kind of traffic you're dealing with. Based on what you observe you can eventually set different actions to handle specific bots you see. Some common and effective approaches:

- For Akamai-categorized bots, use the monitor or allow action for categories that are most relevant to your business and deny the rest.
- For the custom bot categories you have defined, apply the most relevant action depending on whether you want to allow or block the traffic.
- For transparent and active detection, consider setting a conditional action that works best for the resources you want to protect and apply that conditional action to all the enabled detection methods. More on conditional actions (login required).
- For behavioral detection (Premier only), use bot score to set up the most flexible and accurate response strategy on transactional pages like login.

Bot score

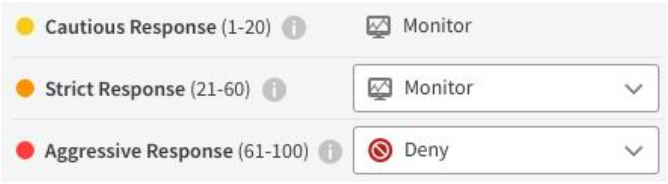
Bot score is an algorithmic measure from 0 to 100 which indicates the probability that a requestor is a bot. A score of zero is a human and 100 is a bot. You use the scores in between to set a varied response strategy based on how strict you want to be for different score ranges. The higher the score, the stronger a response action you can apply, like Deny.

Bot score lets you act on suspected vs confirmed bots differently. Based on your preferred approach and appetite for risk, you set response thresholds by score. For example, if you just want to keep any possible bots out and don't care if you block a lot of humans, you can set drastic actions like deny, even for requests that have a lower bot score. Or you may feel the opposite, and never want to block your potentially human visitors. In this case you could deny only requestors with bot scores of 90 to 100.

After you set thresholds, you craft your response strategy using three response segments:

- Cautious Response includes requests least likely to be bots, which you should monitor

- Strict Response is a mix of bot and human traffic, which you may want to test with a challenge action to let only humans through
- Aggressive Response contains the highest bot scores, which you may mitigate with a strong action like Deny.



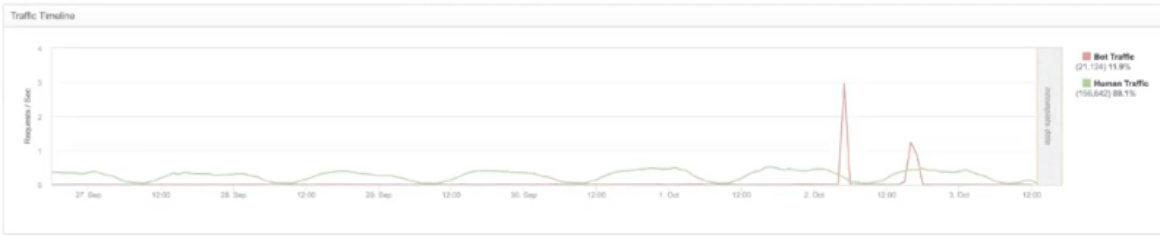
4. Monitor bot activity

After you set protections, use reporting to track their effectiveness. Start with actions set to monitor and alert for a few weeks. You want to understand what portion of all requests come from bots. What type of bots are they? Is Bot Manager detecting them properly? If so, what's the operator's goal, and how does each bot operate?

Bot Manager offers an assortment of reports to help you understand your specific issues, and see how well your settings are working. Use this data to tune your settings, and make sure you're not blocking legitimate users by mistake.

Among many other views, you can:

- See an overview of bot vs. human traffic



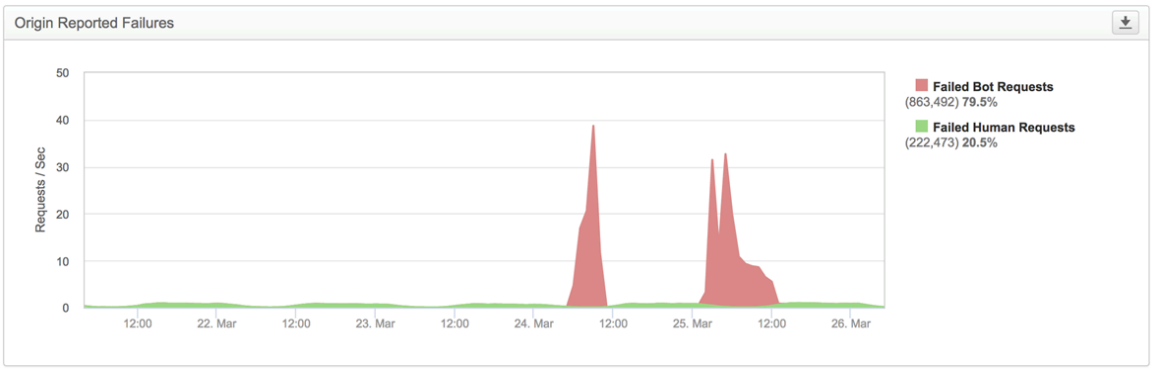
- See what pages on your site bots are targeting. They may skip fluff like images and style sheets, which human requests include. Instead, bots may go directly to a transactional page, like search.
- Drill down to investigate a specific bot. For example, see if it's attacking only you or others in your industry.

  
  View of requests on your site, industry, and all industries

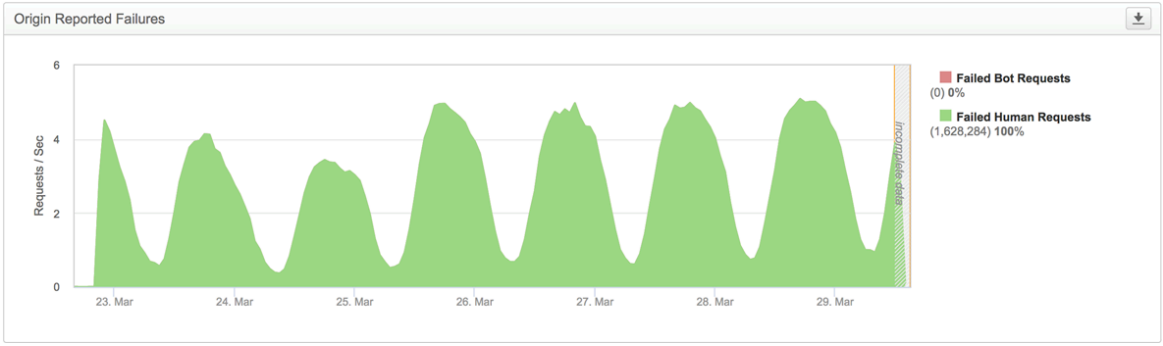
  Even see how others handled the same bot.

  
  Actions Applied

- View the effect of your protections. For example, with a protected resource in monitor mode you see both bots and humans submitting failed login requests:



After you set action to deny, bots are cut out and only human tries get through:



5. Tune your bot response

As you monitor bot traffic, tweak your bot management settings to minimize undetected bots and humans mistakenly classified as bots (login required). When you're confident that detections are working the way you want, change monitor actions to those that mitigate requests, like deny, tarpit, or challenge.

Updated over 1 year ago

← Detection methods

Thwart web scrapers →