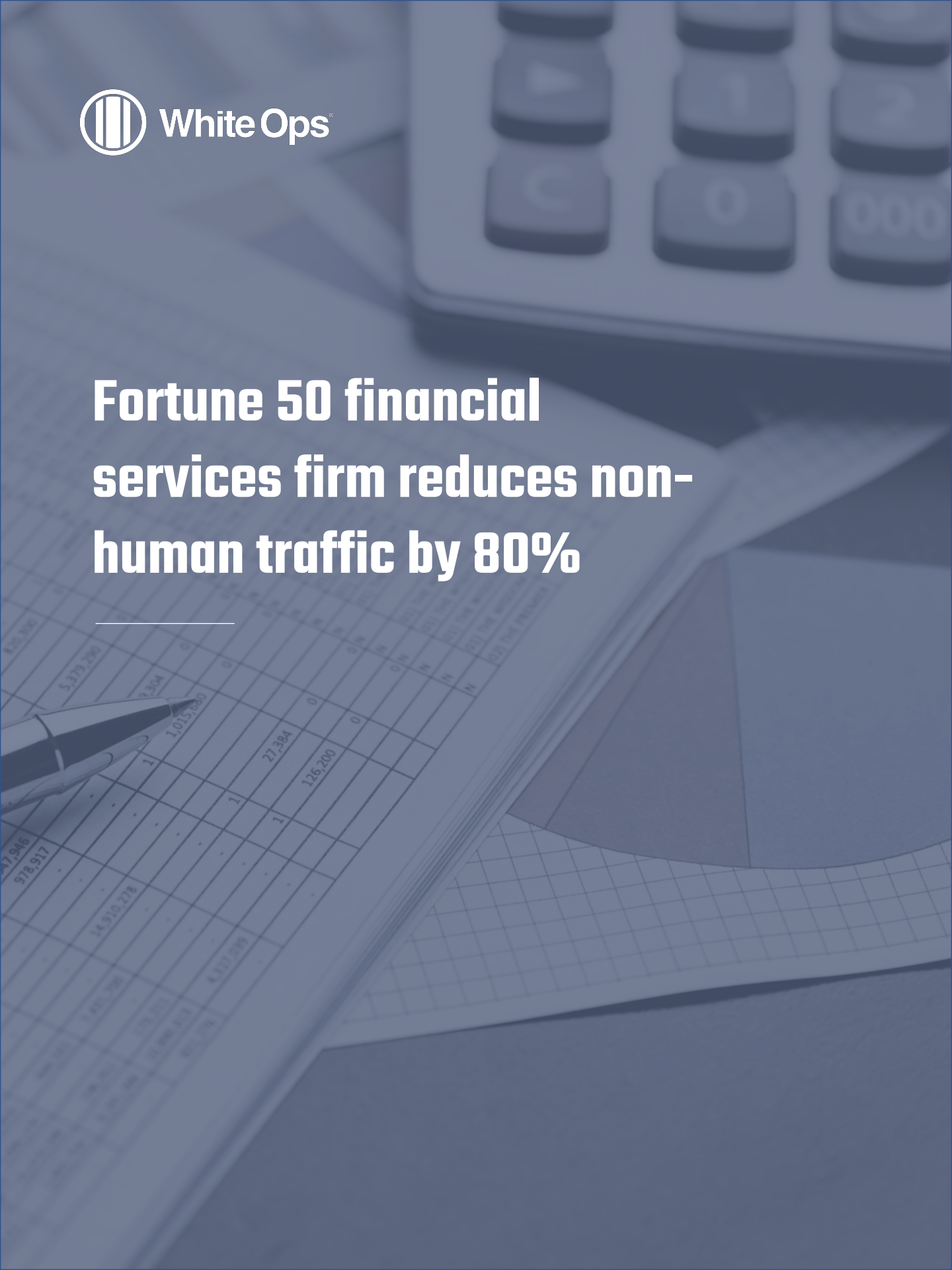
White Ops

Fortune 50 financial services firm reduces non-human traffic by 80%



SUMMARY:

- After finding an alarming 9.2% rate of invalid traffic in its campaigns, a leading financial services company decided it needed to fight the fraud.
- It worked with White Ops to reduce that rate to 1.8%.

THE CHALLENGE:

A worsening fraud problem

A large financial services company participated in a recent White Ops-ANA Bot Baseline Study, and was surprised to discover a 9.2% SIVT rate. This rate of fraudulent traffic was alarming in and of itself, but the company was particularly distraught because this number represented a 30% rise in bot traffic since they participated in the same study a year prior. The financial services company now had some of the worst rates of fraud of all the surveyed companies — and the problem was worsening.

The fraud did not affect all of the company's campaigns and buys equally. For example, direct buys had a 4.1% SIVT rate, but programmatic buys had a 15.5% SIVT rate and network buys had a 16.3% SIVT rate. There were some clear campaigns and domains that were driving these rates up.

There's an assumption in the marketing world that ad fraud attacks all campaigns equally, but this isn't really the case. Instead of skimming a small percentage off the top of all your campaigns, cybercriminals have very specific targets to maximize their payout. The financial services company was learning this firsthand.

Upon further analysis, the company learned that the fraud equated to almost $1.2 million in lost budget. Needless to say, the company was not pleased about this — and took the findings as a serious wake up call about their current detection tools.

THE SOLUTION:

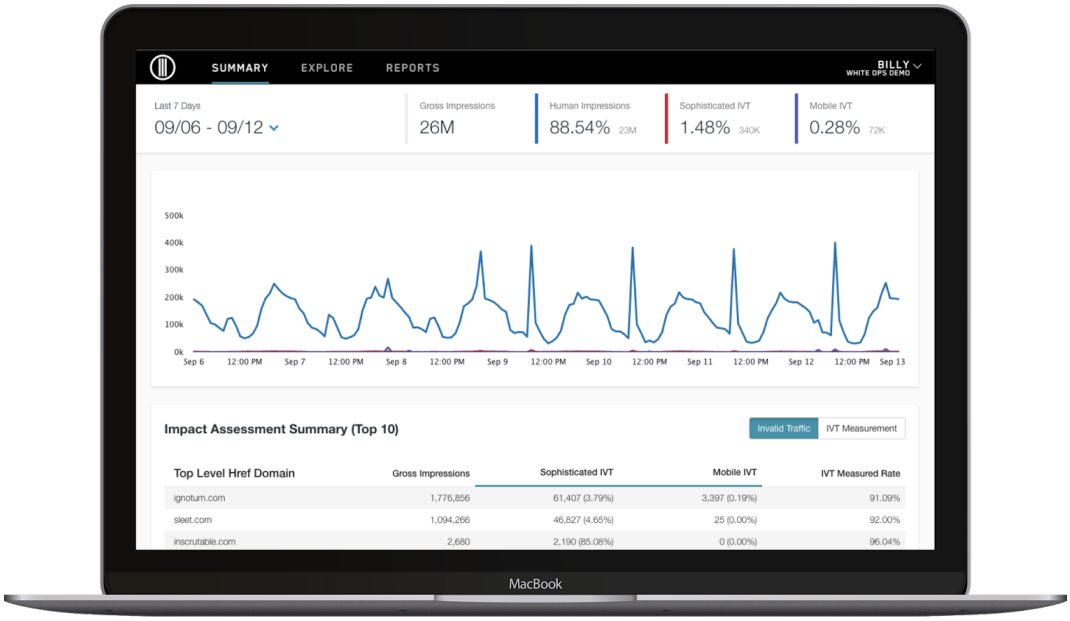
Proactive blacklisting with transaction-level data

Concerned about the impact non-human traffic was having on the effectiveness of marketing spend, the company began using FraudSensor. They placed the JavaScript tag on all campaigns and began developing an understanding of the sources of the most fraudulent traffic. Because White Ops tracks transaction-level details, it was easy for the company to find which campaigns, providers, and sources most contributed to the reported SIVT.

Through weekly hotspot analyses — investigations that analyze the impression data in progressively more detailed ways — White Ops was able to uncover the different sources of the fraud. As these sources were identified and the domains were blacklisted, the rate of non-human traffic fell below 2%.

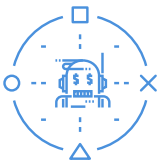
WHITE OPS FRAUDSENSOR

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