WhiteOps

CASE STUDY

Leading insurance company finds 31% non-human traffic in campaign

INDUSTRY

Insurance

CHALLENGES

- Targeted audience segments were exhibiting high rates of fraudulent traffic
- Budget spent on these expensive CPMs were lost to botty traffic

WHITE OPS PRODUCT

FraudSensor

KEY BENEFITS

- Reduced non-human traffic from key publisher by 93%
- Increased efficacy of advertising spend

SUMMARY

A leading insurance provider learned that some of its campaigns were drawing 370% more non-human traffic than the others. With help from White Ops, the insurance company was able to identify the main source of non-human traffic and bring it down to ~1%.

BEFORE WHITE OPS

During a regular campaign audit with White Ops, a leading insurance provider realized that a small number of campaigns were drawing an alarmingly high rate of fraudulent traffic. All of the campaigns shared one thing: a Hispanic audience segment. These campaigns saw 31% non-human traffic – a rate that was 370% higher than other campaigns.

White Ops and the insurance company began investigating the sources of the fraud. Using FraudSensor, the teams were able to identify that most of the non-human traffic was coming from a select few areas.

AFTER WHITE OPS

Armed with this information, the insurance company and its agency reached out the one publisher that was sending the most non-human traffic. Despite being a well-known publisher, its traffic was more than 15% non-human. The publisher was able to resolve the issue, and now traffic from the publisher is ~1% non-human.

The 93% reduction in non-human traffic from the main publisher has improved the efficacy of the insurance company's advertisements. The high-quality traffic now delivered from the publisher suggest that the root of the non-human traffic was effectively neutralized.

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