



White Ops[®]

Fortune 50 CPG company works with White Ops to investigate fraud

SUMMARY:

- A multi-national CPG brand approached White Ops in August 2016 to conduct a year-long analysis of non-human traffic coming to its website.
- The results provided a series of baseline metrics and insights that will help the brand combat fraudulent traffic in the future.

THE CHALLENGE:

Establishing a baseline of fraud

In August 2016, one of the world's largest CPG brands came to White Ops looking for some help. The company wanted to conduct a year-long audit of fraudulent traffic coming to its website. Over 50,000 sites were tagged and the results yielded some very interesting findings.

THE SOLUTION:

Monitor traffic with White Ops to get detailed visibility

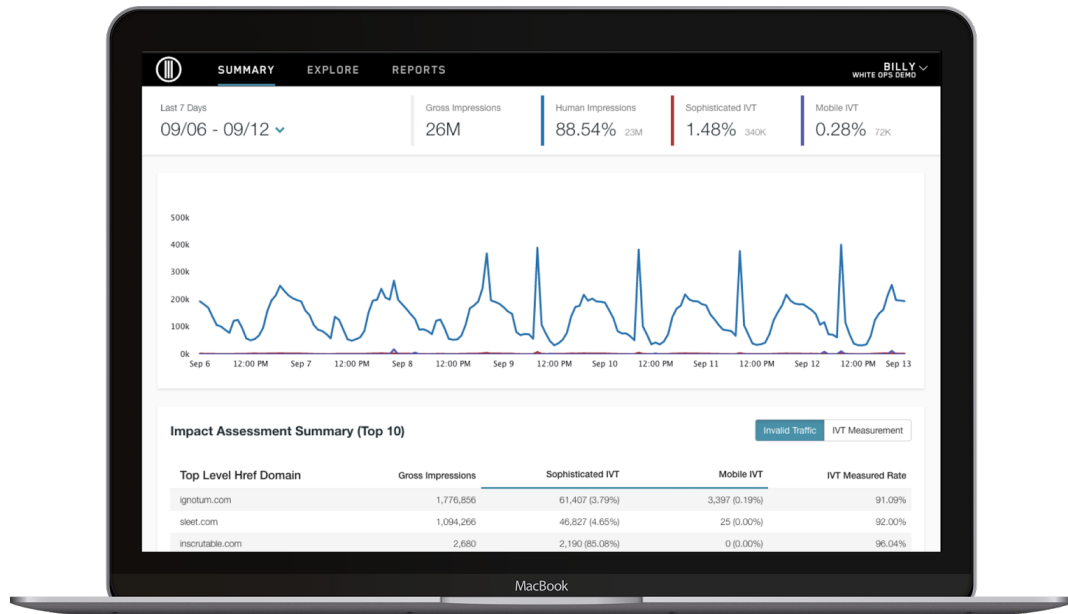
In the United States alone, 99.2 million pages were monitored. These pages had a fraud rate of just over 6.3%. While the overall rate of fraud was fine, there were several examples in which the non-human traffic surged to nearly 80%.

With FraudSensor, the team was able to discover that the surges in fraud were mostly associated with specific event-based campaigns. These campaigns that were run in periods of high demand were prone to much higher rates of fraud. This isn't an issue specific to this one advertiser -- periods of high demand are known for being particularly popular with bots. Cybercriminals carefully craft botnets to look like very appealing audience segments so the moment demand increases, the entire advertising ecosystem is willing to pay to get their seemingly-human impressions.

The White Ops technology also revealed the specific sources, campaigns, and mediums that were driving the highest rates of fraudulent traffic. With this granular data, the CPG company is able to return to the sources of fraudulent traffic and seek remediation and ensure that the traffic is cleaned up.

WHITE OPS FRAUDSENSOR

FraudSensor provides scalable bot detection and reporting to give you unprecedented visibility into the sources of fraud.



Gain visibility

Get insight into the scale and source of your bot problem to find the cybercriminals that hide in plain sight.



Detect & respond

Simply knowing you have a bot problem isn't enough. Ensure you use your data to prevent fraud in the future.



Streamline workflows

Automate reporting and share data with approved parties to help save time and improve your fraud fighting efforts.

