CASE STUDY

# Fraud missed by conventional solution costs insurance company big time

## INDUSTRY

Insurance

## CHALLENGES

- Conventional fraud detection software was missing non-human traffic
- This fraud was costing $35-50k per month

## WHITE OPS PRODUCT

FraudSensor

## KEY BENEFITS

- Confirmed suspicions about fraudulent traffic
- Identified sources of non-human traffic
- Expected to save $35-50k per month that was previously lost to ad fraud


## SUMMARY

A leading insurance provider was told by its current detection software that there were very low rates of non-human traffic in its campaigns. But, suspicious activities on landing pages gave the insurer some pause, so it came to White Ops.


## BEFORE WHITE OPS

A leading insurance provider observed some odd analytics on its landing pages. When the team looked at the bounce rates through Google Analytics, they realized that a significant portion of the users were exhibiting anomalous behavior.

These findings were particularly disheartening because the company already had ad fraud prevention in place. Despite the bizarre behavior, the detection provider maintained that these were valid impressions. The insurance company was not sure and enlisted White Ops to investigate.

## AFTER WHITE OPS

White Ops began monitoring the media and discovered nearly 4% non-human traffic. The fraud was coming from a variety of sources, including some “premium” publishers with expensive CPMs. All told, this fraud was costing the insurance provider between $35-50k per month.

The company has begun an aggressive plan of blacklisting suspicious publishers and seeking remediation for other lost spend. Human Verified Audiences and anti-targeting are also being utilized to mitigate fraud risk. The insurance provider now has complete confidence in its ad fraud protection, and is saving $35-50k per month they were previously losing.

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