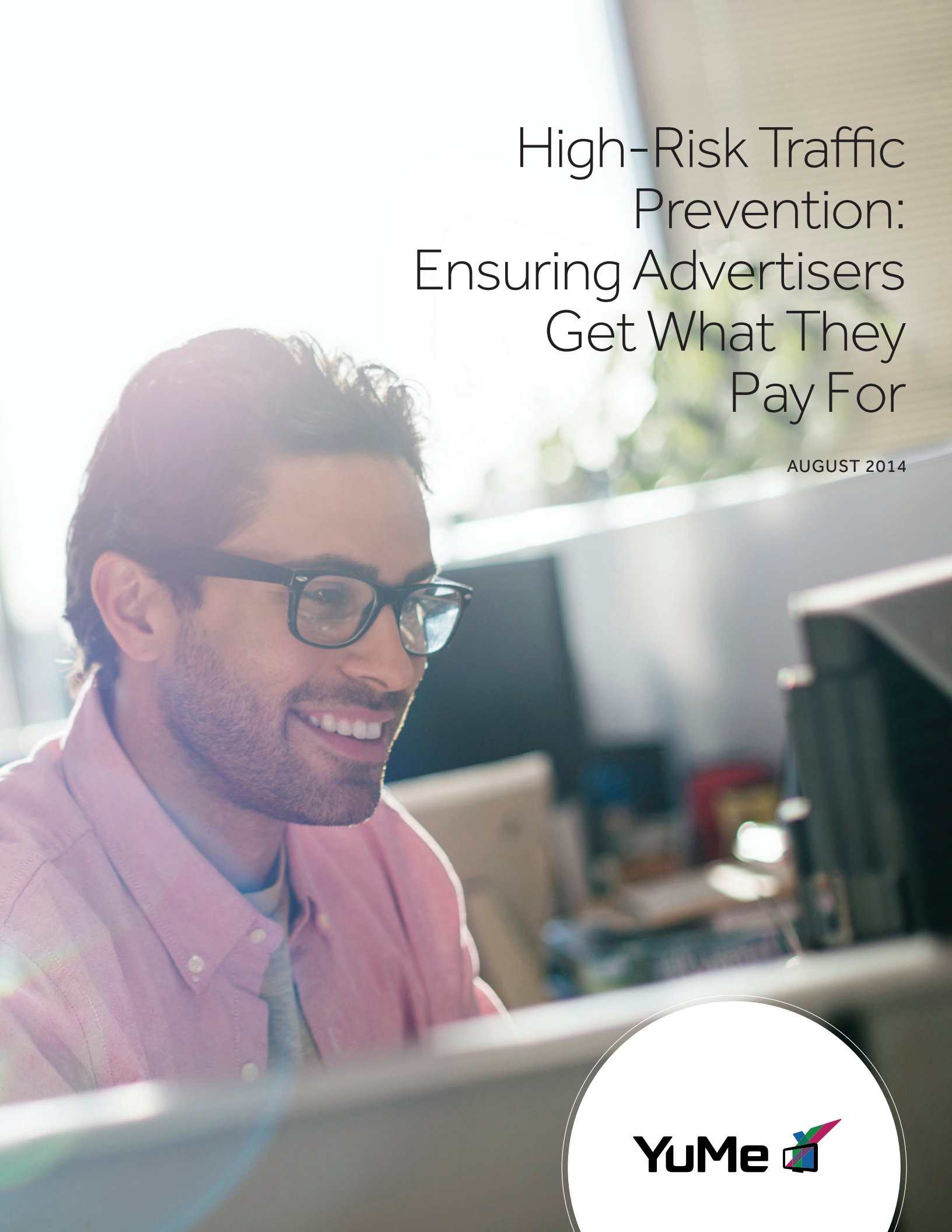
High-Risk Traffic Prevention: Ensuring Advertisers Get What They Pay For

AUGUST 2014



YuMe

A HIGHER LEVEL OF TRAFFIC QUALITY

The advertiser is the most important constituent in the ecosystem, a fact that is often overlooked in a business so highly dependent on technology and data. The foremost objective of the digital advertising ecosystem, therefore, is to ensure that advertisers get what they pay for. In order to accomplish this goal, an impression must be visible to human consumers. However, bot traffic and malicious invalid traffic schemes complicate this basic tenet.

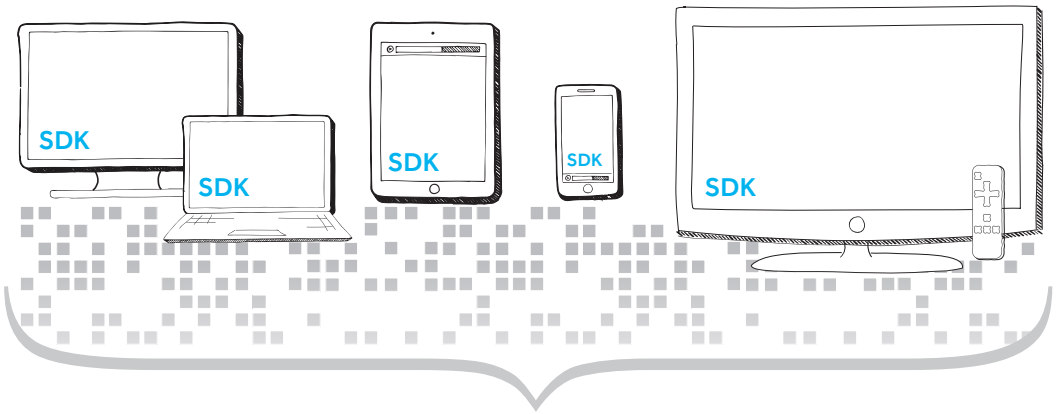
Companies that have taken the role as aggregators of media must take responsibility for identifying and exorcizing as much bot and suspicious activity as possible. YuMe's position is that there can be no passing the buck. That's why our Traffic Quality Lab is responsible for gathering intelligence from various channels to advance YuMe's high-risk traffic fighting methods, to benefit our advertisers, and to share information with partners and even competitors willing to work together towards the common goal eliminating non-human activity from the ecosystem.

INNOVATIVE AND SCIENTIFIC APPROACH TO FIGHTING INVALID TRAFFIC

DATA + SCIENCE

Designed by individuals who think out of the box, digital ad high-risk traffic takes many forms, driven by some of the most advanced technology available. Because high-risk traffic is asymmetrical warfare, trying to combat non-human activity using a traditional engineering approach will only identify a subset of total suspicious traffic in the system. Unfortunately, third-party vendors continue to take this approach. With most having started in the brand safety and verification business, they are adapting their technologies to sniff out bot traffic and are selling advertisers on the efficacy of their shortsighted, reactive method.

At YuMe, data and innovation are at our core, so it makes sense that our approach to detecting and blocking suspicious traffic evolves as creatively and thoroughly as our video advertising products. Data science leads the way, using heuristic analysis to monitor hundreds of data signals, any of which may represent a vanguard to an emerging invalid traffic scheme. As such, technology must be in place to capture not only data across sight, sound and motion but also additional signals that, if triggered, could alert YuMe to the existence of zero-day non-human activity models – schemes that haven't yet surfaced in scale across the ecosystem.

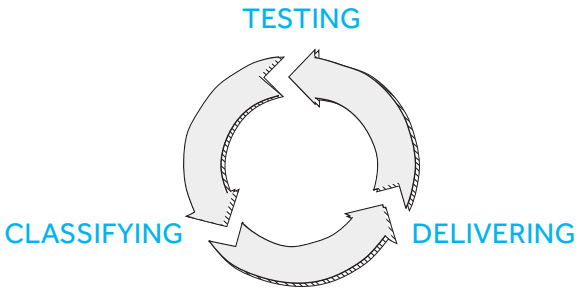


SDKS COLLECT DETAILED INFORMATION ABOUT IN-PAGE ENVIRONMENT THAT FEEDS INTO YUME'S HIGH-RISK TRAFFIC-DETECTION ALGORITHM

MULTI-SCREEN SDKS

Access to the right data is crucial. Our multi-screen Software Development Kits (SDKs) across online, mobile, tablet and connected TVs are uniquely integrated into the video player, so they go wherever the player is being viewed. This enables us to collect detailed information about the in-page environment of a publisher's player, regardless of whether it has been syndicated to a partner website, shared through social networks or embedded on another site – providing billions of data points that inform our proprietary technology.

Data streaming from the rich data pipes connects to video advertisers by way of the YuMe SDK feed, our suspicious traffic-detection algorithm, to continually qualify our multi-screen inventory in real-time. Reported signals are then used to identify trends and build models to make predictions on how future instances of invalid traffic could manifest on the network. This continual ecosystem of testing, classifying and delivering impressions is powered by data science.

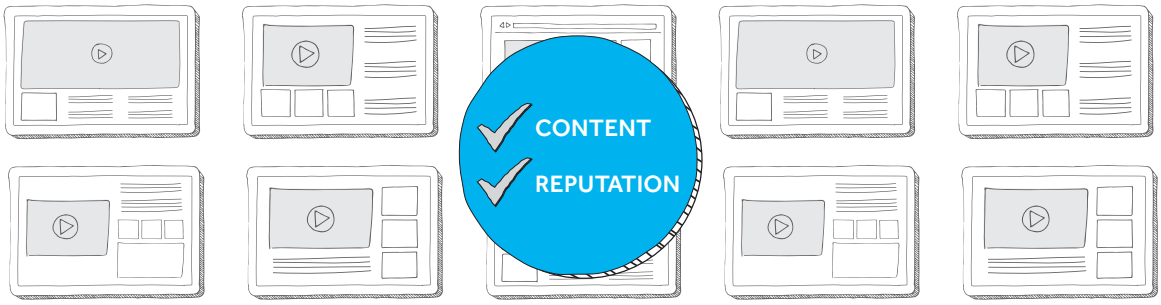


FORENSIC INVESTIGATION AND SUSPICIOUS TRAFFIC SCHEME IDENTIFICATION

Just as important as the data collection, forensic investigation expertise is required to interpret statistical variances in these signals and determine if the shift is explainable by organic reasons or if invalid traffic has entered the network. The result of a forensic investigation is a propensity of traffic packet-level evidence to conclusively point to a party enabling the suspicious activity. The Traffic Quality Lab partners with our legal team to review the evidence and recommend appropriate action, which may include terminating the relationship with a publisher and pursuing legal action to recover damages.

PREVENTING NON-HUMAN ACTIVITY FROM ENTERING THE ECOSYSTEM

In addition to monitoring hundreds of data signals for evidence of bot and non-human activity, it's important to ensure that new publishers entering the YuMe network are thoroughly reviewed for both content and reputation. The best high-risk traffic prevention technology results in barely treading water above a bot- and non-human activity-infested network unless publishers and sites that encourage malevolent behavior are stopped. YuMe accomplishes this by using a multi-dimensional review process supported by a combination of proprietary and readily available tools.



CONTENT REVIEW

Though many ad networks review publishers for content to make sure there are no offensive sites entering the network, YuMe takes this review one step further to increase the opportunity for advertisers to get what they pay for. For example, YuMe ensures that, when videos ads play on a screen, the user is not distracted by other video ads or extensive display ad clutter, ensuring that the user is given the best environment to consume the ad.

REPUTATION REVIEW

The individuals responsible for non-human activity understand that clean, well-designed websites can blind many ad networks to the fact that these sites have been created solely to drive bot traffic to view video ads. That's why YuMe uses several tools to look beyond content and make a determination on the likely quality of the sites' traffic. Sites identified as representing a high existential risk to the integrity of the network are rejected.

FIGHTING INVALID TRAFFIC HAS NO FINISH LINE

The individuals behind invalid traffic are motivated by two desires: to hack and to steal. It's that simple and they don't stop doing either. Ultimately, there is no goal line. Those behind high-risk traffic hack and steal practices continue to be perpetrators while the quality traffic advocates respond.

YuMe is committed to protecting its advertisers and engaging the individuals behind high-risk traffic. To accomplish this, we're building a high-risk traffic prevention program based on technology, data and forensics, using expertise from sources ranging from PhDs to white hat hackers to stay ahead of the non-human activity threats and identify harmful behavior in the network.

To learn more about YuMe's Traffic Quality Lab, drop us a line at yume_info@yume.com.