White Ops for Connected TV Devices, Services, and Platforms

White Ops®

Introduction

It seems like every other week, there's another new streaming service announcement. After the runaway success of Netflix, Amazon, and Hulu, challengers and new players have started to surface: Disney's streaming service launches in 2019. CNN and NBC have announced new services designed to appeal to younger viewers. And all of these services will have new advertising mechanisms built in.

Every month, White Ops has visibility into more than 100 billion CTV bid opportunities.

The global connected TV (CTV) and over-the-top (OTT) markets will climb to over $120 billion by 2023[1]. With a market penetration of 60% of American households[2] by 2022, the opportunity for advertisers is enormous—and since the time that viewers will spend watching CTV content will increase, the amount of available advertising inventory will increase. And in the last three years alone, the proportion of video ads viewed on CTV has nearly tripled[3]. According to PwC's Global Media and Entertainment Outlook findings, advertisers will spend more than half of their budgets on digital advertising by 2023[4]. But with an increase in advertising spend comes attention from fraudsters interested in stealing a piece of that pie.

CTV provides a much more targeted advertising ecosystem than traditional, "linear" television—advertisers aren't working off of an old-fashioned "shotgun" approach, but can tailor their campaigns based on the perceived interests of the viewer. This shouldn't, however, be interpreted as, "CTV is the cure to addressability challenges": those challenges morph but still exist in CTV settings. For example, without cookies, it can be hard for an advertiser to attribute a buying decision to a particular CTV campaign.

Additionally, viewers tend to be more tolerant of advertising in CTV settings; it's seen as the cost of business for cutting the cord or operating in a platform other than the traditional broadcast/cable system.

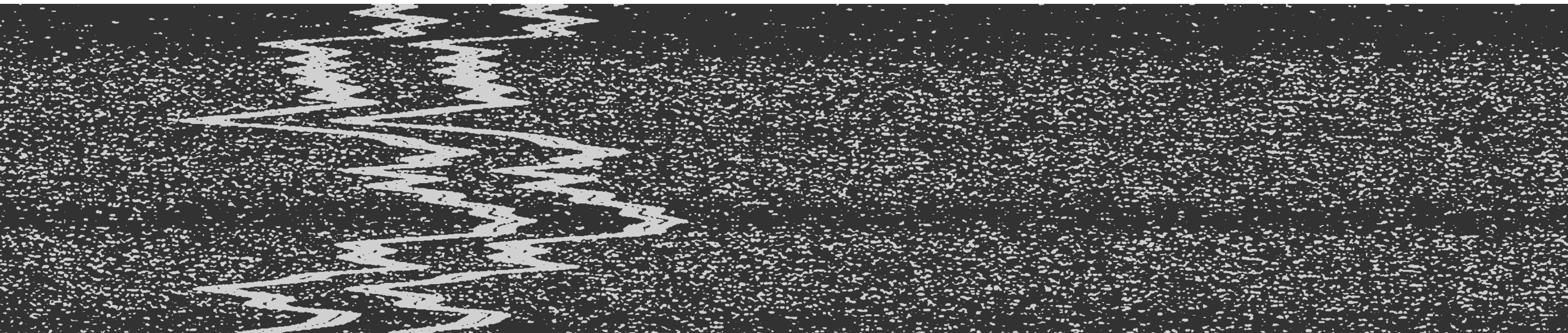
White Ops is leading the fight to protect the CTV advertising ecosystem, from the advertisers and publishers to the DSPs and SSPs that facilitate impressions. This effort ensures that ads are seen by the audience that the advertiser intended and that money spent in this expanding market goes to the people who rightfully earned it. This also safeguards the devices on which users are viewing the new wave of OTT content. White Ops' aim is to lead the market in bot fraud mitigation by ensuring trust in the online advertising marketplace by verifying the humanity of every interaction.

[1] Digital TV Research.

[2] eMarketer.

[3] ExtremeReach, "Video Benchmarks 2018".

[4] pwc Global Media and Entertainment Outlook, 2019.



What are CTV and OTT?

With a new market, naturally, comes a new series of terms that need defining. Many familiar name brands fit into the connected TV and over-the-top categories, but it's useful to know how the buckets are defined to have a meaningful understanding of how advertising works within the ecosystem.

Connected TV (CTV): A CTV is any television that's hooked up to the internet, either directly, through its own hardware or software (i.e. smart TVs) or through third-party devices (i.e. Roku or Fire Stick devices).

Over-the-top (OTT): OTT services are the (generally streaming) platforms that deliver the content through the internet connection. (i.e. Netflix, Hulu, specific channels on the Roku device) "Over-the-top" refers to the service being above and beyond the scope of cable television services.

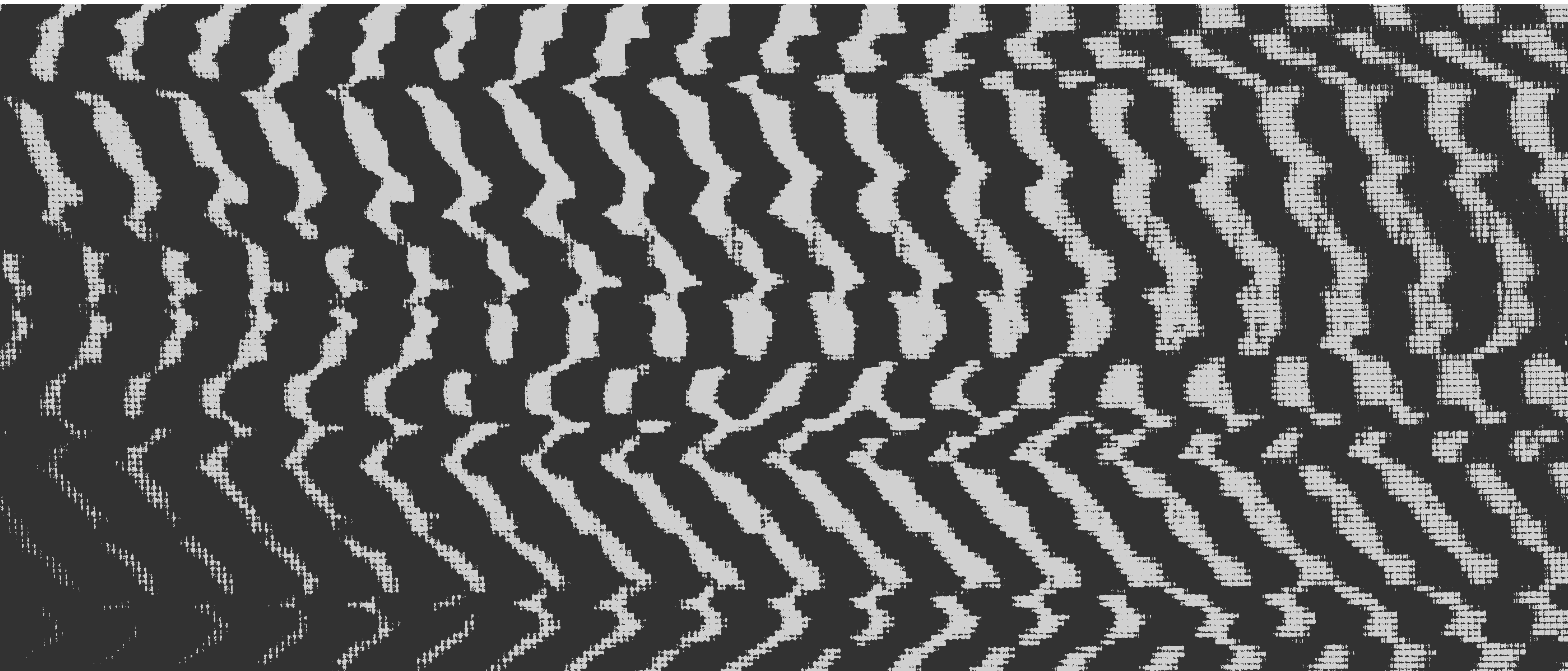
For simplicity's sake in this examination, we're going to refer to CTV to represent the broader CTV/OTT ecosystem.

Those familiar names are a big part of why the CTV market has grown dramatically over the past several years, and why CTV will be a $120 billion industry before the end of 2023. Freewheel reported that 91% of media buyers anticipate linear TV and CTV purchasing to converge by 2021, a clear indication of the prominence CTV will hold in the immediate future[5].

Today, over 75% of bot activity comes from residential machines.

The White Ops platform, too, has seen a spike in the number of CTV-based bid opportunities. Between Q1 of 2018 and Q1 of 2019, the CTV footprint has jumped 1,300%, with a further rise expected. (For context, White Ops currently observes more than 100 billion CTV-based bid opportunities per month.)

[5] Freewheel, Video Marketplace Report.



How does advertising work in CTV?

Media buyers have some options when it comes to working within the CTV ecosystem, and that's in large part due to the speed with which it developed. There's no one app store that grants you access to a broad variety of platforms, nor is there a single protocol that's in place across all platforms and providers. It can be a challenge for media buyers to know what every platform's rules and regulations are, not to mention which platforms are trustworthy and which ones should be avoided.

But in general, buyers work with CTV device manufacturers directly and with the service providers who offer the content. Consider for example, an advertiser who places a static ad on the home page of Roku's platform, as well as a mid-roll video ad within a Hulu show. In order to fully capture audiences, buyers need to consider all of the places that the consumers' eyeballs will land in their CTV experience.

> **According to PwC's Global Media and Entertainment Outlook findings, advertisers will spend more than half of their budgets on digital advertising by 2023.**

Content publishers (think Hulu) often reserve a portion of their ad inventory for direct sales, rather than offering the entirety of that inventory through SSPs. It's for this reason that advertisers work across the entire CTV ecosystem, partnering with DSPs and SSPs but also directly with the content publishers and the device manufacturers.

What are the challenges with working in CTV?

As mentioned above, media buyers looking to connect with CTV consumers face challenges in their work. Without a single clearinghouse like the Google Play Store or Apple's App Store to work from, it's a bit of a Wild West atmosphere with every provider operating with their own terms. Advertisers are expected (forced, really) to learn the system across a wide variety of providers in order to get the market penetration they're hoping for.

Additionally, there's no single standardized protocol for ads within the ecosystem. Some inventory in some platforms may not be adequately tagged and referenced as being CTV-based, which may cause reporting difficulties on the other end. And video ad providers may or may not have adopted the latest VAST version to support those ads, causing compatibility and fraud issues.

Device impersonation is the most common type of fraud found on CTV platforms today.

SSAI (server-side ad insertion) is the process of the ad server connecting the advertisement and the actual content into a single delivered video, creating a seamless experience for the user. SSAI circumvents some common issues for users of OTT content, including latency and ad-blockers. For verification vendors in server-to-server tracking scenarios, it can be problematic: all of the tracking is coming from a single IP address. To an ad server receiving tracking information, the reports look similar to fraud. This allows for a threat model in which the SSAI servers can themselves be spoofed.

CTV is especially attractive for fraudsters given the enormous growth of the market in recent years (and the expected further expansion). CTV platforms and OTT services can command substantial CPMs with that audience size, market penetration, and exclusive content offerings. There are several types of fraud that can present themselves in the CTV ecosystem, and it's important to have an understanding of each:

Device impersonation: Fraudsters can command bots to send fake user agent IDs to ad servers pretending to be legitimate devices. White Ops can spot these fake IDs as belonging to IP addresses that don't belong to CTV devices, making it clear that impressions are being delivered to something other than what the advertiser intends to send them to. Device counterfeiting is one of the most prominent types of CTV fraud today, and resembles a fraud tactic commonly used on mobile devices.

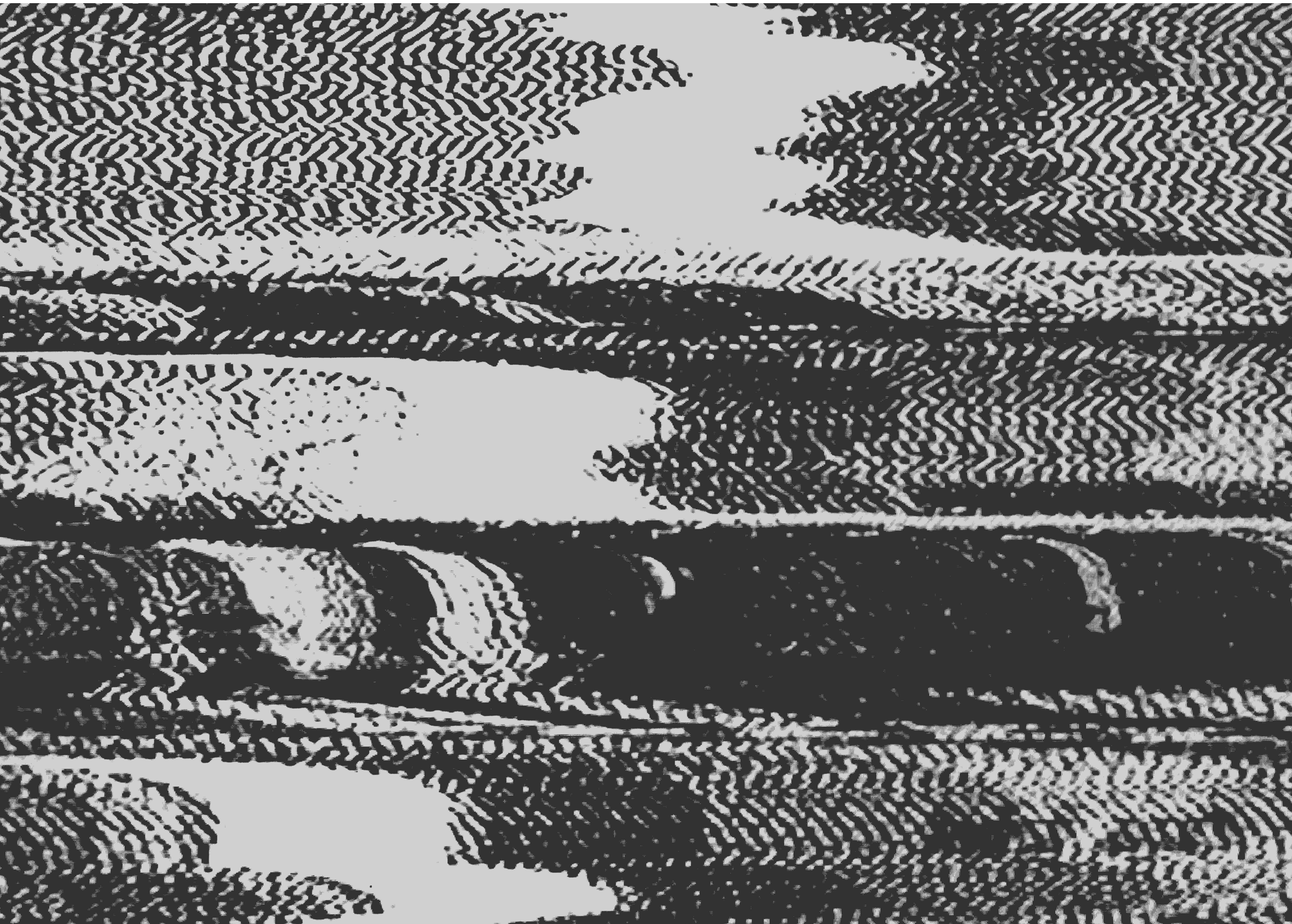
App spoofing: This particular type of fraud is when an app sends fake information—such as the app/bundle ID—to the ad server, resulting in an ad being delivered to a different app than the one the advertiser intends to send it to.

Device farms: Scan through certain corners of Reddit and you can find low-level fraudsters bragging about the mobile device "farms" they've built to steal from advertisers through automated browsing. With the rise of CTV, those farms may start to shift toward the new market; it may even be easier with CTV than with mobile, since there's no expectation that a CTV device is intended to be anything but stationary.

Background/hidden ads: Have you ever visited a website that popped a webpage up behind the active browser you were using? Those pop-unders, as often as not, are full of ads. CTV fraudsters can do something similar: apps on CTV platforms ask for (and receive) permission to run in the background or when inactive and display ads that the user can't even physically see. Apps can also request ads that are designed to be hidden from the user, not just behind the active window.

Incentivized ads: There are some early signs of publishers showing ads in an incentivized model, too. For example, a user may sit through an ad simply to get an incentive promised by the publisher, like a gift card or cash.

SSAI spoofing: With the advent of SSAI, fraudsters have sought out and found ways to beat the new system. Many providers simply whitelist SSAI IP addresses to avoid false positives with security systems, and fraudsters can hide behind those whitelists. Fraudsters can also deploy machines that mimic the proxy servers that handle SSAI processing for some providers, allowing them to sneak into the supply chain.



IV What can the advertising ecosystem do to minimize the impact of fraud through CTV advertising?

The rise of CTV doesn't have to correlate to a rise in CTV ad fraud. Advertisers can protect themselves by taking a series of concrete steps to ensure that their exposure is minimal and that their spend is directed where it's intended.

1. **Choose your partners carefully.**
   Not all platforms and services are created equal. Buyers should thoroughly investigate the companies with which they want to do business. New inventory should be inspected closely to ensure it's what was promised.

   Every player in the CTV ecosystem should be well-educated on (and, ideally, participating in) the app-ads.txt initiative. app-ads.txt is an extension of the original ads.txt; it's a mechanism for publishers to declare who can sell their ad space. Buyers can ensure through app-ads.txt that they're working with authorized sellers. Participation in the app-ads.txt initiative should be, for advertisers, the bare minimum criteria for publishers.

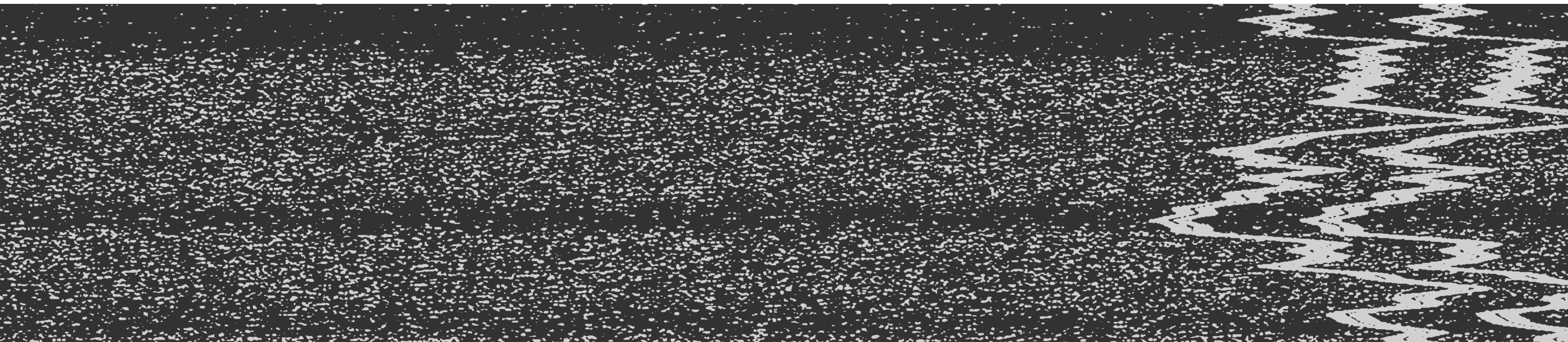
   Additionally, advertisers would be well-served to audit their CTV ad inventory regularly and frequently to ensure that the inventory remains as clean as it was on the first day of the engagement.

2. **Collaborate with industry groups.**
   Organizations like the IAB and the ANA advocate on behalf of advertisers to ensure that the advertising ecosystem is constantly moving forward technologically. Active participation in industry organizations is a crucial way to stay on the forefront of new developments in the ongoing fight against ad fraud.

   For example, the IAB is developing new standards for the CTV ecosystem (such as the Identifier for Advertising [IFA] standard) to reduce fraud through user agents, app IDs, and other spoofable identifiers. Industry group participants can contribute to the development process for projects like IFA to get them over the finish line sooner.

3. **Talk about successes and failures.**
   Being a victim of ad fraud can't be a dirty little secret that every advertiser has but declines to discuss. The only way that we can, as an industry, move past these challenges is to discuss them openly and strategize collectively about how to beat back the fraudsters.

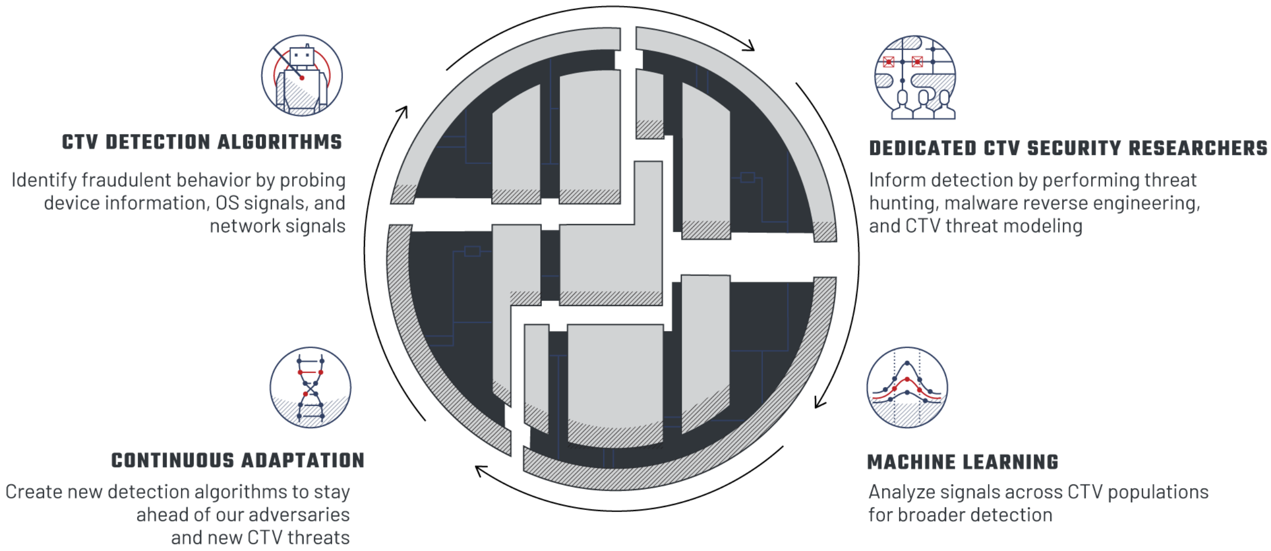
   Word of mouth can also be a helpful tool in identifying who the reputable publishers are, ensuring that only the well-behaved publishers see business from advertisers.



V The White Ops Approach

How White Ops detects and prevents CTV ad fraud

Invalid traffic generated by today's sophisticated bots requires advanced detection techniques. Today, over 75% of bot activity comes from residential machines. This new real estate allows bots to closely mimic human behavior, rendering traditional methods that focus on identifying non-human behavior less effective.



CTV DETECTION ALGORITHMS

Identify fraudulent behavior by probing device information, OS signals, and network signals

DEDICATED CTV SECURITY RESEARCHERS

Inform detection by performing threat hunting, malware reverse engineering, and CTV threat modeling

MACHINE LEARNING

Analyze signals across CTV populations for broader detection

CONTINUOUS ADAPTATION

Create new detection algorithms to stay ahead of our adversaries and new CTV threats

White Ops uses a multilayered approach for all environments—including CTV—that allows us to detect and prevent invalid traffic with unprecedented accuracy, without compromising anyone's viewing experience. This approach consists of:

Technical Evidence: We probe the various CTV devices to gather hundreds of data points on the network, device, software, application, and user configuration to detect technical evidence of compromise.

Machine Learning: We analyze thousands of data points collected across trillions of transactions to predict malicious behavior, enabling us to provide a high level of accuracy, even when there is insufficient technical evidence.

Global Threat Intelligence: White Ops Threat Intelligence analysts proactively hunt for new threats on the Internet, attributing threats to specific botnet operators, campaigns, and feeding findings back into detection algorithms.

Continuous Adaptation: White Ops has continuously adapted over the last 7+ years, creating thousands of markers and hundreds of algorithms. Our speed to identify and build new detection mechanisms means we stay ahead of the adversary more than other solutions that are built on fixed detection mechanisms.

In addition to these approaches, White Ops employs the following techniques to make it difficult for adversaries to reverse our technology, or know if they've been identified:

- **Adaptable, polymorphic challenges:** the way we probe a device changes on an hourly basis, making it difficult for adversaries to evade or reverse engineer our detection
- **Slow feedback loops:** we withhold feedback so adversaries don't know whether or not they've been detected

Our Approach to Detecting Invalid Traffic on CTV

A lack of industry standards on devices, apps, and ads require innovative detection approaches to identify fraud. Instead of applying a blanket approach to detecting fraud, White Ops has a team of dedicated CTV security researchers who create specific algorithms for various CTV device types and platforms. These algorithms identify device, OS, and network level characteristics (among others) that give us visibility into fraudulent activity, even with a lack of industry standards.

Every month, White Ops has visibility into more than 100 billion CTV bid opportunities. We've got insight into where fraud is coming from, whom it's targeting, and how it's being carried out. And with every passing month, that insight grows deeper. The most important part of any stakeout is the intelligence gathering, and White Ops is uniquely positioned to collect information about CTV fraud to protect advertisers and publishers.

How White Ops serves the industry

Publishers

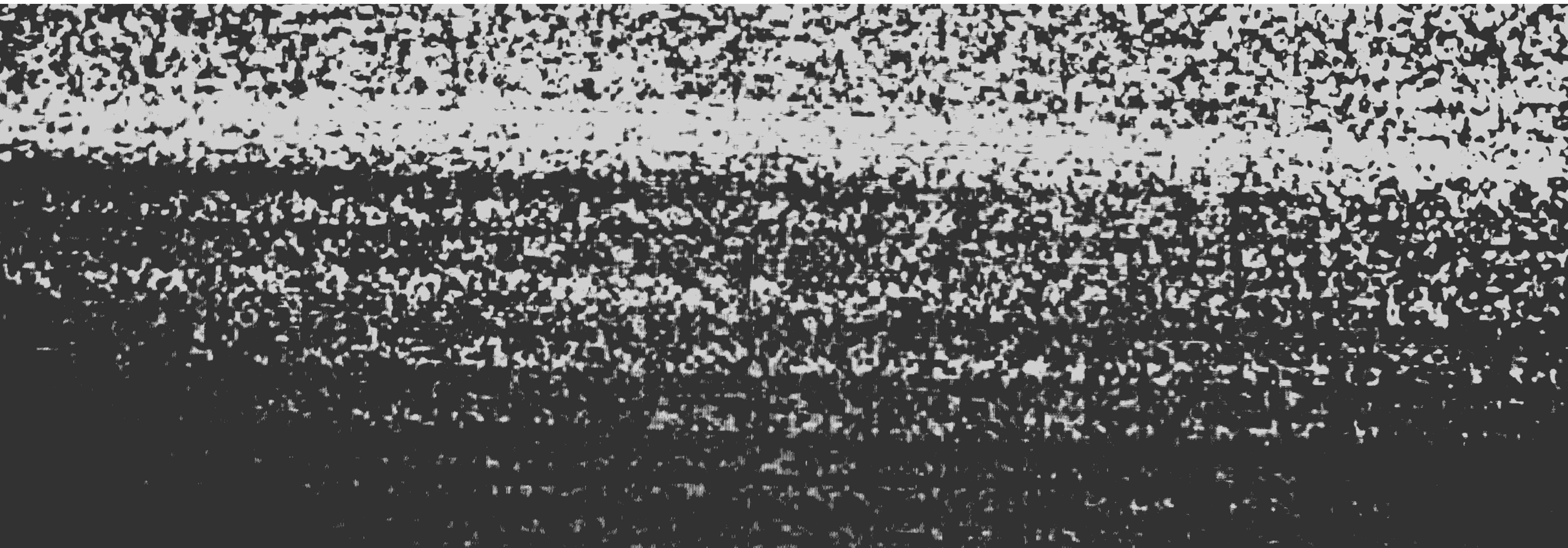
Offer clean, premium inventory to advertisers at higher CPMs.

Ad Tech Platforms

Maintain high CPMs and reduce clawbacks.

Advertisers

Increase the ROI of your CTV spend by working with reputable publishers.



Conclusion

The CTV market has exploded in the last several years, and there are no signs that it's going to slow down anytime soon. And with new eyeballs and new channels every week, there are new opportunities for fraudsters to try to steal a piece of the billions of dollars spent.

White Ops is working diligently to protect the CTV ecosystem, from ongoing research and intelligence to new signal creation and industry partnerships. White Ops is building trust throughout the marketplace and establishing that there are ways to protect advertisers and publishers.

To learn more about White Ops for CTV devices, platforms, and services, contact our team to learn more.