YOTTAA

Anomaly AI

Anomalies are unusual events in your site's data. Using machine learning Yottaa tracks your site over a two-week period and identifies any spikes or plunges in the site data and provides instant alerting. This allows you to identify anomalies with your digital experience before they affect customers and your online sales.

Anomalies are not necessarily bad. For example, a spike in traffic might trigger an anomaly. However, the root cause could be something positive like a successful marketing campaign. Or it could be something negative like a malicious bot. All anomalies are tracked and made available via an online dashboard, email, Slack channel, or other endpoint.

Anomaly AI sets performance thresholds to the behavior of your website pages based on their historical performance over a rolling two-week baseline. If its machine learning algorithms determine that a threshold is consistently exceeded (revealing unusual performance behavior), then the event is tracked and an alert can be generated.

When performance thresholds are consistently exceeded, Anomaly AI alerts you that an optimization is needed (e.g., image compression due to a recently added image with a large file size). Anomaly AI may also recommend specific optimization techniques based on the nature of the performance violation.

Anomaly Detection

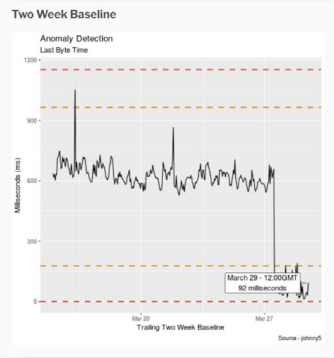
Anomaly AI incorporates three types of anomaly detection: Time series forecasting, threshold tests and analysis of baseline changes.

- **Time Series** – The time series model, Seasonal Autoregressive Integrated Moving Average, SARIMA or Seasonal ARIMA, for detecting anomalies on a periodic set of data such as Pageviews over specific periods of time.
- **Threshold tests** – If the data doesn't follow some period form then we use a threshold to see if the data is above or below this value.
- **Baseline changes** – If we detect that the baseline has changed for the site we will also detect an anomaly.

A Medium or High priority is then assigned to each anomaly based on a high low calculation using multiple algorithms depending on the length of baseline. A breakout detector determines when data is above or below the baseline with a high low forcing data outside of the range to determine priority.

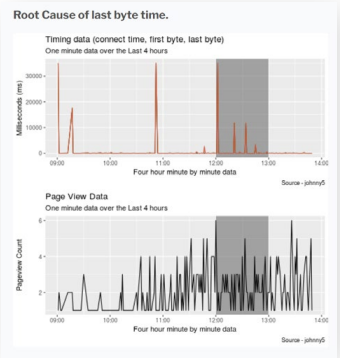
Two-Week Baseline graph

Displays the anomaly metric for the two weeks leading up to the anomaly. Lines show the threshold for a medium-priority anomaly, and the threshold for high-priority anomalies. The graph illustrates whether it was simply an aberration or sustained over time.



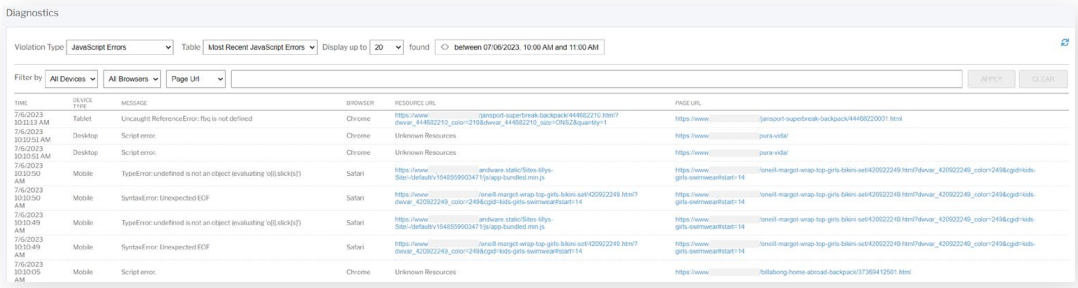
Contributing Factors graphs

Two graphs display potential root causes of the anomaly. The top graph shows other metrics within the same category. The bottom graph usually shows page views. Each displays minute-by-minute values for the four-hour period leading up to the anomaly. The gray bar highlights metrics measured at the same time as the anomaly. In the example, page views did not go up during the anomaly, meaning it is likely unrelated to customer traffic. In this case, the user would have to do further research using the Performance Inventory page and other dashboards to figure out what is causing the anomaly.



Triggering Requests

This information displays JavaScript Errors. It shows the user agent, console error message, page url, and device, among other data points. You can use this information to identify any problems with URLs that may be causing JavaScript errors and to recreate the issue for troubleshooting purposes.



YOTTAA

Alerts

Alerts include line graphs displaying the anomaly as compared to a two-week baseline, as well as contributing factors. Anomaly alerts are provided in a dashboard, via email, and through Slack via YoBot.

Security Anomaly Alerts

When your site also uses Service Blocker and/or Yottaa's edge acceleration service, additional security anomaly alerts can be configured. Whenever a blocked service attempts to access your site's pages, or any element protected by a page security rule, Service Blocker logs it as a violation. If there is a sudden spike or drop in the number of violations, an anomaly alert is generated.

A spike in security violations likely means that a new service is attempting to access your site. This could be a third party that you have recently added to your site, a malicious service, or even a first- or second-party resource that Service Blocker has not yet identified.

The anomaly alert tells you if the service (or services) was flagged or blocked. Flagged violations occur only in rules configured in a report-only mode, which allows third-party services to access a site, site section, forms or form fields. Blocked violations occur only in rules configured in an enforce mode, which prevents third-party services from accessing your site, site section, forms, or form fields.

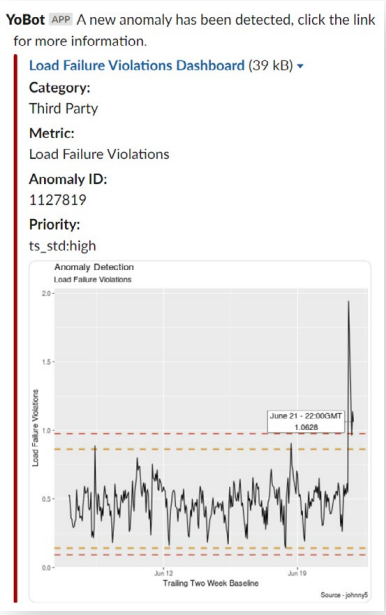
Over a weekend, a Yottaa customer had forgotten to renew the license on their ratings and reviews solution and it began generating errors in the customer experience. Yottaa quickly detected the problem and was able to temporarily remove the service from the product listing pages.

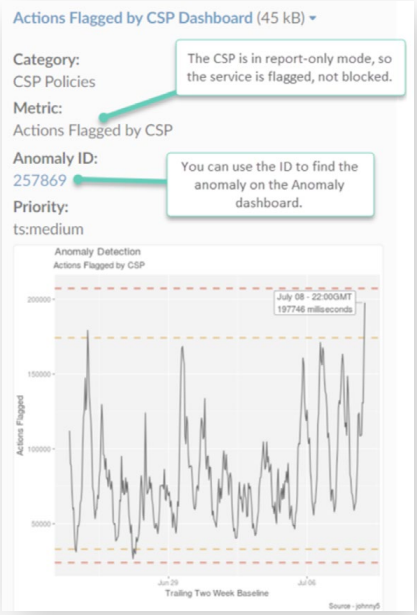
On a Black Friday, Yottaa detected a big increase in delaying page load violations and load failures across multiple customers caused by one of the analytics provider's beacons. It caused page loads to increase by 5 seconds due to a 5 second time out. Yottaa's Anomaly AI identified the problem, alerting customers and Yottaa support and deploying an app sequencing rule to make it a non-blocking script so the storefonts remained in business while each company resolved the issue.

YoBot

YoBot uses Slack, a collaboration tool, to alert you about anomalies, or unusual behavior, on your site. Anomalies are not necessarily bad. Use alerts to triage and investigate further. You can also ask YoBot to generate reports on site metrics. YoBot displays Alerts, Performance Reports, Recent Anomalies, Recent Trends as a chart in a chat thread.

YoBot also sends alerts when it detects a new trend or a consistent change in your site data. YoBot displays trends as a line graph and allows you to ignore the trend or accept it as the new baseline from which to detect anomalies.





Beyond Anomalies

YoBot also provides access to performance reports and trends for onload time, first byte, last byte, and page views over time for the following periods of time:

- The past 24 hours and the previous 24-hour period
- The past 30 days and the previous 30-day period
- The past hour and the past 24 hours

While these events are not extreme enough to trigger an anomaly, they are meaningful enough for you to monitor and investigate.

YOTTAA

Web Metrics with Anomaly AI

Yottaa collects anomaly data and provides the ability to subscribe to each of the following types of metrics:

Pageviews: A sudden increase or decrease in pageviews for your site is monitored. You can investigate pageview anomalies by looking at your traffic analytics tool to pinpoint what the problem might be.

JavaScript errors: JavaScript error anomalies are usually caused by third parties, user paths, and code errors. They can also be caused by a new campaign, A/B testing, or ad technology.

Resource count: Resources are anything that renders on the page (e.g., CSS, JavaScript, fonts, images, videos, etc.). The anomaly alert tells you on which page the resource count anomaly occurred and whether the resource count changed for any specific third party. Resource count anomalies are rare. They usually occur after events like a site redesign.

Violation metrics: Yottaa collects anomaly metrics about violations generated by resources, including third-party violations, page delay violations, and size violations. For more about the different types of violations, see Yottaa's Third-party Service-level Violations capability.

Load time: The performance of each page of your site is tracked and monitored for an anomaly against your baseline load metrics such as onload, first byte time, and last byte time.

Web Browser Performance Metrics

1. first_byte_time
2. first_input_delay
3. first_input_start_time
4. hero_image_display
5. last_byte_time
6. on_load_time
7. largest_contentful_paint
8. cumulative_layout_shift
9. time_to_interactive
10. size_violations
11. page_delay_violations
12. performance_risk_violations

Third Party, JavaScript, and CSP Metrics

1. resource count
2. javascript_errors
3. load_failure_violations
4. blocking_violations
5. security_violations
6. csp_enforce_count
7. csp_report_count

Traffic and Edge Security Metrics

1. event_count
2. ta_event_count
3. rate_2xx
4. rate_3xx
5. rate_4xx
6. rate_5xx
7. waf_firewalled
8. waf_security
9. waf_threat
10. os_first_byte_time
11. os_load_time

Not knowing how well your site is operating, or if there are underlying issues, can result in lost conversions and create negative impressions. Being able to see when something is behaving outside of the norm allows key operational aspects to be monitored closely for real issues. When detailed information on frequency, location and type of anomaly or error is occurring, time and effort to fix is minimized and the best visitor experience is maintained, helping prevent lost revenue and preserving brand value.

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.**