White Ops

White Ops catches 4x more fraud than competitor in head-to-head trial

SUMMARY:

- One of the most well-known programmatic agencies in the world wanted to neutralize risk of ad fraud in its buys.
- It set up a trial among different providers to find out which was the best at detecting non-human traffic.
- White Ops caught 4x more fraud than the next competitor.

THE CHALLENGE:

Determining the best bot mitigation vendor

One of the world's largest programmatic agencies decided to do a side-by-side comparison of ad fraud detection providers. The reason was simple: ad fraud has been an enormous challenge to the media world and the agency knew that in order to keep its competitive edge it needed to select the best provider to defend against fraud.

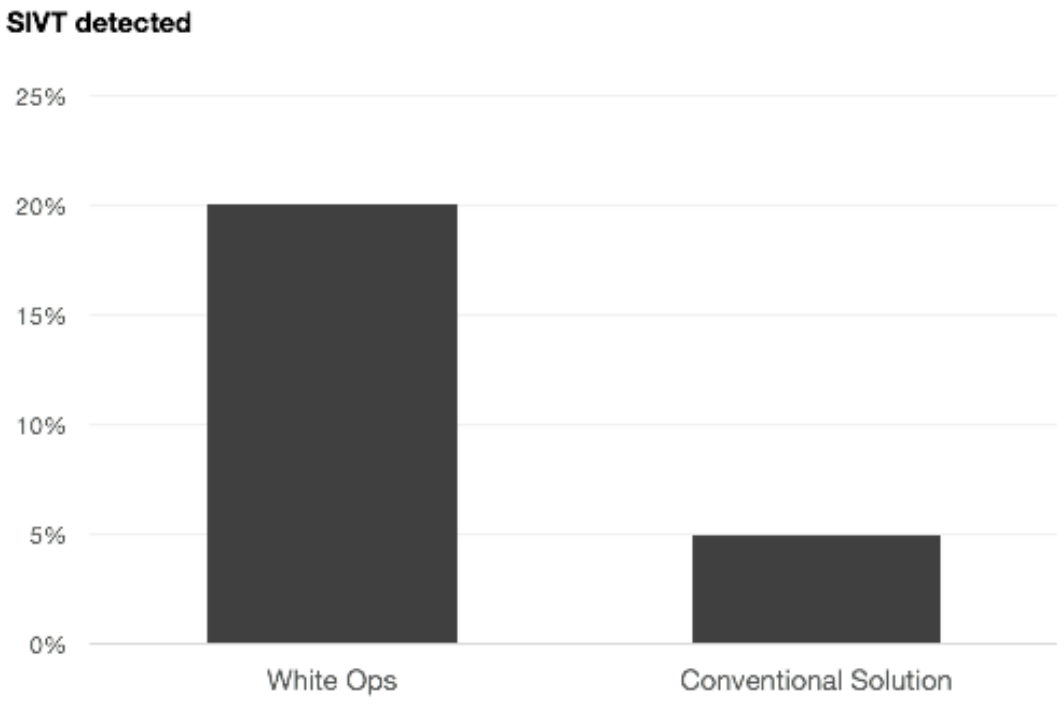
The agency decided to test rates of non-human traffic with one of its video publishing partners, as video has become a well known area of SIVT. Recent research has shown that as much as 22% of video advertising budgets can be lost to fraud. The explosive growth in online video has created high demand for more inventory, and some publishers source traffic to meet that demand. That's where the bots come in.

The agency organized the test to see which had the best results.

THE SOLUTION:

Directly investigate each transaction

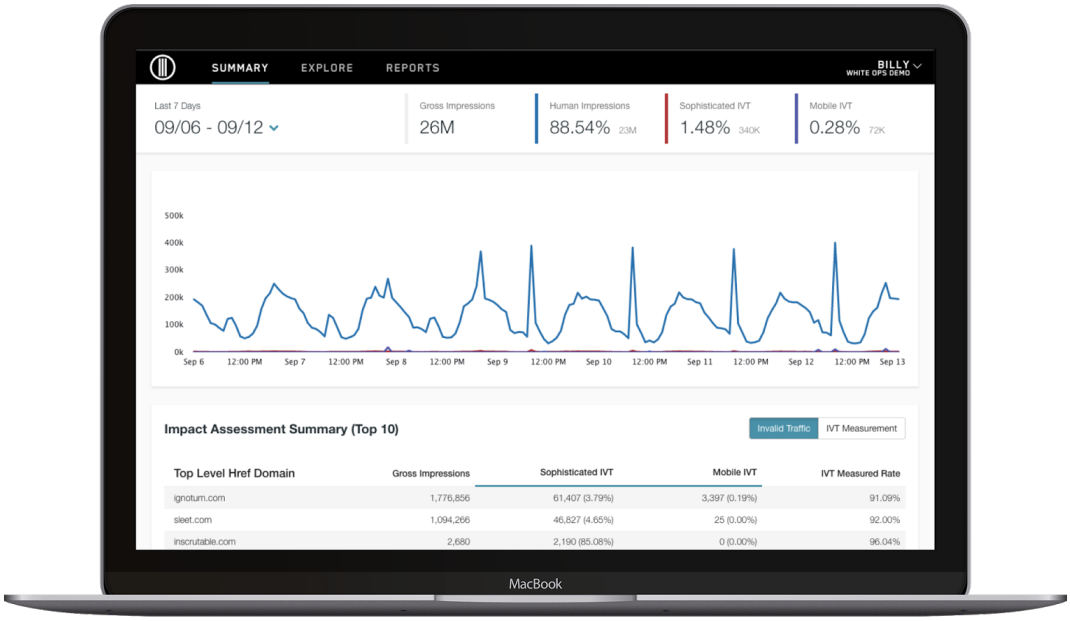
After a few weeks of monitoring, White Ops emerged as the clear choice for ad fraud detection and prevention. On average, White Ops FraudSensor identified a 20% rate of non-human traffic to the website. The closest competitor identified just 5%. This 4x difference in detection could translate to millions of dollars of wasted spend.



White Ops Human Verification technology better identifies bots because it investigates every individual transaction directly, rather than merely scanning for behavioral anomalies. Simply surveying for non-human behaviors was an effective method when bots were simple. Often, these bots were basic scripts operating from a single data center. However, today, due to the rise of "malware-as-a-service" (MaaS), over 70% of bots operate on residential computers. This newfound real estate gives cybercriminals increased ability to impersonate human behaviors. It's time for a different approach to bot defense — one that focuses less on how a device behaves and more on the device's fundamental characteristics.

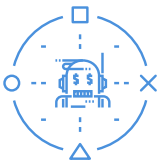
WHITE OPS FRAUDSENSOR

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.


White Ops