White Ops

CASE STUDY

Fraud rates fall 59% after leading beverage company implements White Ops

INDUSTRY

Food & beverage

CHALLENGES

- Suspicions that campaigns were being undermined by fraudulent traffic
- Agency was content with conventional fraud detection technology

WHITE OPS PRODUCT

FraudSensor

KEY BENEFITS

- White Ops identified nearly 5% non-human traffic in campaigns
- Reduced the instance of fraudulent traffic to sub-2%

SUMMARY

A major beverage company had concerns about its new agency's ability to detect and prevent ad fraud. Despite reassurances from the agency, the company partnered with White Ops to investigate. White Ops found fraud rates nearing 5%.

BEFORE WHITE OPS

A multi-national beverage company had recently hired a new agency to manage its digital advertising. The agency boasted that it had solutions in place to protect against ad fraud. However, the beverage company had already been burned by non-human traffic in the past and didn't want to make the same mistake twice.

As it turns out, the agency used a very basic and conventional solution to detect ad fraud. Uncertain that this solution would provide the adequate level of defense against sophisticated cybercriminals, the company came to White Ops to do a discrete investigation.

AFTER WHITE OPS

Using FraudSensor, the post-bid detection software, White Ops and the beverage company conducted hotspot analyses – a series of investigations that analyze the data in progressively more detailed ways – to identify the potential sources of non-human traffic. It turns out the concerns of the beverage company were justified: fraud rates were nearly 5%.

Armed with the exact sources of fraud, the beverage company was easily able to blacklist the malicious domains and reduce fraud rates to below 2%. The 59% reduction in ad fraud has ensured the beverage company is getting the most out of its digital ad spend.

Note: As a security company, White Ops understands that our customers may not wish to publicly state the solutions they are using. To that end, we have removed client name and identifying information from this case study.

About White Ops

White Ops protects the Internet from automated threats: threats such as ad fraud and account takeovers conducted by malicious bots. The biggest and smartest Internet companies in the world rely on White Ops to detect and prevent automated threats that causes billions in damages annually. The company's Human Verification technology prevents automated threats by combating their root cause: the malicious software behind bots, ad fraud, and app fraud. Even when bots use sophisticated techniques like exploiting real people's devices, compromising human identity, or simulating human behavior, White Ops stops these bots with precision and reliability.

New York, NY
whiteops.com
sales@whiteops.com