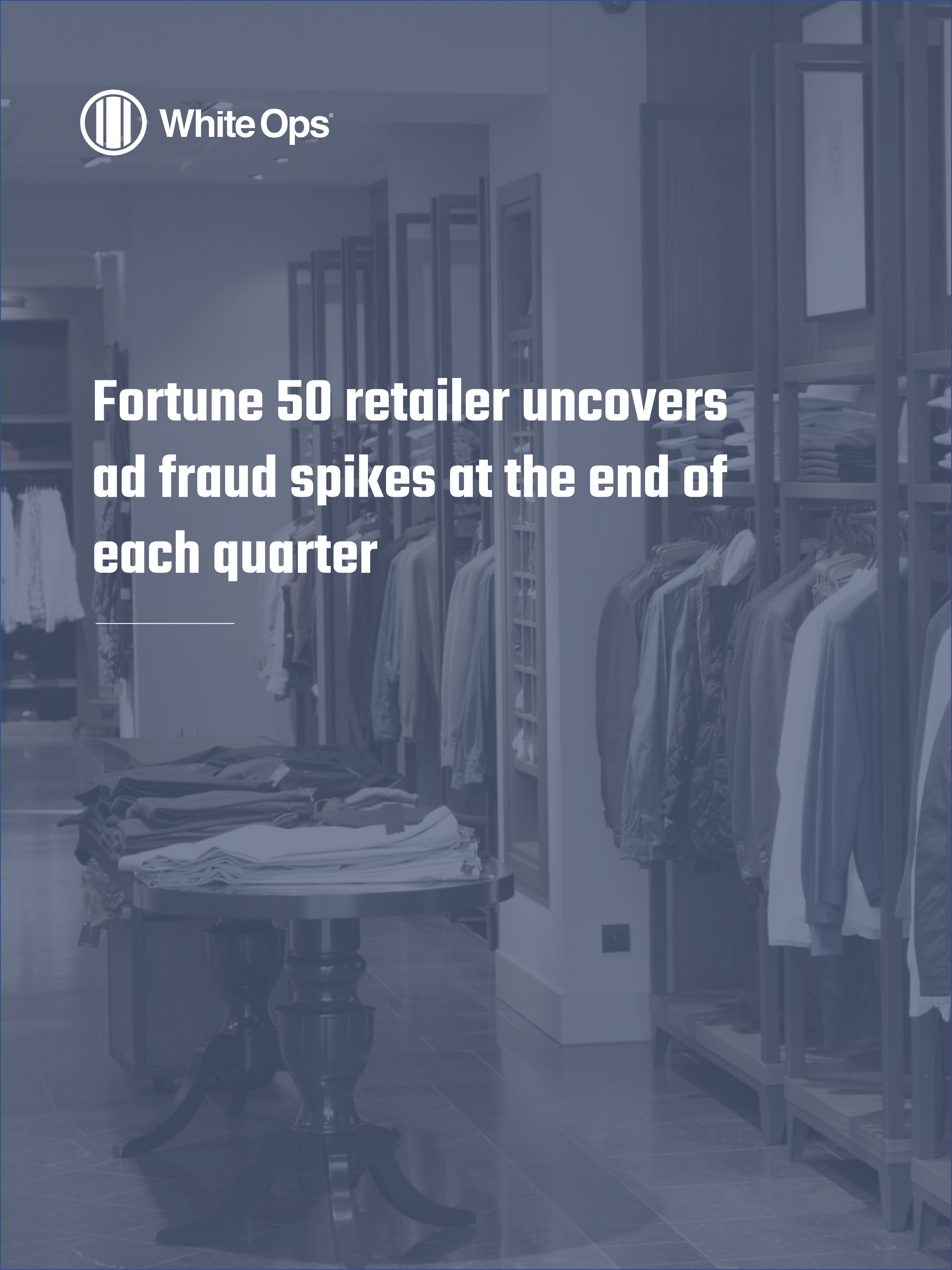
White Ops®



Fortune 50 retailer uncovers ad fraud spikes at the end of each quarter

SUMMARY:

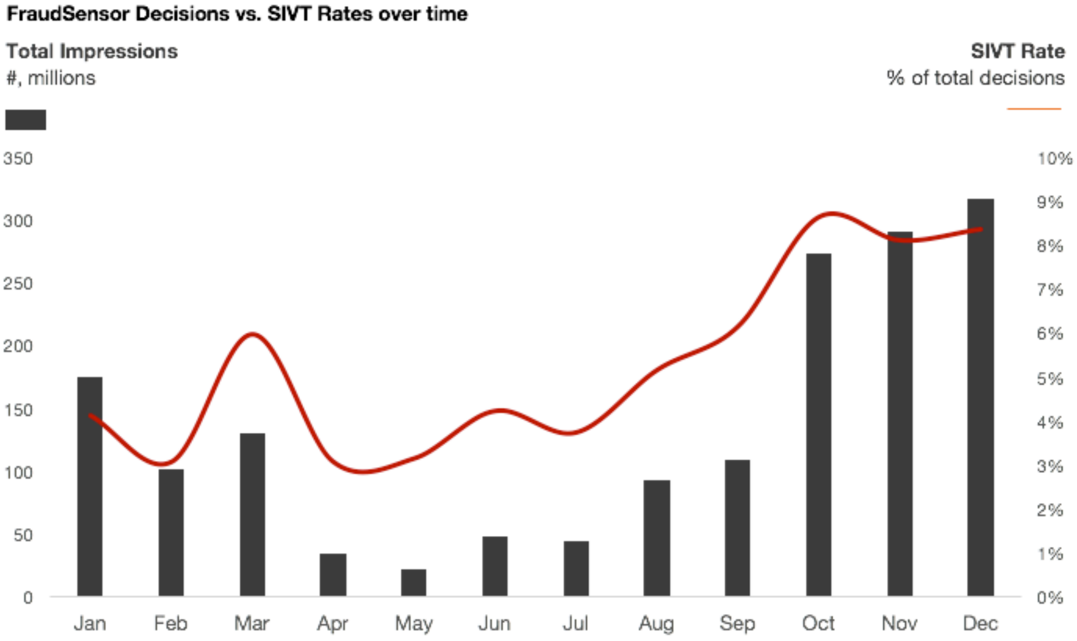
- During a year-long audit with White Ops, a national retailer saw a surge in ad fraud at the end of each quarter, but couldn't figure out why.
- The problem only worsened in Q4, when non-human impressions rose from 4% to almost 9%.
- White Ops helped the advertiser recover most of the lost spend through remediation.

THE CHALLENGE:

Quarterly spikes in fraudulent traffic

A Fortune 50 retailer enlisted White Ops to conduct a year-long review of its exposure to invalid traffic. Digital represented their second largest advertising spend, and the company wanted to be sure it wasn't wasting any of this budget on bots and cybercriminals.

After implementing the White Ops JavaScript tag, it became clear that the brand had generally low rates of SIVT. However, dramatic surges of non-human traffic were seen at the end of each quarter. For example, fraud rates in March were 60% higher than those in January or February. The spikes seemed to mirror the traditional flow of media spend, which typically rises at the end of each quarter and end of the year.



These spikes were persistently reported during the last month of each quarter — but their source was unclear. The situation became particularly problematic in Q4 as most of the ad spend was used. Nearly 9% of Q4 impressions were non-human — 84% more than all the preceding quarters' impressions. This spike represented almost $1.5 million in lost media budget. The brand couldn't determine the reason for the pattern.

THE SOLUTION:

Be wary of purchased traffic

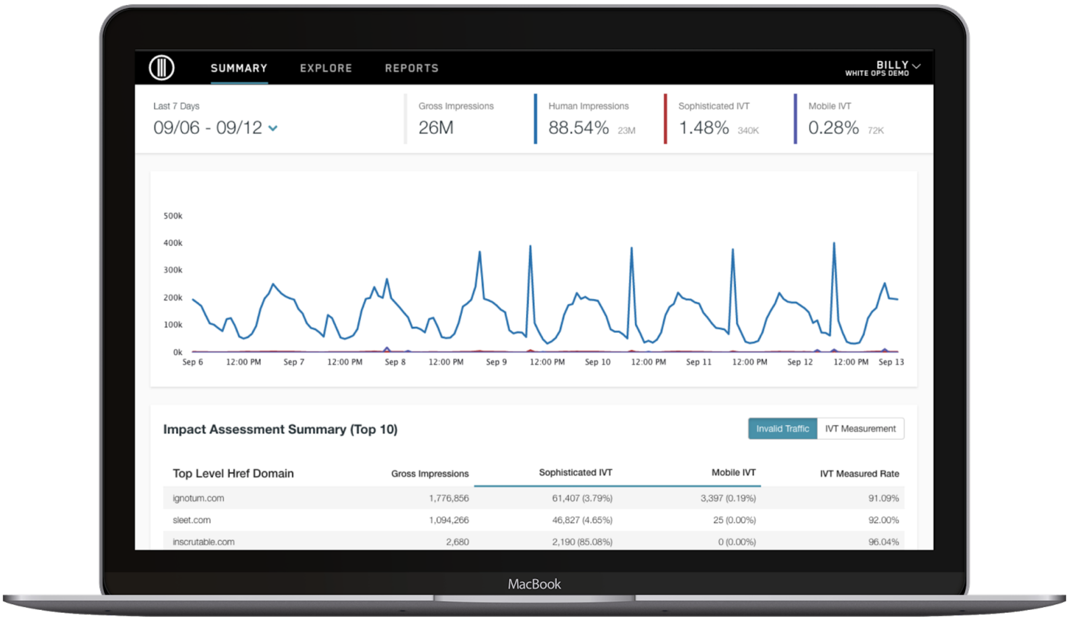
Using FraudSensor, White Ops and the retailer conducted hotspot analyses — a series of investigations that analyze the data in progressively more detailed ways — to identify the sources of non-human traffic. It became clear that the fraudulent traffic was coming from acquired sources that publishers were using to fulfill campaign requirements at the end of each quarter and throughout Q4.

If purchased traffic seems too good to be true, it probably is. Today's sophisticated bots often appear perfectly human and evade detection easily. For instance, over 75% of fraud observed in the most recent Bot Baseline study came from computers housing both human and bot activity on the same machine. Purchased traffic that looks *exactly* like the audience you need is likely manufactured by cybercriminals to appear as such.

The retailer reclaimed the majority of spend lost to non-human impressions with the help of White Ops' transaction-level reporting. Due to the detailed data provided by FraudSensor, the retailer was able to understand precisely what needed remediation and to identify reliable partners for future campaigns.

WHITE OPS FRAUDSENSOR

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



Last 7 Days	Gross Impressions	Human Impressions	Sophisticated IVT	Mobile IVT
09/06 - 09/12	26M	88.54% 23M	1.48% 340K	0.28% 72K

Impact Assessment Summary (Top 10)

Top Level Href Domain	Gross Impressions	Sophisticated IVT	Mobile IVT	IVT Measured Rate
ignotum.com	1,776,856	61,407 (3.79%)	3,397 (0.19%)	91.09%
sleet.com	1,094,266	46,827 (4.65%)	25 (0.00%)	92.00%
inscrutable.com	2,680	2,190 (85.08%)	0 (0.00%)	96.04%

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®