YOTTAA

Bot Mitigation

Automated bots can consist of up to half the traffic to a website, and while some may be benign the vast majority are not. Yottaa's bot mitigation solution enables detection, tracking, analysis, and dispositioning of bot traffic to minimize website and visitor disruption.

Bot attacks continue to grow and are getting more sophisticated. Managing bot traffic can protect inventory availability, protect customer account information, enhance the visit experience, and ensure more accurate analytics data.

Bot Impacts

Yottaa's bot mitigation capability is a cloud native, behavior-based solution which enables the identification and management of bot traffic. It provides effortless integration into existing infrastructure with no release process required.

Web and mobile performance is preserved by using a JavaScript snippet to capture heuristics of each request. Benefitting from a large database of bot information, acquired from a large installed customer base, it operates with a low false positive rate. The bot mitigation capability is backed up by a proactive threat management service provided by always available security analysts and experts.

There are many different threats that are protected against. These can have a direct impact on each company's bottom line as well as compromising site visitors Personal Identification Information (PII).

- **Hoarding:** Bots can lock up products in carts which can artificially deplete availability, frustrate customers, and reduce sales.
- **Scalping:** By buying limited availability products inventory can be reduced for legitimate customers, forcing them into secondary markets with higher costs and lowering satisfaction.
- **Scraping:** Bots constantly scrape your web sites for prices, product reviews, inventory data to enable competitive intelligence.
- **Account Abuse:** User accounts can be hijacked to steal stored value and create new accounts to commit fraud.
- **Carding:** By trying number-pin code combinations bots attempt to "crack" accounts, including gift card and loyalty card accounts, to obtain funds or goods without payment.
- **Analytics:** Up to 50% of site traffic can be caused by bots, so inflating your data and skewing analytics. This results in decreased conversion rate data and misleading business intelligence.

Detecting and stopping bot attacks will save costs, ensure more accurate website data, and protect you and your customers from fraud and account abuse.

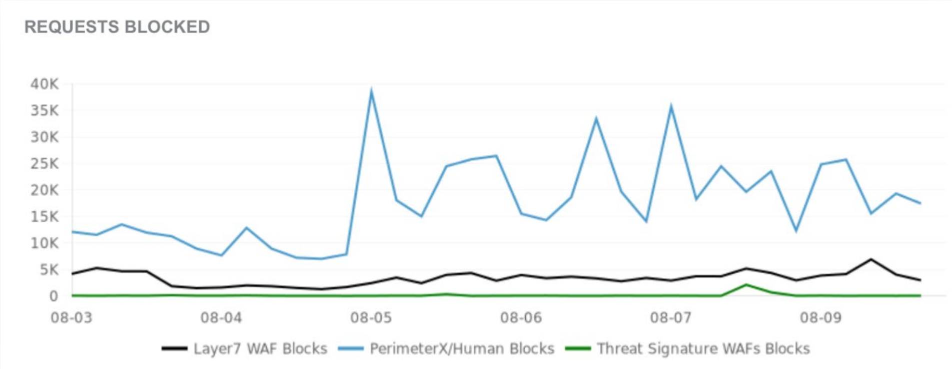
Detection and Mitigation

The YOTTAA bot mitigation capability consists of a detector element and an enforcer process. Detection and enforcement are performed at the edge data center layer and utilizes several tools to identify and characterize known bots. Bot mitigation is simple to install and enable and will not impact Page Load Time due to its asynchronous execution. An extensive database of bot fingerprints can be referenced through the large number of customers already using the tool. Behavioral analysis adds another level of protection to help identify human users from automated traffic.

- **Bot Sensor:** Is a JavaScript snippet that is inserted into your website using an automated content transformer, which loads the sensor to your browser. The sensor collects and sends data to analyze the user's device and behavior, as well as different network activities. It analyzes the authenticity of the device and application, and tracks user behavior and interaction.
- **Bot Detection:** Uses fingerprint-based tools, behavioral analysis, and predictive security intelligence to evaluate sensor and enforcer data in real-time to create a risk score. The user is then identified as being malicious or not and sends the risk score in a secure and encrypted token back to the user's device.
- **Bot Enforcer:** Is a module that is integrated as part of the Yottaa cloud, and is responsible for executing the enforcement functionality. All malicious bot traffic is blocked before it can reach a targeted site.
- **False Positive Resolution:** It is possible that some user traffic is incorrectly flagged as a bot. Built in validation processes can help resolve false positives using the "Press and Hold" process. A whitelisting capability is available to ensure specified web traffic is not subject to bot mitigation actions.
- **Real-Time Analytics:** The Yottaa dashboards provide detailed views of bot traffic and monitor incidents. These allow security rules to be adjusted in real-time.

Enablement of the bot mitigation capability does not require any code changes and allows simple control to switch the capability on or off if required by the customer. Yottaa bot mitigation is deployed across an entire site rather than specific pages to provide better, more deterministic data which allows informed decisions to be made for traffic control.

An SDK is available to integrate into native applications which are increasingly being used. There is an increase in the number of bots starting to use native application user agents to try to bypass defenses, but the SDK and native integration help detect and prevent them.



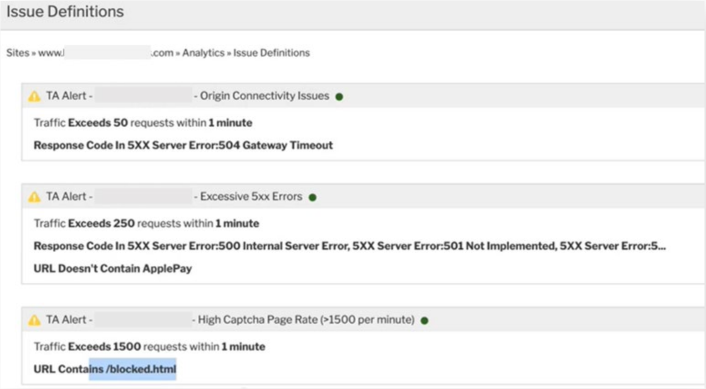
Firewall and Bot mitigation complement each other to protect websites from unwanted requests.

Bot mitigation with Yottaa allows effortless integration using a cloud-native behavior-based solution.
Its operation preserves performance, providing low false-positives and continuous proactive threat management. A simple ‘real visitor’ check process allows fast verification and minimal disruption.

Configuration and Settings

Using the Yottaa Transformers a small JavaScript element can be injected into the page that will quickly and effortlessly enable bot mitigation without the need for any source code updates. Once installed several settings can be made directly in the Yottaa forms to optimize the bot mitigation operation.

- **Configuration** to set bot mitigation in test or block mode; redirecting the block to a custom URL.
- **Sensitive Routes** allow defining headers and route prefixes and suffixes to apply additional scrutiny for extra security against bots. These may include login pages, ‘check my balance’, gift card, or checkout pages.
- **Whitelists** allow defining URLs and User Agents to not have bot checking performed such as VPN IPs, Partner IPs, analytics URLs, etc.


Issue Definitions

Sites » www.[redacted].com » Analytics » Issue Definitions

⚠ TA Alert - [redacted] - Origin Connectivity Issues ●

Traffic **Exceeds 50** requests within **1 minute**

Response Code In 5XX Server Error:504 Gateway Timeout

⚠ TA Alert - [redacted] - Excessive 5xx Errors ●

Traffic **Exceeds 250** requests within **1 minute**

Response Code In 5XX Server Error:500 Internal Server Error, 5XX Server Error:501 Not Implemented, 5XX Server Error:5...

URL Doesn't Contain ApplePay

⚠ TA Alert - [redacted] - High Captcha Page Rate (>1500 per minute) ●

Traffic **Exceeds 1500** requests within **1 minute**

URL Contains /blocked.html

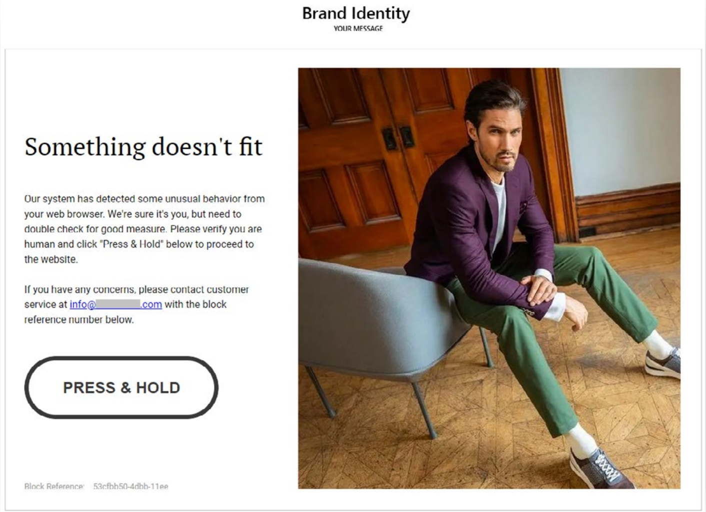
Alert definitions can send an alert if a limit is reached (e.g. over 1500 challenges within one minute)

Verification

While there should be no impact on regular visitors to a website there are times when the system may not be able to clearly identify a bot or regular traffic. While no PII is collected, the detector will look for user interactions such as mouse movements and mouse clicks, the rate of hits and click stream at a site. If the browser indicates a mobile device the detector will try to identify a battery and battery level indicators. If still unable to decide, the enforcer will put out a challenge page to verify a human visitor. Challenges, commonly referred to as “CAPTCHA”, use a patented “Press and Hold” technology which is simpler to use and is very suited for mobile devices with their small screen size.

Blocks are by default identified by a 403 response code. An option is available in the portal to generate a 307 redirect response code and a custom page with tailored text and image can be used as redirection for a challenge.

For the best user experience the number of false positives should be as low as possible. A target of under 0.4% of successful “CAPTCHA” challenges is the goal which can be monitored via the dashboards and by setting up an alert. The ability to setup alerts is a valuable feature for quickly being able to become aware of changes in visitor behavior, allowing quick investigation and follow up actions to be taken if required.


Brand Identity

YOUR MESSAGE

Something doesn't fit

Our system has detected some unusual behavior from your web browser. We're sure it's you, but need to double check for good measure. Please verify you are human and click "Press & Hold" below to proceed to the website.

If you have any concerns, please contact customer service at info@[redacted].com with the block reference number below.

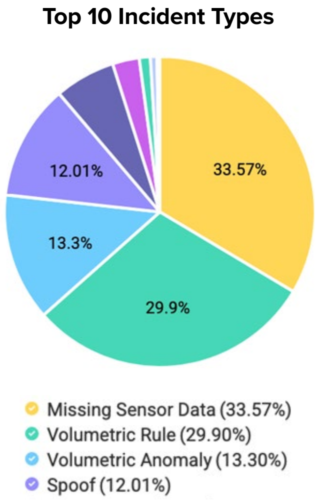
Block Reference: 53cfbb50-4dbb-11ee

Example of a custom “CAPTCHA” page showing the PRESS & HOLD challenge.

Analytics

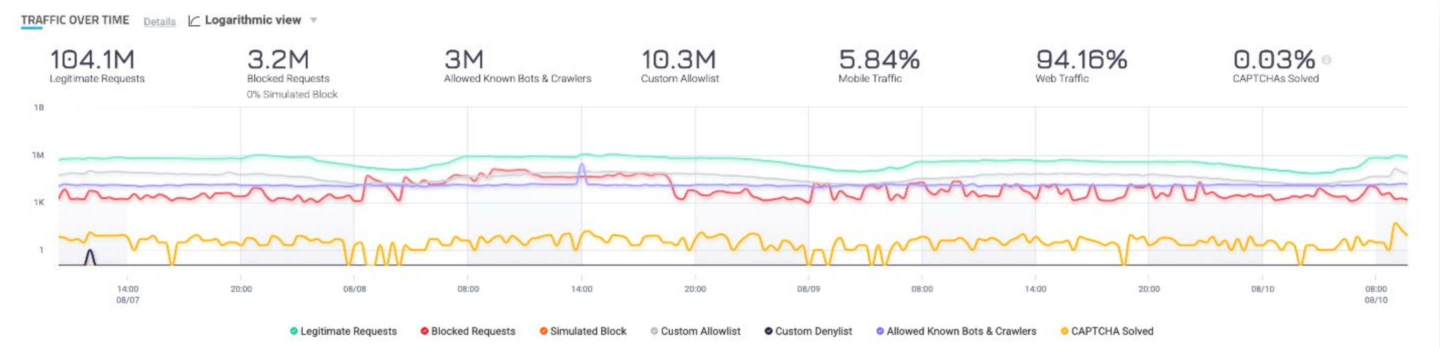
Several charts, tables and graphs can be accessed to obtain a detailed understanding of unwanted bot and legitimate visitor traffic. Having bot mitigation enabled will allow analytics tools to get more accurate analytics data for legitimate visitors. Unwanted bot requests are blocked at the server so never reach the site and analytics tools will never catch a page view. As bot traffic can comprise up to 40% or more of traffic to a site there could be a significant drop in page views, but the new number is more representative of real business levels of legitimate activity.

Many different bot attacks can be detected and blocked including when bots attempt to fool a site by trying to disguise the sender as something it is not. This could be making it look like it is from a mobile device, but no sensor data is available, or from a legitimate service such as a Google bot but analysis of the signature identifies it as a malicious bot.



Accurate Insights:

Bot mitigation shows a site’s bot traffic. Removing bad traffic results in accurate analytics, reduces fraud or downtime, and protects inventory and sales for customers. Traffic volume measured by analytics tools decreases, but reflects real visitors, as bot traffic is blocked at the server.



This logarithmic chart shows solved CAPTCHAs, blocks, and legitimate requests.

Note the logarithmic scale for the traffic chart above. When viewed over time, increased periods of bot attack can be seen. For this site the level of false positives is being very well controlled with a solved “CAPTCHA” rate of 0.03%. Table data can be viewed which lists the blocked traffic and can be drilled down to specific reasons for the block. The tables show the target URL, and the IP address of the sender.

Most data is retained for 14 days, such as “CAPTCHA” Reports, all “Tops” Tables, and the Investigation Page (when using search filters). Top Incidents and all Graphs Over Time are retained for 14 months of data.

Yottaa bot mitigation is implemented in partnership with Human (formerly PerimeterX) and is powered by their best in class, industry proven defense platform. The partnership provides access to their vast knowledge base of good and malicious bots and enables fast protection to be implemented when any new threats are detected.

The simple implementation of bot mitigation provides visibility of bot attacks and delivers more accurate traffic analytics allowing for better informed business decisions. The dashboards and charts are supplemented by a weekly security email showing all aspects of protection including the bot traffic and trends.

The Next Step

Don’t just assume that your eCommerce site is performing as fast as it needs to – be sure with a free, no obligation YOTTAA trial. Start the process today with a FREE Performance Snapshot. **Click HERE for more information. You can’t afford not to.**