

Combating Ad Fraud: A Review of Status Quo, Existing Vendors and Future Challenges

Business Intelligence Group

Advised by Prof. Yoo-Seong Song

Dec 04, 2020

Meet the team



Deepika Kochhar
Senior Manager

Information Management



Gaganpreet Baansal
Project Manager

Information Management



Akanksha Shetty
Senior Consultant

Information Management



Claire Ke
Consultant

Advertising



Megha Manglani
Consultant

Information Management



Zizhou Sang
Consultant

Information Management



Jane Xuan
Consultant

Advertising

Contents

1

Market Research for Ad Fraud Industry

2

Vendor Assessment Metrics

3

Research on Ad Fraud Solutions

4

Research on Ad Fraud Solution Providers

5

Mid-Term Summary of Vendor Assessment

6

Research on Ad Fraud Challenges and Events

Market Research for Ad Fraud Industry

Chapter 01

Agenda

1

Introduction of Ad Fraud

2

Effects of Ad Fraud and prevention techniques

3

Various software providing solutions for Ad Fraud

The rise of online advertisements and its malicious exploitation through perpetrators

What is an Ad Fraud?

A type of invalid traffic generated intentionally to increase their own profits at the cost of other members and that does not represent the legitimate ad traffic that should be included in measurement data.

Invalid Traffic (IVT)

Most of the ad fraud occurs because nonhuman traffic receives the ad promotions, but actual humans never see the ads targeted for them. This is termed as invalid traffic.

Types of invalid traffic



Traditional Bots

Browser Hijacks

Ad Injectors

Domain Laundering

Negative Impacts of IVT on media buyers



Wasted ad spending

Lack of transparency

Missed opportunities to create impacts

Reduced ROI

Negative Impacts of IVT on media sellers



Lack of trust in the value of their inventory

Damage to their relationships with buyers

Loss of revenue to long-tail sites

Failure to fetch response from client data

With the growth in online advertising, cyber criminals have infiltrated the ad industry by several fraudulent practices that have adverse effects on the entire digital ecosystem

Segregating the types of ad frauds and evaluating its negative effects on organizations

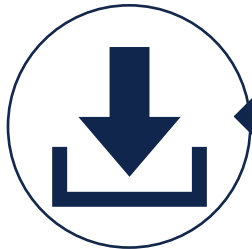
Types of Advertisement Frauds



Impression Fraud:
Results from HTTP requests that users never see



Click Fraud:
Occurs when sources other than legitimate users are making HTTP requests



Conversion Fraud:
Occurs when HTTP requests are issued with the intent of artificially producing conversions

Increased spending on online ads

Recent data indicates marketers have wasted between **\$6.5B - \$19B** due to ad fraud

Tremendous negative impact on brand value

Impossible to reach targeted customers thus decreasing the brand reputation

Promoting the demand for AdBlockers

Acute reach problem for advertisers since nearly **20% of millennials** between the **ages of 18 and 24** use ad blockers.

Infected demographic reporting

Inaccurate demographic composition leading to wrong conclusions and **poor optimization decisions**

Impacts of Ad frauds on companies

Irrespective of the type of ad scam, they always impact organizations negatively, affecting a range factors like revenue, brand image, online reach, campaign effectiveness and audience count

Piracy and ad fraud are affecting the ad industry in many negative aspects

Piracy in Ad Fraud

Information products (such as music, movies, books and software) are protected by intellectual property (IP) laws. The violation of IP laws is defined as “piracy”. Advertisers are fighting back ad fraud in the way that preventing ads to be shown on top piracy websites, which containing counterfeit products, pirated movies, terrorist groups, or fake news.

Commercial Piracy

- The act of criminal organizations
- Motivation: high profit margins that the large-scale reproduction and distribution of copyrighted products generates
- Ad views make huge profit

End-User Piracy

- The act of individual consumers
- Motivation: low cost of copying, or with a low willingness to pay for quality original products
- Trade-off between “free content” and “viewing ads”

Buyers



Already annoyed by irrelevant and invasive ads, become haplessly complicit in digital ad fraud; they fight back with ad blockers

Advertisers



Wonder how many actual human beings actually see their ads; they grow suspicious of programmatic placements in general (and media agencies that buy them)

Digital Publishers



Even premium ones would lose brand integrity and credibility with skeptical advertisers and, in the process, lose valuable revenue

Detrimental Effects Caused by Piracy and Ad fraud

Eliminating fraudulent digital advertising traffic, combating malware, fighting ad-supported Internet piracy has become new priorities for advertisers

Available ad fraud prevention techniques provide the key to protect your business

Signature-based ad fraud prevention

- Use a special pattern to decipher shady actions, clicks, impressions, or traffic
- Monitor web activity to decide further investigation
- Stop the suspicious activity before it starts
- Save you both time and money

Anomaly-based ad fraud prevention

- Detect anything weird going on with your ad campaign, which includes things like strange ad space placement and mysteriously spiking traffic rates
- Fight against any click-farming facilities or neutering bots

Credential-based ad fraud prevention

- Figure out what kind of fraudulent activities your organization could be hit with before it happens
- Reverse check and crawl through your content and tagging
- Compare your impressions to your trustworthy ranking value. And if things don't add up, it will let you that some sort of fraudulent activities going on

Honey pot-based ad fraud prevention

- Create an extra field on a form that's invisible to users, but since bots aren't aware of this, they'll auto-fill in the field, busting themselves in the process
- Cause a domino effect, triggering the rejection mechanism and preventing any more suspicious bot activity from going down

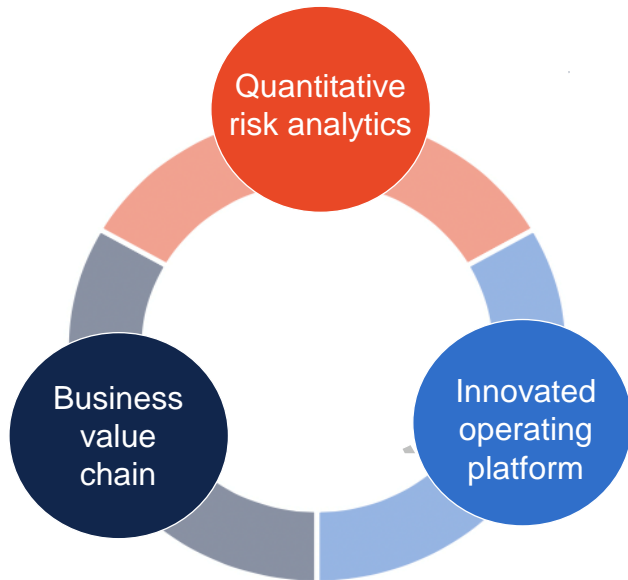


Data offers a clear advantage for advertisers, because it can be used to detect and prevent ad fraud in multiple ways

Cybersecurity operating needs to take actions to become enablers of digitalization.

Problems

- Fundamental tensions arise between the business's need to digitize and the cybersecurity team's responsibility
- Regular cybersecurity operating models which do not operate at "cloud speed"



Using quantitative risk analytics for decision making

- Strengthen their business and technology environments



Building cybersecurity into the business value chain

- Treat cybersecurity as a core feature of product design to establish customer relationships, supplier interactions



Enabling an agile, cloud-based operating platform

- Make technology fast and scalable enough to support an enterprise's digital aspirations

These three actions ensure that new digital platforms to reduce the risk for the enterprise as a whole

The rapid growth of ad fraud makes the scale of the problems become overwhelming

Channels

- Open web programmatic and display
- Paid search
- Paid social
- OTT (Over-The-Top) / CTV (Connected TV)

Forms

- Click fraud
- OTT/ CTV ad fraud
- SIVT (Sophisticated Invalid Traffic)

**\$30
bn**

Advertisers wasted \$30 Billion on ad fraud in 2019

5 x

Ad fraud grew almost 5 times from 2016 to 2019

77%

SIVT makes up 77% of US ad fraud

Ad fraud devastates the industry severely within multiple forms through many channels

Specific software provides advertisers a secure way to avoid ad fraud

	WhiteOps	Moat	IAS (Integral Ad Science)	Double Verify	Cheq	Protected Media	Kochava
Ad fraud	✓	✓	✓	✓	✓	✓	✓
Viewability		✓	✓		✓	✓	
Brand Safety and Suitability		✓	✓	✓	✓	✓	
Conversion rated optimization	✓						✓

Relevant software offers a safe method for advertisers not only to prevent ad fraud but also provide additional service

Vendor Assessment Metrics

Chapter 02

Agenda

1

Various Ad Fraud vendors

2

Metrics for vendor assessment

3

Matrix for vendors and the metrics they fall under

Advertising industry consists of various prominent vendors for ad fraud prevention

CHEQ

 **comscore**

KOCHAVA ★

**PROTECTED
MEDIA**

 **fraudlogix**™

 **pixalate**

 **TRUST METRICS**

FORENSIQ

 **MOAT**

 **DoubleVerify**

 **OXFORD
BIOCHRONOMETRICS**
STOP FRAUD STAY RELEVANT

 **White Ops**®

There are various ad fraud vendors in the advertising market, each having their own capabilities and specializations contributing to their brand value in the market

Specific software provides advertisers a secure way to avoid ad fraud

	WhiteOps	Moat	IAS (Integral Ad Science)	Double Verify	Cheq	Protected Media	Kochava
Ad blocking detection	✓	✓	✓	✓			
Brand Reliability and safety	✓	✓	✓	✓	✓	✓	✓
Reporting and Dashboards	✓	✓	✓	✓			✓

Relevant software offers a safe method for advertisers not only to prevent ad fraud but also provide additional service

Specific software provides advertisers a secure way to avoid ad fraud

	Pixalate	Forensiq	Confiant	FraudLogix	Trust Metrics	ComScore	Oxford BioChrono-metrics
Ad blocking detection	✓	✓	✓	✓			
Brand Reliability and safety	✓	✓	✓	✓	✓	✓	✓
Reporting and Dashboards	✓	✓	✓	✓	✓	✓	

Relevant software offers a safe method for advertisers not only to prevent ad fraud but also provide additional service

Research on Ad Fraud Solutions

Chapter 03

Agenda

1

Effects of Ad Fraud on Ad Industry

2

Existing issues and available solutions for Ad Fraud

3

Identifying major Ad Fraud solution providers

4

Expert reviews on Ad Fraud solutions

Ad fraud is increasingly causing billions of loss for online advertising industry

\$5m

Sophisticated bot operation is ringing up as much as **\$5 million per day** in fraudulent online advertising

\$44b

The global cost of digital ad fraud is expected to reach **\$44 billion by 2022**

\$333b

\$1m

The annual global digital ad spending reached **\$333 billion in 2019**
69% of brands spend **\$1 million per month** reported that at least **20%** of their budgets were being lost to digital ad fraud; **70%** of marketers reported the willingness to increase their budget

Factors preventing marketers from shifting more budget to ad industry:



■ % of respondents, June 2019

Considering the detrimental effects of ad fraud, some marketers are cutting their budget to digital advertising, however, the prospect of the market is still considerable

Multiple types of ad fraud and related problems are identified by industry researchers



Placement Fraud

- modifying publisher pages or the web pages showing on the users' devices to increase impressions or clicks

Stuffing or Stacking

Fake Sites

Domain Spoofing

Ad injection and Malware



Traffic Fraud

- manipulating the network traffic to inflate the number of impressions

Impression Fraud

Click Fraud



Action Fraud

- targeting users' meaningful business actions to re-target valuable customers

Conversion Fraud

Re-targeting Fraud

Affiliate Fraud

Understanding the comprehensive review of ad fraud in categories may help us to further detect and solve related problems

Companies are currently solving ad fraud by various approaches

Unstructured Data Analysis (UDA)

- Predictive models are designed to find intricate **patterns of unusual behavior** to uncover fraudulent schemes
- **Machine learning** techniques are used to adapt to new schemes are being built and put into **detection** and prevention
- **Deep learning solutions** (e.g. facial recognition) combine with biometry data analysis
- *Questions answered are -*
 - *Why does a fraud exist?*
 - *Where is the fraud coming from?*
 - *What are the risks for the organization?*
 - *What should you do to address & prevent fraud?*

White/Blacklisting

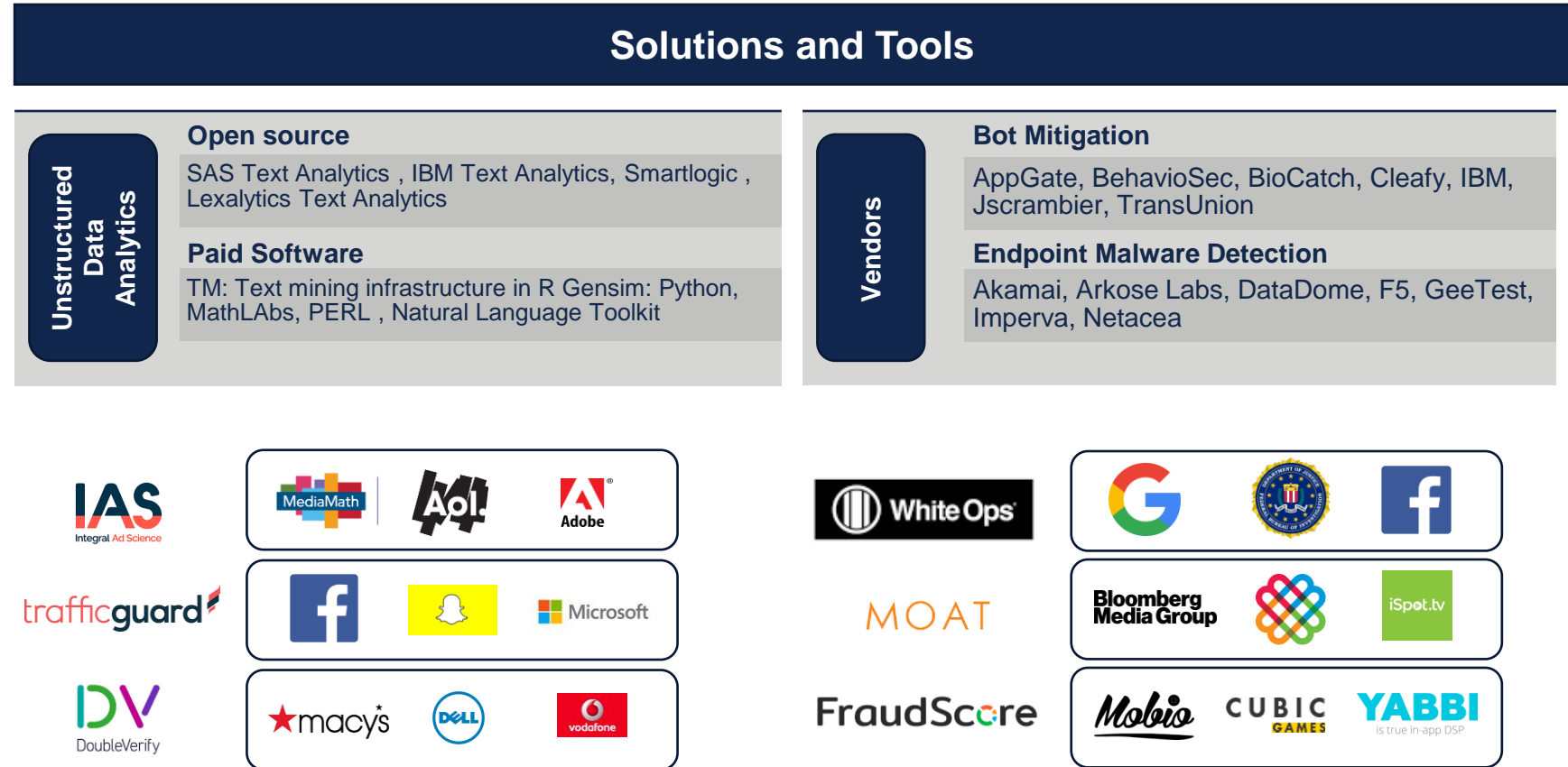
- Add programs such as JavaScript or iframe codes into client computers, then **track the behavior information**
- “Are You A Human” (AYAH) Inc., Once a user’s behavioral data is **verified as a human**, information will be added into a “Verified Human Whitelist” and re-verified from day to day
- Forensiq Inc’s pre-bid fraud detection is based on **impression score** and **IP reputation** to form an evolving intelligence database

Blockchain Technology

- A ledger of records linked cryptographically and shared across a network of computers, design for ad fraud that **not caused by bots** (e.g. millions of mobile impressions caused by rogue flashlight and keyboard apps)
- MetaX, a blockchain startup, has announced adChain Audits, a service that uses machine learning and experts to detect and **block digital advertising fraud**.
- Only **5 percent** of marketers reported current solution show promise, over 40 percent were unaware of it

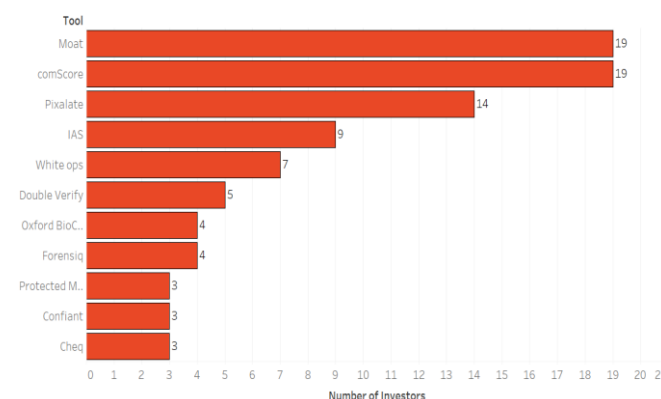
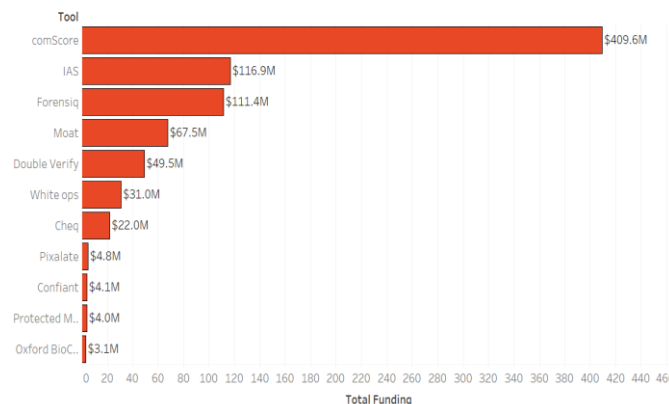
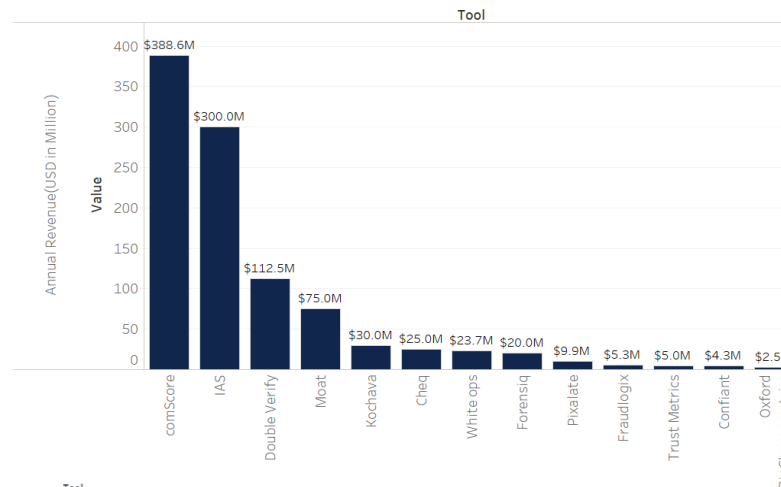
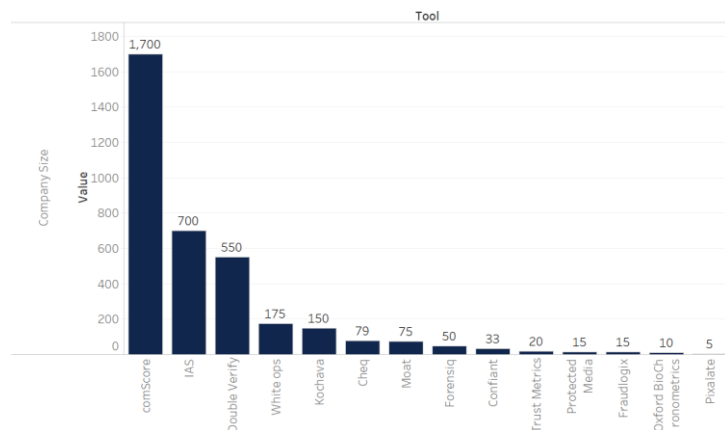
Advanced technologies provide various promising ad fraud solutions for marketers

Ad fraud in-house tools and solutions provide the key to protect your business



Choosing the appropriate ad fraud tool is tricky and comes with challenges however there are various in-house solutions and third-party vendors trying to mitigate this issue

Comscore proves to be the biggest ad fraud solution provider by its current market share

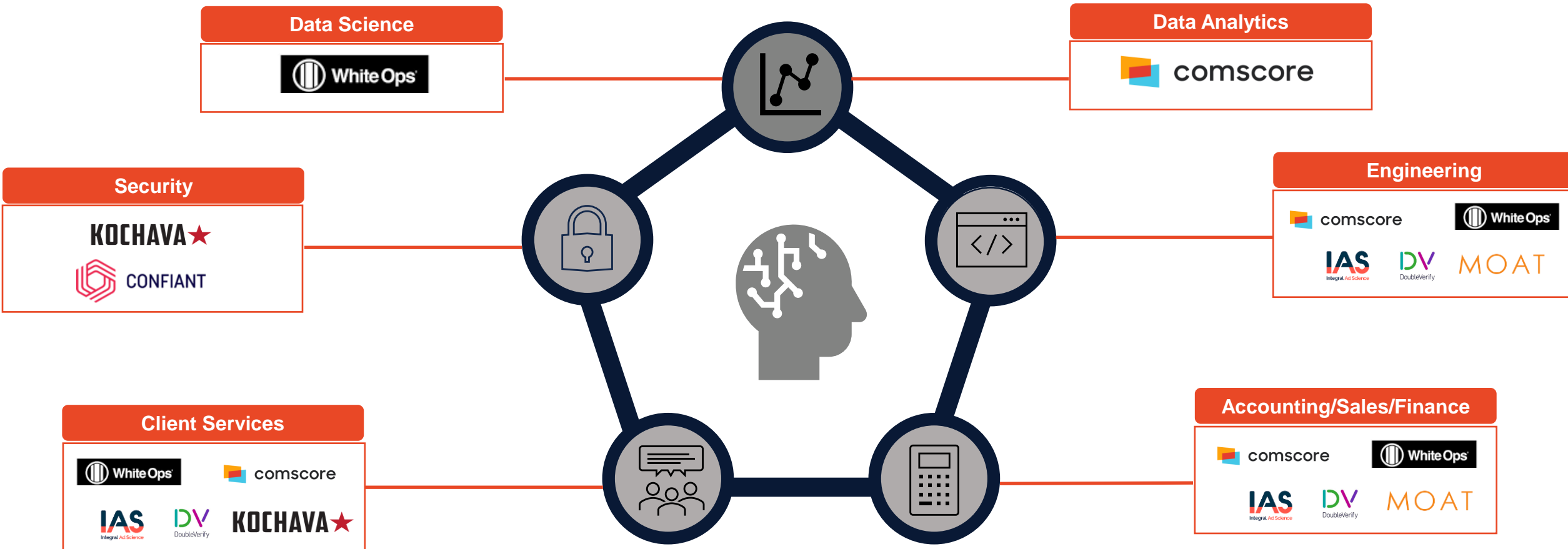


Key Insights

- IAS seems to be the **second biggest firm** having promising market share statistics in the ad fraud industry after Comscore
- IAS, Forensiq and Comscore have **secured impressive investment figures** of above **\$100M**
- Comscore has gained **three time more funding** than IAS and Pixalate
- The total funding is **not** always **directly proportional** to the number of investors. Eg: IAS, Forensiq, Pixalate

The annual revenue of ad fraud solution firms is directly proportional to the number of employees working there in most scenarios

Open positions are hinting towards the invested interests of top fraud solution providers



Ad fraud solution providers are recruiting skilled individuals from diverse backgrounds ranging from finance, engineering, sales, analytics and security

Understanding users and expert's opinions allows us pore deeper upon better brand landscaping

Vendors	Expert Perspectives	Validated User Reviews
Kochava	<ul style="list-style-type: none">Managed to uncover a global ad fraud scam in 2018Guarantees 99.98% uptime to its platformProvides users with a combination of both analytics and attribution features as well as iBeacons support, a server-to-server API and IdentityLink technology (cross-device app user identification) <p>-- Artyom Dogtiev, <i>Business Of Apps</i></p>	<p>“ The fraud monitoring features, and ease of data pipeline integration have been the most helpful. It has been easy to reconcile the post back data with our first-party data warehouse. The documentation is not so clear, and some features are not easy to setup without a proper documentation. ”</p>
ComScore	<ul style="list-style-type: none">Overstated revenues by US\$50 million and making “false and misleading statements”Purchased a fraud detection tech company called MdotLabs in 2014 <p>--Dr. Augustine Fou, <i>Forbes</i></p>	<p>“ I like it for trusted source to pull site traffic and as an apples to apples comparison across partners, and the ability to pull media traffic trends over time. But I don't feel like the source is extremely accurate, especially when comparing across different platforms. ”</p>

Each brand has its ultimate beneficial owner while still needs improvements

Understanding users and expert's opinions allows us pore deeper upon better brand landscaping

Vendors	Expert Perspectives	Validated User Reviews
Moat	<ul style="list-style-type: none"> • Uses a proprietary algorithm that identifies non-human traffic • Sends an email to alert the client when facing a bot • Uses Moat programmatically remove bot traffic <p>-- John Lincoln, <i>John Lincoln marketing</i></p>	<p>“ It is great for tracking viewability, brand safety, fraud, and multiple other metrics. Moat doesn't track on real time although it is about a 24-hour turnaround. Especially with short flights, it would be better to track at the beginning of the campaigns quickly . ”</p>
IAS	<ul style="list-style-type: none"> • Provides real-time solution to deliver verified inventory • Reduces Impression Waste by removing invalid traffic • General Purpose IVT Detection <p>--Dr. Augustine Fou, <i>Forbes, Automatad</i></p>	<p>“ I love that it's so easy to access brand safe metrics and out of geo metrics, both which are important to our campaigns. Unfortunately, IAS current reporting system needs some additional work. Their reporting system is overly complicated and not intuitive. ”</p>
Double Verify	<ul style="list-style-type: none"> • Accredited by MRC for in-app SIVT detection and filtration • Close direct deals with premium brands proving the inventories are viewable and safe — at one go <p>--Dr. Augustine Fou, <i>Forbes, Automatad</i></p>	<p>“ It is trusted and it's one third party standard across all publishers Currently, DV is top notch in their brand safety metrics. Unfortunately, with major competitors such as IAS and Moat providing much better reporting features, DV is being slowly phased out. ”</p>

Each brands have their own advocates and opponents depending on the user's needs

Research on Ad Fraud Solution Providers

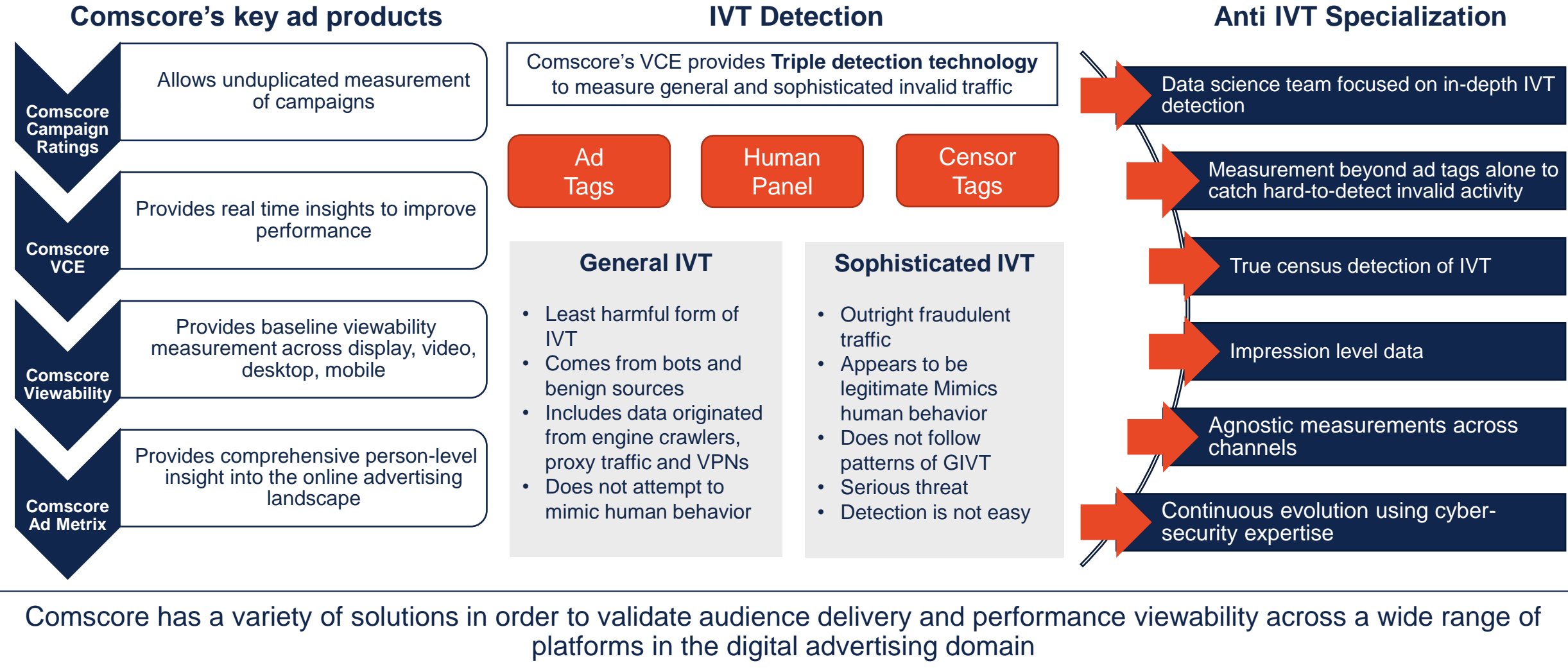
Chapter 04

Agenda

1 In-depth analysis on various ad fraud solution providers

2 Appendix

Research illustrates that comscore's VCE tool specializes in sophisticated invalid traffic detection

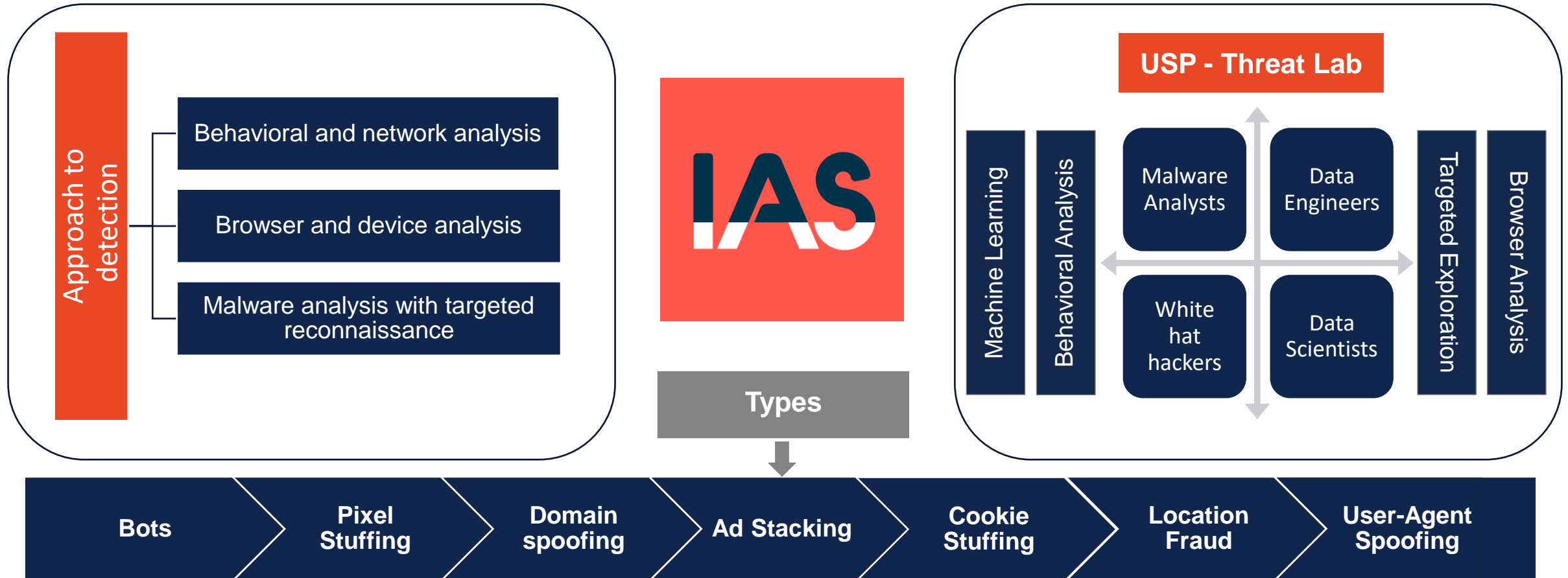


Comscore is making continuous advancements to increase transparency in digital advertising



Comscore's VCE is a holistic measurement solution that offers sophisticated ad fraud prevention and in-depth reporting by incorporating constant technical advancements

IAS has its own threat lab focusing on ad fraud and its prevention



Integral As Science develops sophisticated tools and has a dedicated threat lab to fight Ad fraud leveraging Machine learning and deep learning techniques

IAS fights ad fraud with the help of behavioral, network, browser & device analysis

Methodology

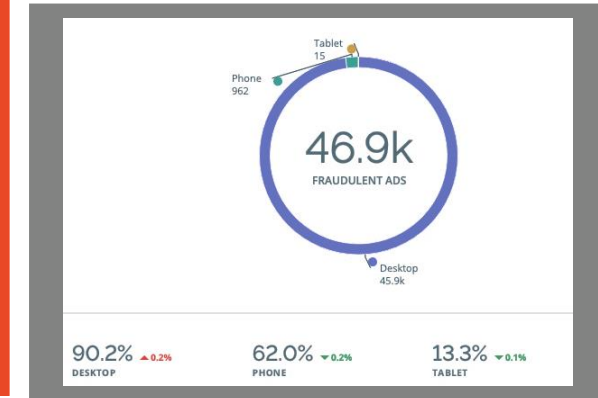
Behavioral & network analysis

- ✓ Processes and **analyzes** hundreds of billions of impressions that indicate fraud, across all channels and platforms
- ✓ **Creates scalable detection models** to distinguish real human behavior from bots
- ✓ **Impressions** are measured for:
 - Delivery channel, web page, inventory source, user
 - **Geographical distribution** of traffic
 - Temporal and historical browsing **patterns**
 - Page interaction: **scrolling**, clicking, mouse movements

Browser & device analysis

- ✓ Looking at **signs** sent during a specific **browser session** or from a specific device.
- ✓ Bots have a **signature set of features** that can be identified through detailed mapping of the browser environment and device characteristics
- ✓ The signals monitored include
 - **500+** static and dynamic browser features
 - **Targeted identifiers** of sophisticated malware
 - Page element **hierarchies** & styling

Dashboard



Reporting

“

“With Publisher Optimization, publishers finally have a real-time solution that helps deliver verified inventory to their clients. We’ve been able to significantly improve campaign yield, drastically reduce impression waste, and eliminate IVT as a result.” –

Marc Boswell,
SVP, Sales Operations and Client Services
Business Insider

”

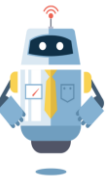
IAS methodologies identify scrolling and clicking patterns to differentiate bot and human behaviors

Wombles mimics the behavior of malicious bots and provides a control for the human traffic

Malware analysis and targeted reconnaissance

Just as fraudsters can try to reverse engineer security signals from tech companies, malware analysts can reverse engineer bots and other forms of fraud through activities such as:

- **Disassembly of fraudulent malware and software**
- **Direct analysis of paid traffic**
- **Infiltration of hacker communities**
- **Social engineering tactics**



90.8% more bot traffic was identified by IAS tech

Wombles, a crawling bot that allows IAS to objectively measure the amount of **invalid traffic** that IAS technology blocks by functioning as a pressure test for **verification and firewall technologies**

- Threat Lab is able to monitor for spikes in fraudulent activity to alert customers – in one case, the lab's investigation saved a major media platform **\$2.7 million** annually from a single fraudster
- The Threat Lab identified **Avireen**, a stealthy and flexible ad fraud botnet that generates approximately **1,500 fraudulent website impressions per hour per infected computer**
- The lab regularly conducts studies into emerging threats, such as **incentivized browsing, Poweliks, and Proxy8**

Benefits of IAS Publisher Optimization Tool

- **Prevent** over delivery and **impression waste** on viewability campaigns
- Customize **viewability**, brand safety, and **IVT goals** based on specific advertiser requirements
- Streamline workflow through **real-time** automated optimization and ad delivery
- Automate the creation of highly viewable, brand safe, and **fraud-free Private Marketplace (PMP)** deals for programmatic buyers
- **Monitor** and sequester fraudulent activity across device

IAS makes uses reverse engineering to detect invalid traffic thereby making the community aware of Ad fraud and its risks

Double Verify claims its platform is the industry's first unified service and performance platform



DV's Unique Selling Proposition

- Accredited by **Media Rating Council (MRC)** for SIVT detection and filtration
- Offering a safe platform for Buy & Sell-Side
- Acquired SaaS based **reporting and analytics** platform for digital publishers, **Ad-Juster**
- Covering on emerging channels (e.g. certified protection for **Programmatic, OTT, CTV**)



Brand Safety protecting features

75+

Content
Avoidance
Categories

200K

Ontological
concepts used in
Classification

1B

Keyword API
Calls Evaluated
Daily

DV's fraud solution techniques and services

10+ yrs

The Tenure of
DV's Fraud Lab

100x

Daily Frequency with
which DV Updates DSPs
on New Fraud Signatures

2M+

Bot and Malware
Devices Identified
Daily

500K

Fraudulent CTV
Devices Identified
Daily

- **Fighting fraud with real-time, accurate coverage** — gains transparency of monitored impressions by detailed breakdown of fraud (e.g. bot fraud, site fraud/IVT, app fraud/IVT), data center traffic, adware/malware (e.g. hijacked devices, injected ads), and emulator devices to identify weak links and opportunities
- **Full coverage throughout the media transaction** — from pre-bid avoidance segments to post-bid monitoring and blocking
- **All channels protection & 1st CTV Fraud Certification Program** — extends to desktop, mobile web and app and CTV, and is integrated across all major DSPs and social platforms, ensuring full protection across media buys. The first ad tech platform to receive certification include: Amobee, MediaMath, SpotX, The Trade Desk and Xandr

DV Pinnacle® powers meaningful insights to maximize return on advertisers' digital investment, and eliminate impression waste and maximize revenue potential for publishers

Double Verify provides a dedicated dashboard, giving clients transparency into media quality

Double Verify Pinnacle®

200+

Analytic &
Reporting
Metrics

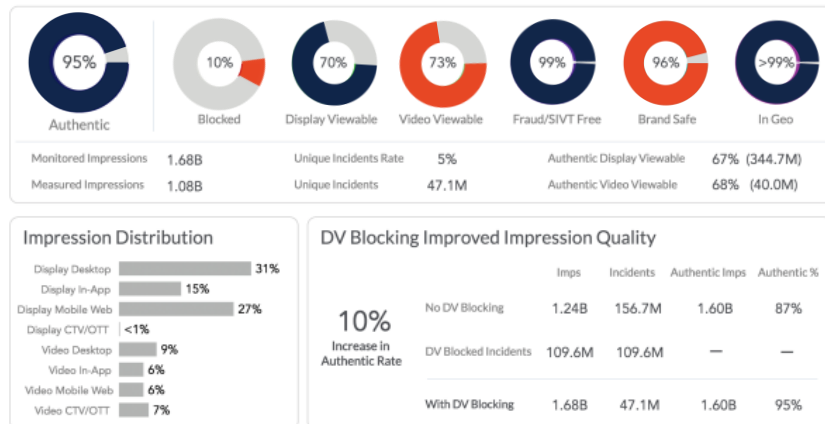
30+

Pre-defined
Reports

50+

Industry
Benchmarks
Filters

Easy-to-interpret dashboards provide a snapshot of key quality and performance metrics:



Double Verify's Authentic Impression® metric

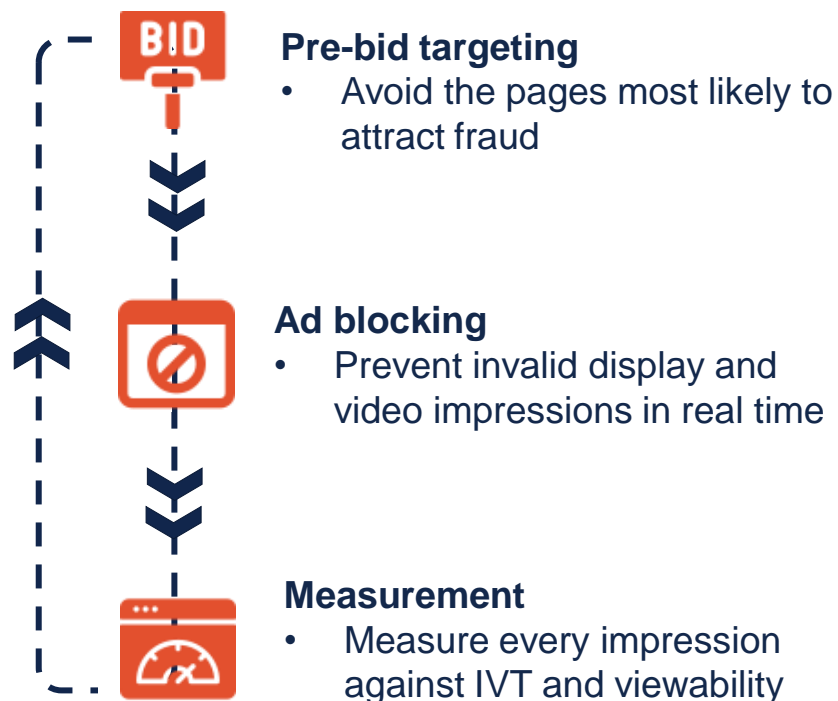
DV provides its proprietary Authentic Impression® metric that shows which ads were seen, by a real person, in a brand-safe environment and in the intended geography:

- **Measure the Authentic Impression® Everywhere**
 - net impression monitoring to promote supply transparency
 - defining KPI for quality, identifying and resolving domain and bundle ID mismatches across inventory
 - maintaining standards across multiple campaigns, platforms, and formats
- **Comprehensive Brand Suitability Controls in One Place**
 - package inventory in line with advertiser suitability standards
 - align pre- and post-bid brand safety settings universally with single set of controls
- **Custom Reports on Schedule**
 - accessing standard reports or build custom ones based on more than 200 data points, flagging critical opportunities for optimization

Double Verify help clients to turn insights into action with offering a definitive measure of quality across campaigns via their analytic and reporting dashboard

Measuring IVT helps moat to identify abnormal traffic patterns and block malicious non-human traffic

Moat's USP: "Pre-Bid by Moat"



Moat's goals and optimizations

Granular Viewability Standards

- Allows marketers to set viewability rates for specific ad slots and sizes
- Offers unprecedented precision before placement

Invalid Traffic Avoidance

- Benefits from learnings from Oracle's other anti-fraud acquisitions, including web security and managed DNS
- **Helps identify abnormal traffic patterns on the web**
- **Detects and blocks malicious non-human traffic**

Contextual Brand Safety Analysis

- Uses the contextual intelligence platform from its Grapeshot acquisition
- **Analyzes and interprets the actual content of each web page, not just its URL-level keywords**

Winning the Adweek "Readers' Choice: Best of Tech" Award for brand safety and verification with "Pre-Bid by Moat" allows Moat to offer three dimensions of optimizations for its clients

Offering SIVT detections for OTT and CTV enhances moat to corporate with multiple clients

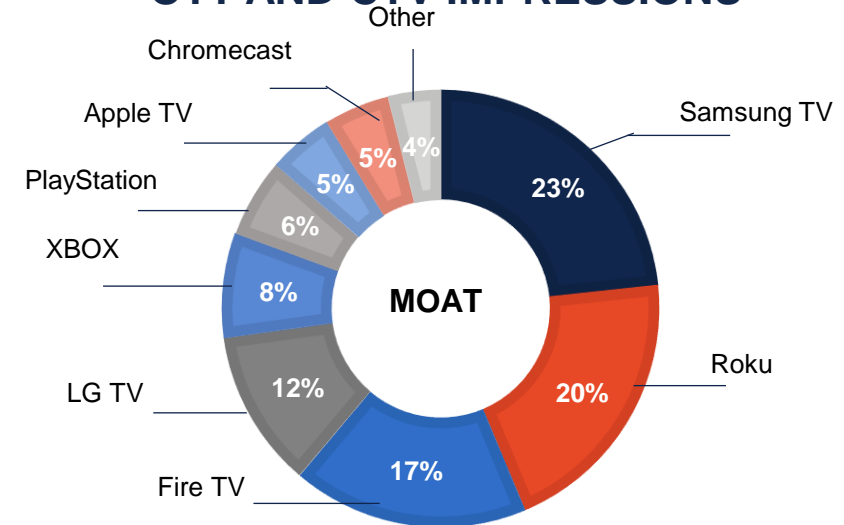
"Session Hijacked" by Moat

- **Monitors OTT(over-the-top) and CTV (connected TV) ad consumption patterns**
- Corporates with Sony Crackle in 2015 to provide a first-of-its-kind viewability measurement for OTT
- **Flags non-human traffic and other suspicious behavior**
- **Takes audience's modern viewing habits into account**, without taking it as impression-thieving bot
- **Detects the impressions that OTT devices serve continuously even when the TV is off**



Moat uses the MRC's latest viewability mandate: 100% of the pixels in view for at least two consecutive seconds. Because it is still early stages for OTT and CTV measurement, and there is no specific Media Rating Council standard for OTT.

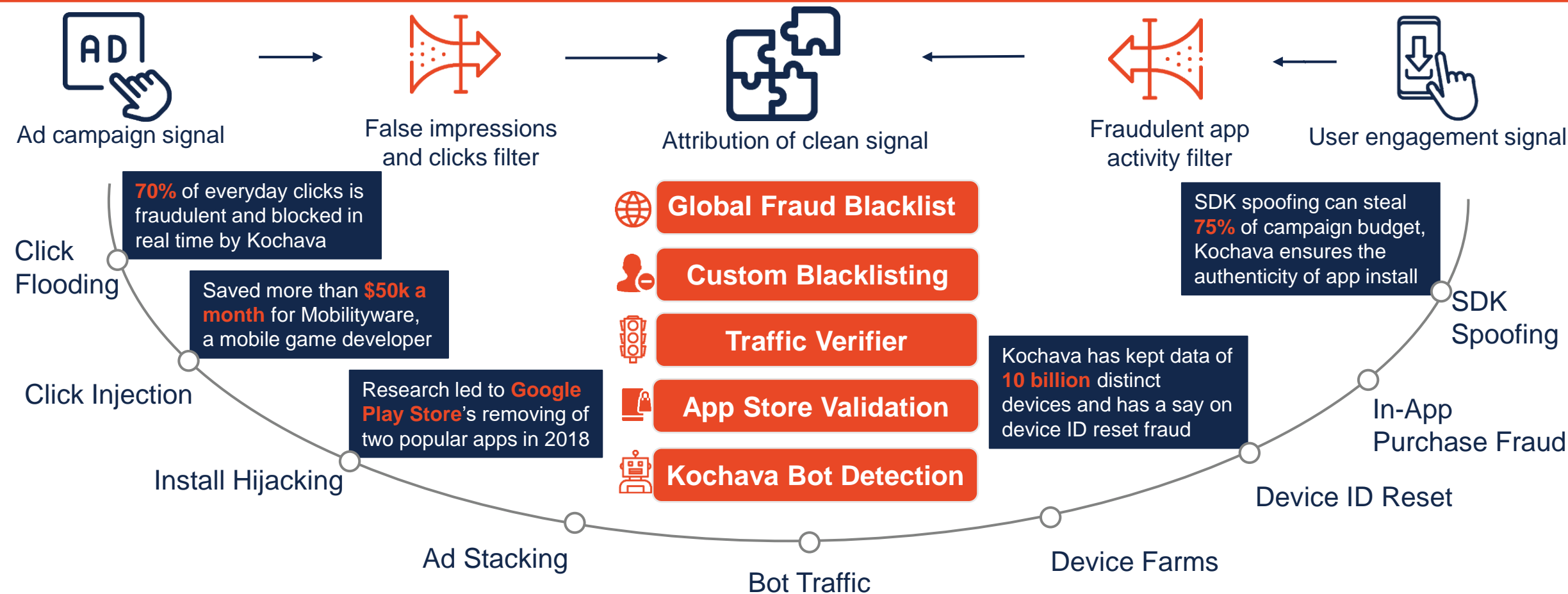
OTT AND CTV IMPRESSIONS



- Samsung Ads: partner with Moat to measure viewability and **the SIVT rates for ad delivery on OTT inventory across Samsung Smart TV household**
- Samba TV: integrates with Moat's SIVT detection and its content consumption across its CTV impressions

Moat provides "Session Hijacked" technology to brands to detect their OTT and CTV invalid impression

Kochava is a unified audience platform focusing on mobile marketing attribution and fraud prevention



Focusing on mobile ad attribution, Kochava clients report an average 17% saving on ad spend which may result from preventing ad fraudsters

Customers are satisfied with Kochava's anti-fraud tech as well as that from top 4 in mobile attribution

Successful cases lend credence to Kochava's expertise

“Without Kochava, we wouldn't know what traffic was legitimate. There's often such few installs to the amount of clicks reported. We wouldn't have the ability to **drill down to that publisher level and really see** who's defrauding us“ — *TwinSpires Spokesman*

“**Mobile ad fraud** literally use to keep me up at night, but Kochava's fraud protection has helped ease these nightmares“ — *Mobile app Marketing Manager, Credit Sesame*

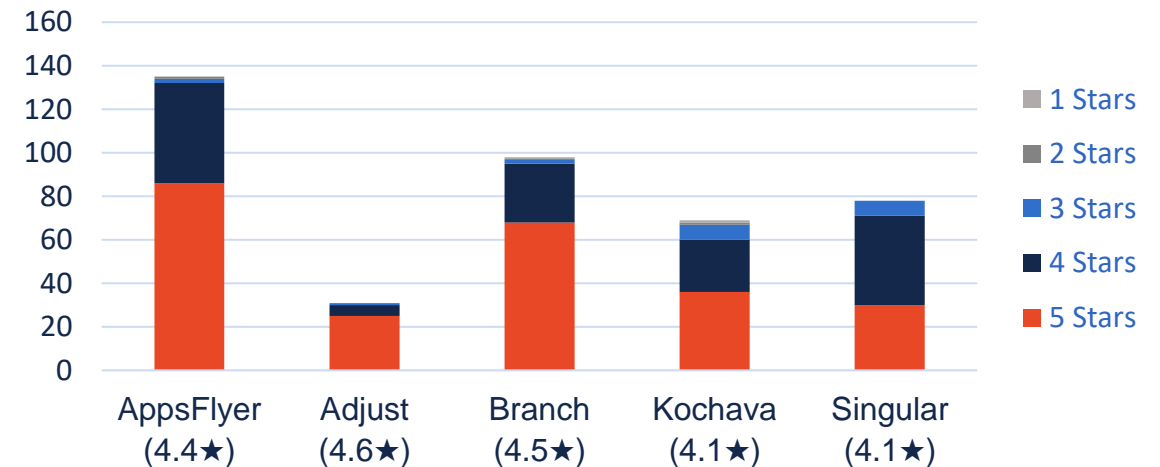
“Machine Zone chose Kochava for **mobile attribution analytics** not only because of their **better technology**, but also because of Kochava's **direct personalized customer service**, which may be their biggest competitive differentiator“ — *Chief Revenue Officer, Machine Zone*

Security job openings at Kochava

Senior Information Security Specialist

- Solid foundational knowledge of **TCP/IP networking**, systems administration, and general computer programming
- Familiarity with one or more **InfoSec and privacy frameworks** such as ISO 27001, SOC2, GDPR, CCPA, etc.

Review distribution under G2 mobile attribution sector



AppsFlyer, Adjust, Kochava all integrated thousands of mainstream media platforms partners, and provide similar services like fraud prevention, data analytics and free starter pack to support mobile advertisers

Having its unique selling points while Moat still has the limitations to overcome

Validated User Reviews of Moat

*It is great for tracking viewability, brand safety, **fraud**, and multiple other metrics. Their user interface is phenomenal, and they provide easy to digest graphical information.*

*I've had personal experience with mostly all the platforms and consistently I as well as our biggest brand advertisers find MOAT to be **the most reliable** (had to do something right to **be bought by Oracle**).*

*MOAT wasn't MRC accredited for SIVT until after they were already owned by Oracle. In my testing MOAT always **under measured relative to the avg between platforms** but was generally in line with IAS.*

Expert Perspectives of IVT measurement



Dr. Augustine Fou
Independent Ad Fraud
Researcher

- **Has significant limitations when measuring in new environments**, like video ads, ads in mobile apps, and now connected TV (CTV) streaming ads
- **May not be correct due to the various reasons**: the detection tagging getting blocked, not loading and executing, or sending any data back
- Becomes **“black box”** fraud detection in many verifying vendors with MRC

Moat's IVT measurement gains many compliments from its users, but the expert still points out that the technology needs improvements to present the most correct results

White Ops uses deep learning and machine learning methods in their system

Technical Evidence

- Collects an average of **2,500** signals for each interaction
- **Privacy-sensitive approach**
- Enables to **gather data** on the **network, device, software, application, and user configuration** to detect technical evidence of compromise



White Ops follows a multi-layered approach

Global Threat Intelligence

- Specializes in threat hunting, **malware reverse engineering**, and threat modeling
- Analysts proactively hunt for new threats on the internet, **attributing threats** to specific botnet operators, campaigns, and other threat actors

Machine Learning

- Analyzes **thousands of data** points collected across trillions of transactions
- Predict malicious behavior, enabling us to provide a **high level of accuracy**, even when there is minimal technical evidence

Continuous Adaptation

- White Ops **speed to identify** and build **new detection mechanisms** in order to stay ahead of the adversary more than other **solutions** that are built on fixed detection mechanisms

White ops won Eight 2020
Cybersecurity Excellence
Awards

Fraud Protection

Application Integrity

Marketing Integrity

Bot Mitigation Platform



White Ops is one of the most trusted tools that work on strengthening their backend algorithms to mitigate ad fraud

White Ops provides services to both supply-side and demand-side platforms

DSPs

Protect and Grow Revenue

DSPs ensure the **highest** level of human-verified inventory and deliver more reliable results for advertisers

Minimize Clawbacks and Inefficiency

By preventing fraudulent behavior before the bid, DSPs **avoid middle-man** remediation conversations with suppliers and reduce clawback payments to advertisers

Deliver Seamless Experience to Brands and Clients

DSPs using White Ops **removes** the **burden** of **fraud protection** from clients to deliver a seamless experience for advertisers

SSPs

Minimize Fraud to Ensure Clean Inventory to Buyers

Insights to inform publisher partnerships and act when necessary

Reduce Downstream Costs

Prevents fraud before the bid to avoid remediation conversations with publishers and DSPs

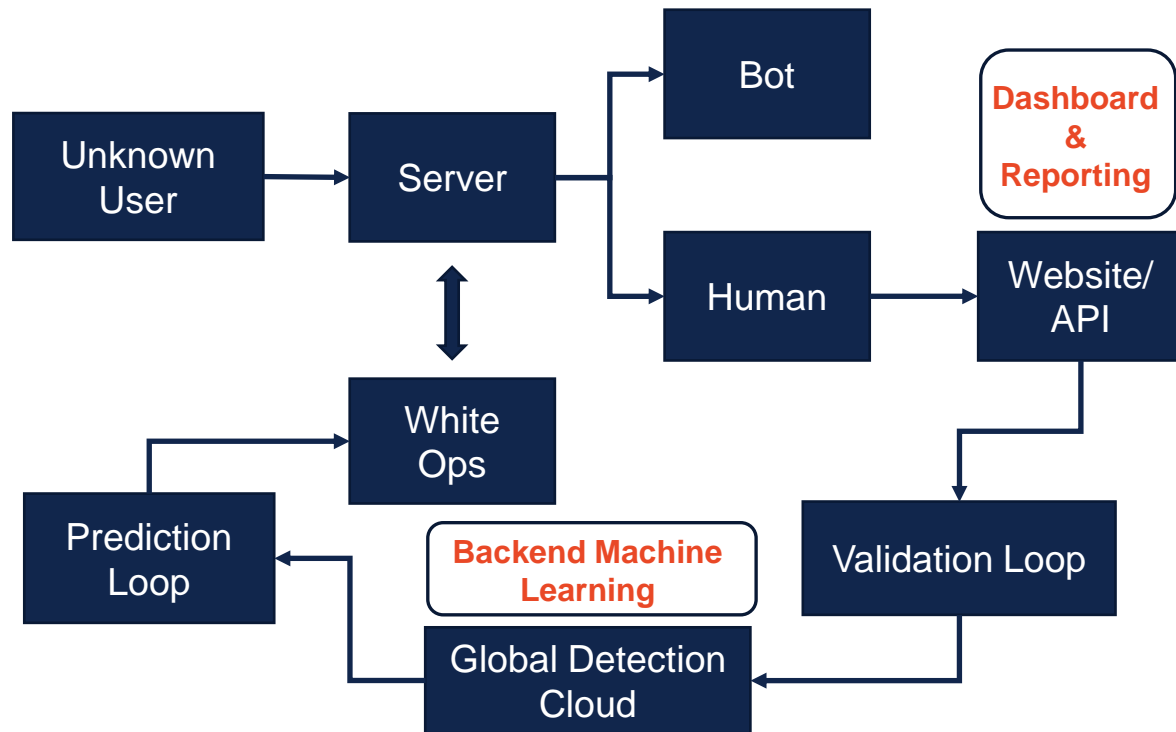
Make the Internet Safer for Advertisers

Ensures that **fraudulent supply** doesn't make its way to buyers

White Ops helps its advertisers and publishers with features such as reduced costs, deeper insights leading to smooth operation on both ends

White Ops focuses on improvising their existing dashboards to meet end user needs

Methodology



Reporting and Dashboards

- Provides full **visibility** into fraud
- Reporting gives you full visibility into **bot and nonstandard events**, including the specific threat category and factor observed
- Analysts can also create **custom reports** and visualizations to gain a clear picture of how to reduce fraudulent activity
- Reports can be **saved**, scheduled to run on a cadence, and **easily exported** to share with stakeholders
- White Ops Application Integrity dashboard is **easy to use** regardless of background or role

Pre-Serve IVT- Fraud rate in an unprotected environment

Post-Serve IVT- Fraud rate after blocking

Total IVT Potential - clearer chart, Post-Serve IVT rate and the Potential IVT rate side-by-side

Coverage Clarity – Helps measure Post-Serve impressions

White Ops works on customer reviews and helps its end users have an easy interface to understand the IVT

Cheq offers award-winning cybersecurity solutions to fight against ad fraud

CHEQ 's Achievements and Accreditation

- A true leader in cybersecurity industry accredited by multiple, prestigious awards:



2X Ad Fraud Solution 2019/2020
Best Search Software 2020

**Top 10 AI Solutions of
the year 2019**



**Tech Transparency Award
Winner 2019**

Best AI-driven Ad Fraud solution 2020



World's 100 Hottest Startups 2019

Cheq's solutions for Display & Video

Ad Fraud

- Real-time cyber-security analysis and blocking** — examining 1,000 different user and network parameters to detect and prevent invalid traffic (GIVT /SIVT)
- Advanced filtration modules** — including fingerprinting (OS /Device /UA), behavioral /network analysis, dynamic honeypots and more

Brand Safety

- Real-time NLP content analysis** — classifying and scoring the content against 200+ proprietary contextual categories
- Customized Enforcement** — creating custom brand suitability categories and tweaking sensitivities according to specific needs
- Advanced Contextual Modules** — including lexical semantics, conversational learning, computer vision and more

Viewability

- Pre-impression Measurement** — providing granular, per-impression measurement of viewability, as opposed to today's industry-standard
- 3D Viewability Measurement** — offering the only viewability solution for 3D gaming environments, with tracking of ad angle, brightness, time-on-screen and obstructing objects

Cheq's leading cyber-driven ad-verification platform for advertisers, is built with next-gen ad-fraud prevention, brand safety enforcement and viewability control

Cheq promises to save wasted ad-spend across all major PPC buying channels for advertisers

Cheq's solutions for Pay-per-click (PPC)

- **Protect all the channels**
 - **One-stop-shop solution**
 - eliminating invalid clicks across all the major PPC / Search buying channels, including Google Search Ads, Bing, Facebook, Instagram, Twitter, Snap, Yahoo, Baidu, Yandex, VK and more
- **Exclude invalid audiences**
 - offering the first and only solution allowing clients to **build invalid audience segments**
 - excluding them from all campaigns via a simple SSO (Single Sign-On) connection
- **Run powerful JavaScript to catch bot traffic without over-blocking**
 - looking at **over 1,000 unique parameters**
 - performing advanced OS / Device fingerprinting, behavioral and network analysis

Cheq's SaaS Cases and Performance

INSIDE × A major online fashion retailer in U.S.

18%

Reduced CPA

35%

Improved ROAS

\$65K

Ad Spend Saved (Monthly)

INSIDE × Dentsu's Cyber Communications Inc (CCI) in Japan

1st

For the first time deep learning is applied for digital advertising

10M

Documents that NLP was heavily trained in Japanese

39

Nuanced categories of brand safety in Japanese

700

Custom parameters was deployed for verification

183M

Fraud impressions blocked

576M

Brand safety impressions blocked

95%

Accuracy rate

250%

CTR increased

Cheq applies best-in-class cybersecurity, machine learning and bot mitigation capabilities to proactively eliminate invalid activity plaguing today's PPC industry

Designing “Immunity” to measure security issues enables Confiant to help publishers and SSPs

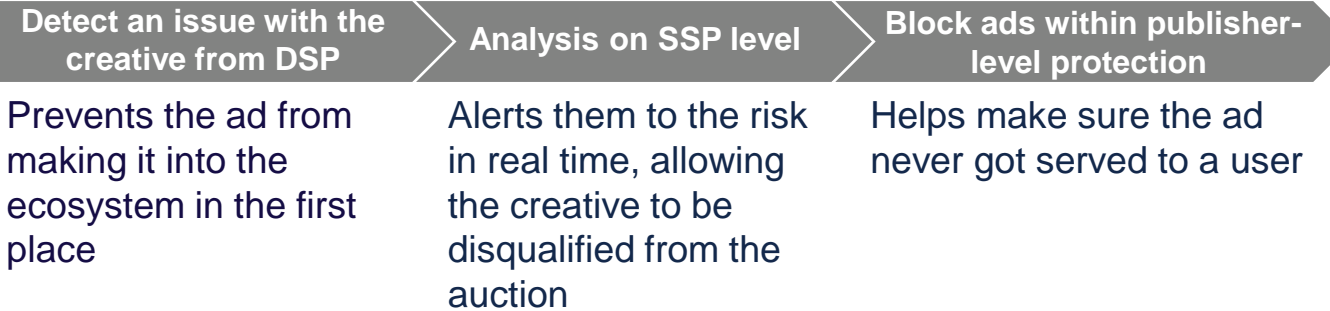
Confiant’s solutions for publisher and SSP



- **Identifies and blocks all types of malicious creatives in real-time automatically**
- Stops turning off revenue streams
- gives publishers **the transparency and controls needed to stay on top of problematic ads**
- Tracks DSP ad quality and publisher performance
- **Uncovers and instantly blocks unwanted ads from winning an auction**
- **Polices in real-time the bid stream with purpose-built verification technology**

Confiant is currently enrolled in the Verified by TAG program

Confiant’s USP: “Immunity by Confiant”



The dashboard across different forms



Confiant provides “Immunity by Confiant” to measure ad frauds across devices and channels for publishers and SSPs

Oxford BioChronometrics is a small sized company specialized in cybersecurity of bot's prevention

Block bot traffic

Identify out-of-area traffic

Gain insight into audience and fraud

Generate on-demand report

Core tech and etymology

- Oxford: started at Oxford Innovation lab in 2014
- Bio-Chrono-Metrics = Life + Time + Measurements = **measure by human patterns with changes over time**
- Uses 500 variables such as user type, text, click, swipe on device etc. to derive a behavioral profile called “eDNA”

Awarded NATO 2017 Defense Innovation Challenge

- **Singled out** for its technology to detect the “weapon of choice” for state-sponsored cyberattacks (aka Remote Access Trojans), as one of ten final winners
- Challenge was for “transformational, **state-of-the-art** technology solutions from small business and academia”

Winner of a blind comparison test by Shailin Dhar

- OBC detected **90%** as IVT, where other famous vendor detected: **DataDome (52%), Moat (38.27%), IAS (17%)**
- **Dr. Augustine Fou** commended Dhar’s experiment

Team background (10 employees on LinkedIn)

- Adrian Neal, **Founder** and Chief Scientist
 - Worked as **senior security consultant and security architect** in UBS, Zurich Financial Services, Roche, ASB Bank, NAB, Telstra, founder of Oxford Scientifica
 - M.S in Software Engineering, Oxford University
- David Scheckel, **CEO**
 - **No previous experience** in cybersecurity or media
 - B.A in Economics, Fordham University
- Sander Kouwenhoven, **CTO**
 - R&D at ABN AMRO Bank (3rd Dutch largest bank)
 - Engineer degree in Informatics, Hogeschool Utrecht

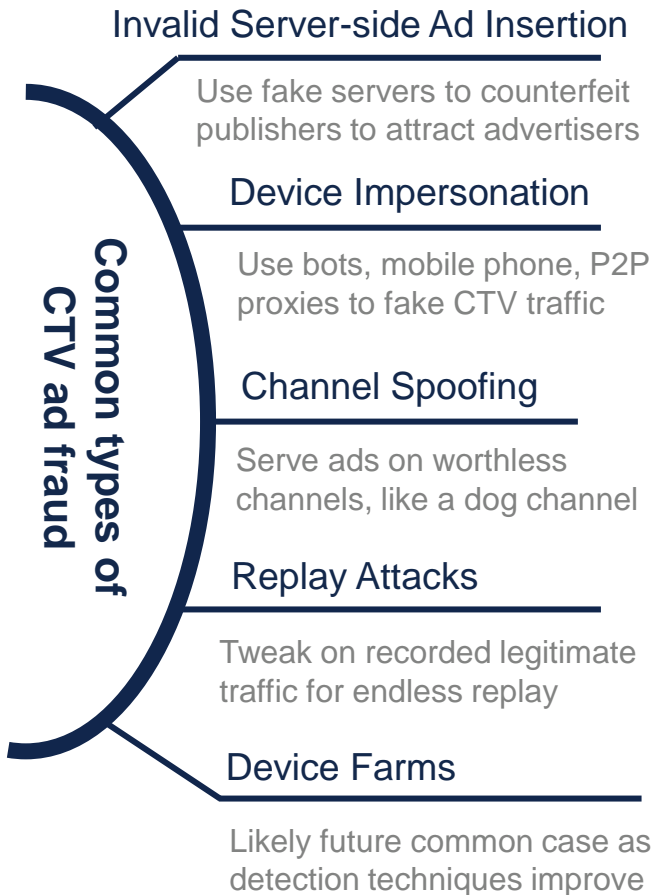
Possible weaknesses

- **Small company size** may be a sign of underdevelopment, few cases or reviews to prove the success of the company
- OBC may showed lack of relevant background , **lack of experience and connection** in advertising industry

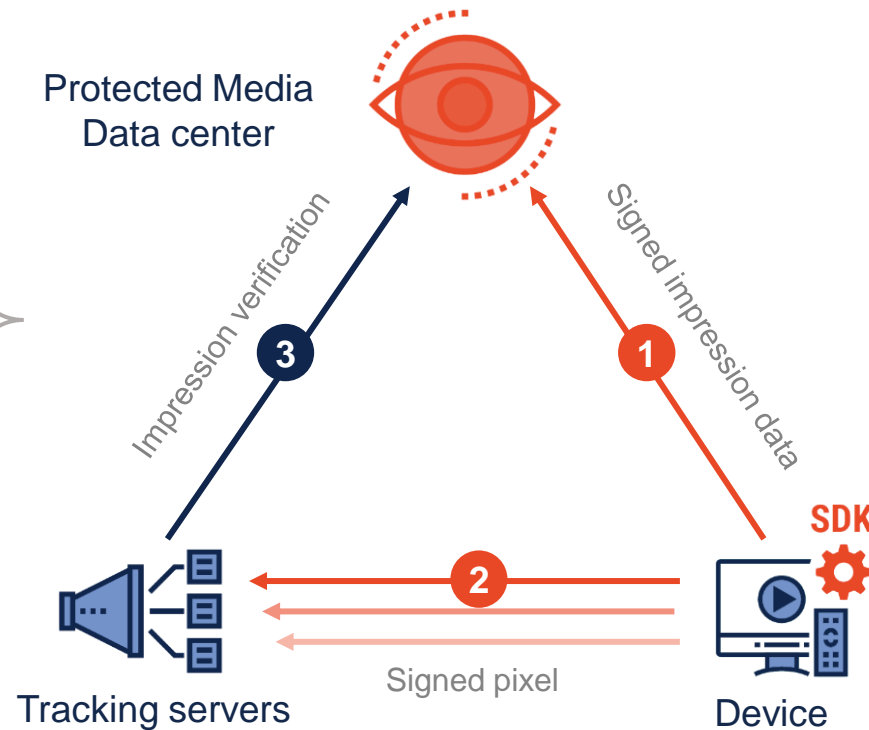
STOP FRAUD
STAY RELEVANT

OBC may be capable of offering cutting edge tools for advertisers to prevent bot-related fraud, yet the small size of company over these years casts doubts on its effectiveness

Protected Media is a company focused on CTV ad fraud prevention for advertisers and publishers



Protected Media uses Three-Way Handshake to verify the validity of each transaction



Accreditations of Protected Media



PM is MRC®, TAG and IAB-TCF accredited
TAG: 88% lower IVT than MRC® vendor in 2019

Partners with Protected Media



Different from the web market, CTVs are more like black boxes to ad fraud and often fail to provide sufficient training data for traditional machine learning approaches

Offering proper measurements insights allows Moat's dashboard help clients to evaluate different ad platforms

Moat's Dashboard

Desktop Display

- **In-view time:** time spent with advertising at minimum 50 pixels for at least one continuous second
- **Interaction rate:** % of impressions where a user remains active for 0.5 seconds
- **Interaction time:** time spent interacting with advertising

Mobile

- **Active page dwell time:** Time spent with content in the foreground tab
- **In-view time:** time spent with advertising at minimum 50 pixels for at least one continuous second
- **Touch rate:** % of impressions touched on a mobile device

Video/Digital Streaming Service

- **Percentage of video played in-view:** % of video users watched in-view
- **Completion quality:** % of completes in-view with audio enabled
- **Audible rate:** % of impressions where video was audible
- **Completion rate:** % of impressions where video was played to completion

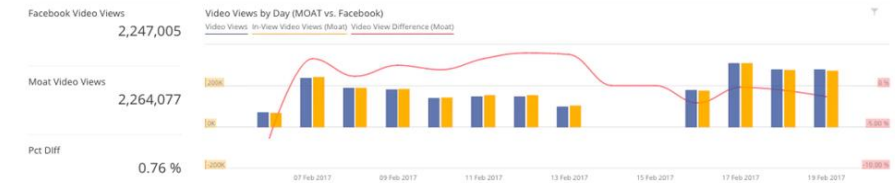
Branded Content

- **Scroll rate:** % of page views where users scrolled
- **Scroll depth:** % of total page length to which users scrolled
- **Active page dwell time:** Time spent with content in the foreground tab

Data as of 7:41 pm EDT | Exports | Settings

BlueKai Segment	Impressions Analyzed	In-View %	In-View Time (s)	Total Exposure Time (hr)	Universal Interaction %	Universal Interaction Time (hr)	Total Ad Dwell Time (hr)	Hover %	Time Until Hover (s)	Attention Quality	Scroll %	Time Until Scroll (s)	Active Page Dwell Time (s)	Click %	Moat Index	Moat Score
MOAT	120,147	68.52%	52.03	1,189	5.97%	12.26	22	17.55%	87.33	33.99%	73.28%	40.87	75.58	1.64%	100	776
In-Market > Retail 19	12,412	64.87%	57.15	128	7.41%	22.9	6	19.51%	87.62	37.97%	71.29%	45.46	75.57	3.04%	107	808
In-Market > Retail > Clothing > Shoes & Accessories 3177	4,611	69.81%	52.76	47	5.52%	25.79	2	19.31%	104.72	28.57%	75.80%	30.88	82.02	1.26%	99	773
In-Market > Retail > Clothing > Shoes & Accessories > Clothing 10930	4,263	71.43%	50.94	43	5.26%	5.21	0	18.80%	114.72	28.00%	76.71%	29.35	81.16	1.30%	82	689
In-Market > Retail > Electronics 151	4,205	72.41%	47.21	40	5.34%	1.63	0	15.27%	69.57	35.00%	80.56%	48.58	74.95	0.69%	85	705
In-Market > Retail > Entertainment 11336	4,002	71.01%	52.27	41	3.17%	2.23	0	15.08%	91.1	21.05%	75.18%	45.14	74.78	0.72%	71	638
In-Market > Retail > Entertainment > Tickets 1658	3,857	71.43%	51.96	40	3.31%	2.23	0	14.88%	94.84	22.22%	75.76%	47.45	74.49	0.75%	72	643
In-Market > Retail > Clothing > Shoes & Accessories > Clothing > Women 145	3,857	75.94%	49.86	41	5.04%	1.18	0	19.33%	117.69	26.09%	79.55%	30.99	82.08	0.75%	80	681
A/B Test Groups > Group 07 3845	3,712	64.84%	74.86	50	6.03%	47.3	3	23.28%	77.23	25.93%	70.87%	50.11	75.28	0%	98	767
A/B Test Groups > Group 10 3842	3,712	60.16%	46.16	29	3.42%	77.24	2	15.38%	74.56	22.22%	66.41%	22.38	59.71	1.56%	87	713

Video Views



Campaign Level Impressions Comparison (MOAT & Facebook)

Campaign Name	Media Buy Name	Creative Name	Video Views	In-View Video Views (Moat)	Video View Difference (Moat)
23842638704720458	23842638704720458	23842638722204058	378,907	373,319	-1.47 %
23842638704720458	23842638704720458	23842638718880458	21,624	18,142	-16.01 %
23842638704720458	23842638704720458	23842638712190458	479,801	475,967	-0.80 %
23842638704720458	23842638704720458	23842638722304058	160,248	163,413	1.98 %
23842638704720458	23842638718880458	23842638718880458	404,524	416,931	3.07 %
23842638704720458	23842638718880458	23842638718880458	707,094	718,245	1.58 %
23842638704720458	23842638718880458	23842638718880458	78,449	80,919	3.15 %
23842638704720458	23842638718880458	23842638718880458	16,358	17,121	4.66 %
Total			2,247,005	2,264,077	0.76 %

1 - 8 of 8 items

Moat's analytics affords clients the ability to reflect on performance over time and across channels, product lines, creative strategies, industry benchmarks

Mid-Term Vendor Assessment

Chapter 05

Agenda

1

Breakdown of the Ad fraud Industry

2

Overview of various Ad Fraud solution providers

3

Vendor Assessment Matrix

4

Visualization

5

Appendix

Programmatic ad's opaque triggers ad fraud to become the biggest market for organized crime

\$2.9
Trillion

Overall ecommerce sales are projected to grow by 30.4% to **\$2.9 trillion** in 2020

\$59
Billion

Marketers will invest **\$59 billion** in advertising during 2020

\$1
Million

69% of brands spend **\$1 million per month** in 2020

\$42
Billion

Juniper estimated advertisers worldwide would lose **\$42 billion** to digital ad fraud in 2019

20%

At least **20%** of brands' budgets were being lost to digital ad fraud in 2019

25%

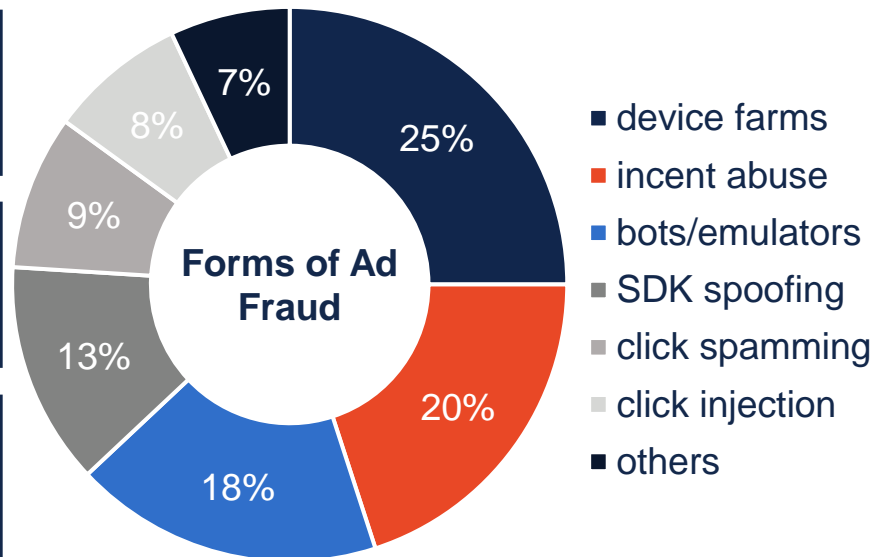
25 % of marketers are unclear about fraud exposure

48%

48% of marketers are seeing results but still have work to do

27%

27% of marketers are significantly reducing results below industry average






Pain Points

- Digital ad budgets being wasted
- **OTT and CTV ad fraud** is the next challenge
- **Mobile in-app** has the highest ad fraud rates
- Ads.txt is not a one-stop-shop solution to all ad fraud

Digital ad fraud is still a major problem for programmatic advertisers and their partners throughout the supply chain to solve

Research shows top vendors are using cutting edge technologies to fight against ad fraud

	comscore	IAS	IDV	MOAT	White Ops
 Specialization	Viewability and IVT	General Purpose IVT	General Purpose IVT	Viewability and IVT	Malware-based Fraud
 Main Feature	Validated Campaign Kit	Targeted Exploration	DSP Integration	Granular Viewability	Visibility Into Bots
 Core Technology	True Census Detection	Scalable Detection	SAAS Analytics	Hijacked Session	Continuous Adaptation

pixalate	CHEQ	KOCHAVA	CONFIANT	OXFORD BIOCHRONOMETRICS	PROTECTEDMEDIA
Pre-bid Blocking	IVT Detection	Mobile App Install Fraud	Malvertising	Bot Traffic Prevention	CTV Fraud
Omni-channel Protection	Wide Channel Coverage	Cleaned Attribution Data	Malicious Ad Blocking	Secure Ad and Contact	Evidence-based Solution
Customizable ML	Real-time NLP Analysis	App Store Verifier	Ad Performance Track	eDNA Behavioral Profile	Three-Way Handshake

Vendors are detecting IVT with the application of machine learning and deep learning techniques paired with data analysis thereby specializing in ad fraud using their own unique mechanism

Vendor Assessment Matrix

Vendors	Deployment Platform	Vendor Type		Type of Media Supported				Dash-Boarding and Reporting	Accreditations		Tags	% Market Share	No. of Employee	Number of Patents	Funding raised	Type		
		DSP	SSP	Video	CTV	OTT	Display		TAG	MRC						Private	Subsidiary	Public
Comscore	CTV, mobile, desktop	✓	✓	✓	✓	✓	✓	✓	✓	✓	Marketing Technology Research Analytics	16.30%	1,800	101	\$562.4M			✓
Integral Ad Science (IAS)	CTV, mobile, desktop	✓	✓	✓	✓	✓	✓	✓	✓	✓	Marketing Technology Analytics Media	9.91%	700	17	\$120.8M	✓		
Double Verify	CTV, mobile, desktop	✓	✓	✓	✓	✓	✓	✓	✓	✓	Marketing Advertising Analytics Media	15.82%	550	2	\$81.8M		✓	
Moat	CTV, mobile, display	✓	✓	✓	✓	✓	✓	✓	✓	✓	Marketing Technology Sales automation	13.04%	150	3	\$65M		✓	
White Ops	CTV, mobile apps, web	✓	✓	✓	✓	✓	✓	✓	✓	✓	Technology Cyber Security Fraud Detection	<0.01%	159	4	\$31.1M	✓		

Double Verify and Moat is doing better in capturing the market than Comscore even having less available resources

Vendor Assessment Matrix

Vendors	Deployment Platform	Vendor Type		Type of Media Supported				Dash-Boarding and Reporting	Accreditations		Tags	% Market Share	No. of Employee	Number of Patents	Funding raised	Type		
		DSP	SSP	Video	CTV	OTT	Display		TAG	MRC						Private	Subsidiary	Public
Pixalate	Display, in-app, video, OTT	✓	✓		✓	✓	✓	✓	✓	✓	Technology, Security	2.24% (OVP)	~33	0	\$4.8 M	✓		
Cheq	Display, Video, PPC	✓		✓			✓	✓	✓	✓	Technology Cyber Security Fraud Detection	<0.01%	~71	3	\$21 M	✓		
Kochava	Mobile, web, desktop, gaming	✓	✓		✓	✓		✓	✓		Marketing advertising mobile app mobile marketing platform	0.14%	~150	2		✓		
Confiant	Desktop, mobile, video		✓					✓	✓		Technology, cybersecurity	0.20%	~33	0	\$4.1 M	✓		
Protected Media	CTV, display, video	✓	✓		✓	✓	✓	✓	✓	✓	Technology Cyber Security Fraud Detection		~150	0		✓		

Pixalate is capturing the market for Online Video platform better than Cheq and other solution providers

Market Share



- White Ops < 0.01%
- Pixalate 2.24%
- Cheq <0.01%
- Kochava 0.14%
- Confiant 0.20%

Fund Raised

White Ops \$31.1M

Pixalate \$4.8M

Confiant \$4.1M

OxfordBC \$3.1M

Protected Media \$4M

Cheq \$21M

IAS
\$120.8M

DV
\$81.8M

comscore
\$562.4M

MOAT
\$65M

BIG
Business Intelligence Group

comscore
1800

IAS
700

DV
550

159
White Ops

150
MOAT

150
KOCHAVA

150
PROTECTEDMEDIA











71
CHEQ

33
pixalate

33
CONFANT

Number of Employees

Research shows leading ad fraud solution providers are delivering insights across various environments

Vendor	Framework	Platforms	Vendor	Framework	Platforms
 comscore	SDK	CTV, mobile, desktop	 pixalate	API	Display, in-app, video, OTT
 IAS Integral Ad Science	SDK JS tag script	CTV, mobile, desktop	 White Ops	Tags via JS, SDKs, 1x1 pixel	CTV, mobile apps, web
 DV DoubleVerify	VAST tag JS tag script	CTV, mobile, desktop	 CHEQ	API Server-to-server	Display, Video, PPC
 MOAT	JSON return tag SDK	CTV, mobile, display	 PROTECTED MEDIA	SDK AI datastream	CTV, display, video
 KOCHAVA★	SDK Server-to-server	Mobile, web, desktop, gaming	 CONFIANT	Tags, custom integration	Desktop, mobile, video

Major ad fraud vendors are incorporating the open measurement SDK for android and IOS web browsers as a common industry standard for measurement and verification of insights obtained through monitoring ad traffic

Research on Ad Fraud Challenges and Events

Chapter 06

Agenda

- 1 In-depth analysis of role of piracy in Ad Fraud
- 2 Evolution from Ad Verification to Ad Security
- 3 Overview on industry actions and limitations
- 4 Rise in Ad Fraud threats in the OTT Industry
- 5 Analysis of Ad Fraud in DOOH and major Ad Fraud events

Applying programmatic ad technique causes ad-supporting piracy's prosperity

Harm to advertisers

- **Contents being stolen**
- Digital ad budgets being wasted
- **Reputation being damaged**
- Criminal being funding
- **Losses in \$4 trillion by IP theft**
- Brand unknowingly support piracy
- Digital ads fund **85% of online pirate streaming activity**

Harm to consumers

- **Private information being stolen**
- Devices being **loaded enormous quantities of ads behind the scene**
- Devices being used to **mine cryptocurrency**
- Devices being transformed to **a part of a large botnet to carry out other attacks**

“ Marketers should:

- **Dig deeper beyond just placement reports** that just show domains and quantities of impressions purchased
- **Use additional technology and services to detect exactly where their ads ended up and aggressively block the piracy sites that appear**

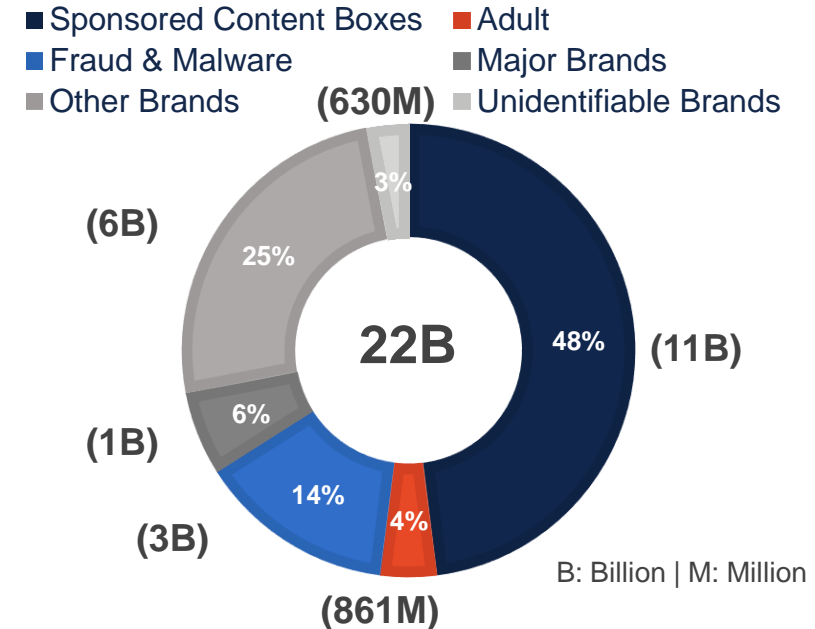
-- Dr. Augustine Fou ”

Rarely see piracy sites?



Ads that ran on piracy sites are conveniently commingled with ads that ran on *nytimes*, *USA today*, and other mainstream sites

Ad campaign type | Est. ad impression



- **Piracy sites monetize by Sponsored content boxes**
- Piracy sites proactively obfuscates or pretends someone else's domains (**domain spoofing**)

Sponsored content boxes is the major piracy ad campaign type to devastate both advertisers and consumers

Digital advertising industry has worked proactively and collaboratively to fight ad supported piracy

Digital piracy

Criminals **steal** copyrighted digital content and then make that content available illegally on their own websites. Such **copyright thieves' profit** by selling advertising on the sites that they have set up to distribute stolen content, and by **infecting end-users** of those sites with **malware** that allows them to commit more crimes

TAG Certified Against Piracy Program

- TAG launched its **Certified Against Piracy (CAP)** Program in **2015**
- Helps advertisers and their agencies **avoid damage** to brands from ad placement on websites and other media properties that facilitate **the distribution of pirated content and counterfeit products**

The TAG-CreativeFuture Partnership

- TAG and CreativeFuture have alert advertisers when ads are found next to pirated content
- Employ a process **including identification of high-risk sites, application of ad-scanning, analysis of scanning results**

Plan of Action

- Take Responsibility
- Choose Right Partners
- Employ the Right Tools



- Develop and Execute Strategy
- Accountability with agreements & contracts

TAG Partnering with Policy-Makers

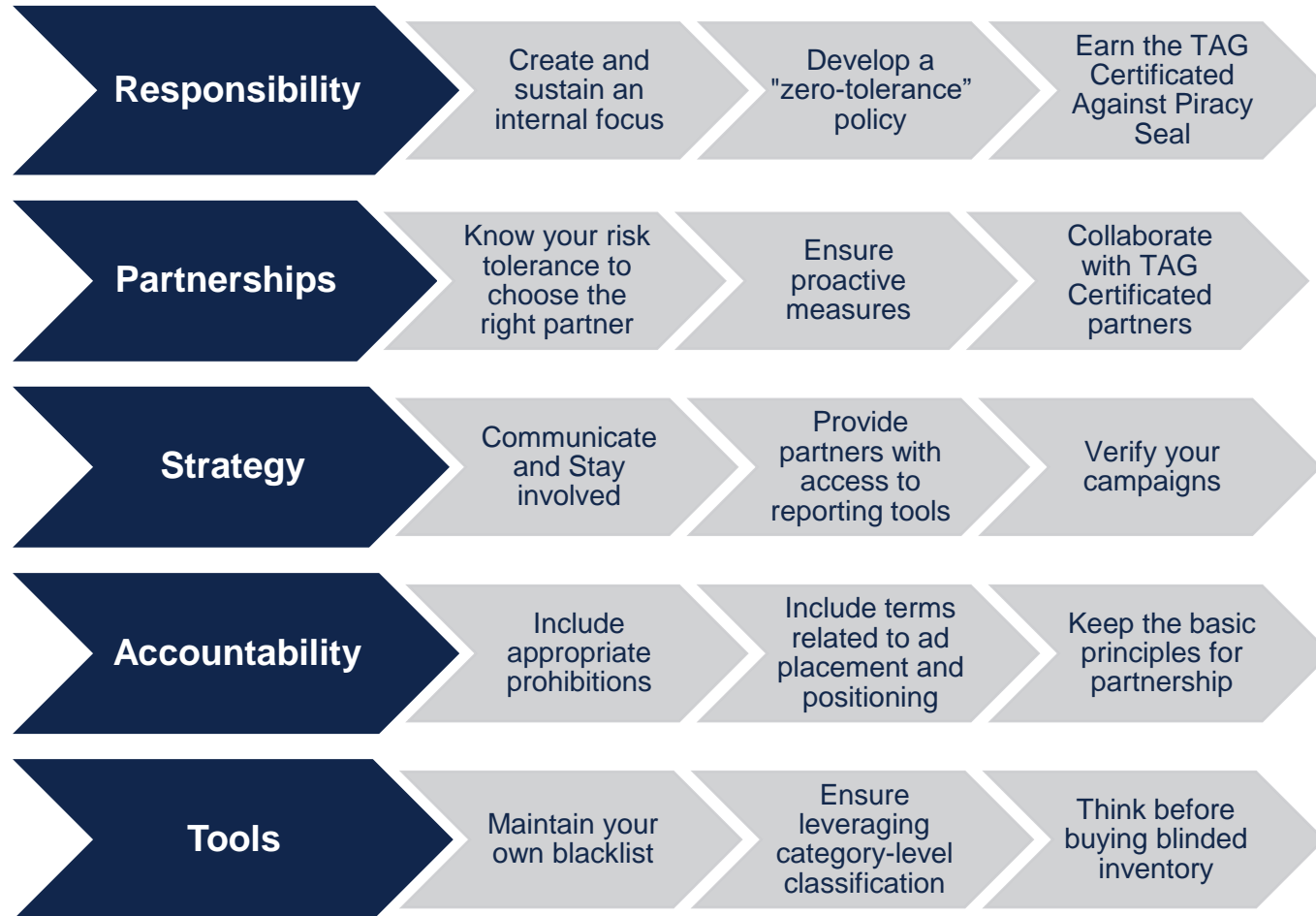
- Initiated by **European Commission**
- TAG CAP Program offers a mechanism by which companies can meet the **MoU's** requirements on online advertising and intellectual property rights (IPR) for their European operations








Impact

- Anti-piracy steps have reduced ad revenue for pirate sites by between **48 and 61 percent** measured by Ernst & Young in 2015
- **Prevention of \$102 to 177 Million** in potential earnings for pirate site operators

Using TAG certified programs and effective MoU's have reduced digital piracy by a significant percentage

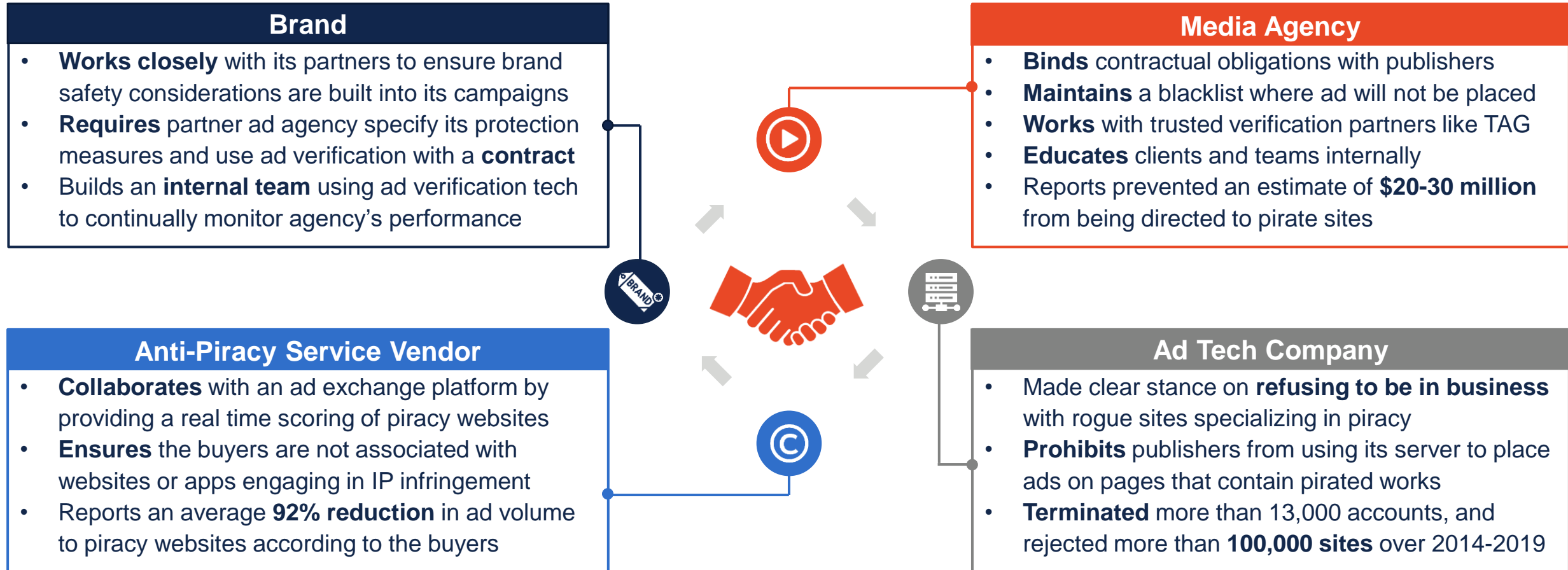
The actions marketers take to fight ad-supported piracy provide a roadmap of best practices



TAG Certified Against Piracy Companies		
Direct Buyer and Self-Attested Digital Advertising Service Provider (DAAP)		
		
Self-Attested Digital Advertising Service Provider (DAAP)		
		
		
		
Validated Digital Advertising Service Provider (DAAP)		
		
		
		

Brands can benefit from the best practices and choose the TAG certified partners to fight against ad-supported piracy

Fighting ad-supported piracy requires joint effort from every participant across the ad ecosystem



Signing legal contracts and collaborating with trustworthy partners are two popular effective measures to fight against piracy

Cybersecurity measures have evolved from ad verification to ad security



Fraud in digital advertising

- Ad fraud is alarmingly ubiquitous. If companies think ad fraud doesn't affect them then either it is almost certainly **the victim of digital advertising fraud** or may also, be an actual perpetrator or **enabler of digital ad fraud**
- May 2019 report of White ops proves substantial decrease in desktop ad fraud. However, **cybercriminals** see reduced profit opportunities in desktop ad fraud, they are **moving to other formats**



Investment of companies on Ad fraud

- With **no laws** against ad fraud, there's **no legal recourse** for advertisers. And with thousands of fraudsters out there, there are **too many** to track down and **block** on your own
- For most **cost is an issue**, the solution is out of their **price range**, some do not believe that the solution is as **beneficial** for the company while the rest do not see ad fraud to be as big of an issue



Evolution from Ad verification to Ad Security

- Ad verification and Ad security have a different **filtration approach**
- Ad verification typically relies on **IP blacklisting** to filter out bad traffic
- It is problematic in the sense that these IP lists age quickly and tend to **miss** a great deal of the **invalid traffic** out there
- Many of these lists, procured from third-party IP vendors are unvetted
- The ad security approach replaces the reliance on blocklists with **real-time user analysis**, based on **JavaScript challenges** to the user's browser
- If the user's browser declares their operating system to be iOS 10, a series of challenges will be sent to the browser with the aim of **triggering a response**
- The algorithm can tell if the user is on iOS 10, or if the **data** has been **manipulated**
- Ad verification takes **sampling** approach, by which they would only inspect a small portion of the traffic and make probabilistic assumptions based on that. Therefore, their scope differs
- The ad security approach, borrowing its philosophy from the **cybersecurity** and **bot mitigation industry**, mandates the real-time inspection of every single impression

White ops
Scope

2400
Campaigns

130K
Placements

606K
Domains

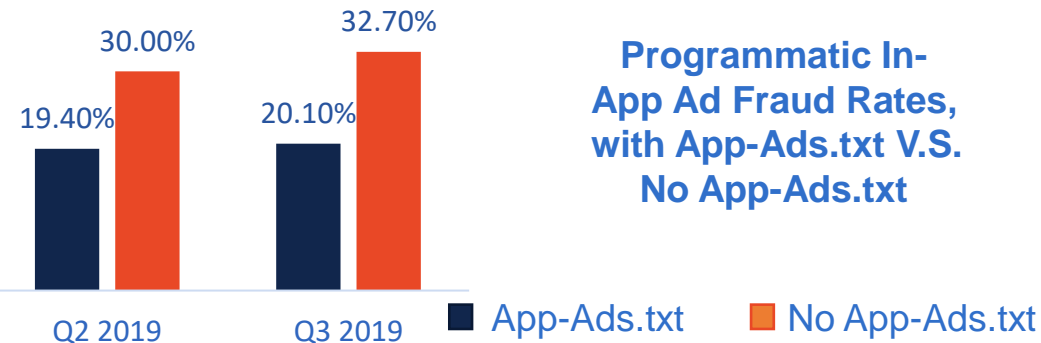
27B
Impressions

Due to ad fraud being omnipresent, it is essential for companies to focus on ad verification and ad security both having scopes different from each other

Inconsistent quality of monitoring ad fraud requires the industry to take more actions

Industry Actions

- Traffic sourcing more difficult and expensive within anti-fraud measures
- Traffic vendors **have gone further underground due to the TAG**, reducing “retail” bot buying on the open web
- Ads.txt has **reduced domain spoofing**
- TAG requires publishers to **have completed ads.txt files**
- More dollars being spent through programmatic platforms with built-in fraud prevention measures
- The alleged masterminds behind the **Methbot** operations **have been arrested**



Industry Limitations

Outdated Technology

- Uses outdated technology that permits **only low-fidelity validation**, like 1x1 pixels
- Prevalent with **video ads**

Walled Gardens (Large Ad Platforms)

- **Exerts more access control** over their platforms than publishers on the open web
- Hard to hold every publisher to **the same standard of validatability within user privacy**

Human Error

- Occurs during **implementation of the JavaScript tag**, like adding a JavaScript tag as a 1x1 tag
- Does not let the code fire properly execute

Intentional Evasion

- One of the **clearest indicators of fraud behavior**
- Silently drops fraud detection tags are often trying to hide something
- Blocks the solutions that cannot beat

The Industry applies structural improvements against ad fraud but the incredibly uneven auditability of ad campaigns across formats still needs to be fixed

Research shows that fraudsters are infiltrating the OTT industry with highly specialized ad scams

An overview of online ad fraud trends in 2020

Most prominent fraud types

- Non-viewable ads
- Non-existent installs
- Unwanted publisher ads
- Organic hijacking

Efficient combating techniques

- Viewability
- IVT detection
- Install verification
- In-app bot detection

Ad frauds in streaming video platforms

- Currently, **over 80%** of U.S. households are equipped with OTT devices and the demand is increasing exponentially
- Examples of OTT devices include Apple TV, Chromecast, Amazon Fire, Roku in addition to Smart TVs (Connected TVs) and gaming platforms
- The OTT ad market is estimated to reach **\$50 billion** by the end of **2020**
- However, sources reveal **more than 18%** of streaming video ad requests on OTT platforms are **fraudulent**
- Marketers have wasted **more than \$1.4 billion** on unauthentic OTT ads in **2019** alone and this number is predicted to **grow by 39%** in **2020**

OTT ad scams – a rising threat

- OTT uses **SSAI** for delivering video content and ads in a single stream
- SSAI makes viewing experience better but **decreases ad blocking efficiency**
- SSAI ads **don't run JavaScript** and traditional fraud tools don't have an effective way to track it in the same way as their services for mobile and desktop environments do
- 40%** of OTT ads are served using server-side ad insertion(SSAI)
- The most prevalent OTT frauds include **device-based** fraud, **app-based** fraud, geography **misrepresentation** and **domain spoofing**
- OTT scams initially started with **Roku** platforms (Monarch, Dicaprio)
- However, fraudsters have now started moving to **Amazon Fire TV** after Roku has started to aggressively crack down on these scams
- Factors such as **higher CPMs**, a **decentralized** ecosystem, a **lack of industry standards** and **increased CTV content demand** have made OTT a perfect breeding ground for new digital frauds

The increase in demand for OTT and CTV inventories along rising CPMs has created a perfect storm of opportunities for online advertisement fraud in this domain

Digital OOH is one of the top three growing marketing channels with the rise of fraud

\$2.72b

DOOH ad spend in 2020

\$3.84b

DOOH ad spend estimated by 2023

33%

DOOH accounts for **33%** of total OOH ad spending in 2020; and it will increase to **42%** by 2023

Major Players

- Lamar Advertising
- Prismview
- JCDecaux
- BroadSign
- Mvix
- Outfront Media
- Clear Channel
- DaKTronics
- oOh!Media
- NEC Display Solutions

Vendors working on traffic verification in DOOH advertising



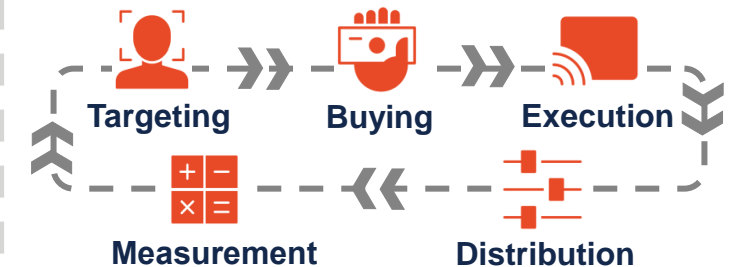
- Uses AI to combine **anonymized data** from over **150 million** monthly active users along with first- and third-party data
- Combines **location intelligence** with **real-time mobile data**
- Creates exposed and **control groups** to address biases
- Allows **programmatically plan, target, manage, and measure** DOOH ad campaigns



- Quality Impressions™** builds verification, optimization, and analytics solutions
- Develops a new industry standard, creates **clear, validated and standardized data** to assess OOH campaign delivery, across multiple formats, in close to real time



- World's 1st blockchain-powered DOOH** for Foodpanda across South East Asia
- Blockchain lets brands and advertisers gain **real-time visibility** of campaign performance, and **transparency** of the impression lifecycle
- ML process** to receive classified sensor data corresponding to **viewership measurement** of a digital media asset at a particular location to generate trained data



Experimental traffic verification and measurement technology are increasingly applied for programmatic digital out-of-home network which is believed to be a future vital component of OOH

Reflection on major ad fraud events bring forward takeaways for future preventions

3ve: Global sophisticated family of online fraud operations

3B

Daily bid requests

60K

Ad selling accounts

1M

Compromised IPs

10K+

Counterfeited websites






700K




Infections at a time

1K+

Data center nodes

3ve was jointly taken down by **Google, WhiteOps** and 16 other companies in **2018**

-  Mimicking human behaviors
-  Tag evasion
-  Regenerate IP addresses
-  Malware anti-forensics
-  No single point of failure

-  **Create and adopt industry standards**
Ads.txt file created by IAB Tech Lab helps to see authorized seller easily
-  **Be mindful and proactive about fraud**
Trust your intuition and check CTR to ensure the effectiveness of fighting fraud
-  **Use layered methodology to fight fraud**
Use both in-house defense and third-party verification to look for indicators of bots

ICEBUCKET: Largest CTV ad fraud scheme ever

2M

Impersonated IPs

1.9B

Impressions per day

300

Counterfeited publishers

1,700+

SSAI server IPs

30

Spoofed countries

300+

Different appIDs

ICEBUCKET's activity **peaked in Jan 2020** and was first identified by **WhiteOps**



Ensure working with a collectively protected ad supply chain



Add consistent appID declarations to provide stronger links to publisher



Consult with ad tech partners to ensure new threat are understood



Develop standards to increase transparency for CTV inventory

Conforming to industry standards and increasing awareness are ways to fight ad frauds with ever-growing size and complexity

SSAI is one of the predominant methods used to cause CTV and OTT frauds

	Trends in CTV Ad fraud	Techniques used by fraudsters to cause CTV fraud
Easy to commit	<ul style="list-style-type: none"> Fraudsters declare bots to be streaming devices Video ad impressions for CPM prices ten times higher than other forms of digital ads Impact of pandemic- Augustine Fou notes three large-scale cases of CTV fraud, caught and documented in 2020. Codenamed DiCaprio, Monarch, Icebucket were making millions of dollars 	<ul style="list-style-type: none"> SSAI, which is used in roughly 40% of OTT ad serving and can be seen in action via ICEBUCKET "Platform Mismatch," - fraudsters disguise mobile inventory as CTV ads to capitalize on the higher CPMs App ID spoofing - low-quality apps pretend to be something more premium to deliver the ads
Easy to hide	<ul style="list-style-type: none"> Impressions in CTV/OTT cannot be fully validated due to limitations of the technology. WhiteOps disclosed that video ads like these are only 1/3 "validatable at the highest level" SSAI - It much easier for data center bots to openly commit CTV fraud since it could be legitimate, until proven otherwise 	<p>38% of all programmatic OTT/CTV advertising use SSAI</p> <ul style="list-style-type: none"> Fraudsters cause fraud by faking all the associated HTTP header fields (X-Forwarded-For, X-Device-User-Agent, extensions) Scammers use machines to mimic SSAI proxy servers, and because bona fide SSAI is such a common practice in OTT/CTV, their schemes are often overlooked as harmless If advertisers blindly trust all SSAI integrations, then they put over one-fourth of their OTT/CTV budgets at risk
Easy to avoid	<ul style="list-style-type: none"> In order to not get scammed, making direct purchases is a good approach Work closely with reputable SSAI vendors to understand and validate their credentials Observe trends such as high video completion rates, spikes in traffic, number of devices, bid pricing 	

With the rise in CTV/OTT ad fraud, advertisers and publishers must keep an eye out for the trending approaches hackers are using and work on techniques to mitigate the issue

Research shows the emergence of a new type of app install fraud within the cost-per-install space

Attribution fraud is an **app install** fraud where **organic downloads** are **attributed incorrectly**, and it accounts for **54%** of all fraudulent installs

Mechanism of attribution frauds

- Clean publisher requests ads
- Ad Network sends high revenue campaign
- User clicks the ad shown by publisher
- Fraudster publisher sends a fraud click
- Credit assigned to fraudulent publisher
- No credit for the clean publisher
- Decreased motivation to select high revenue ads

Impact of attribution frauds

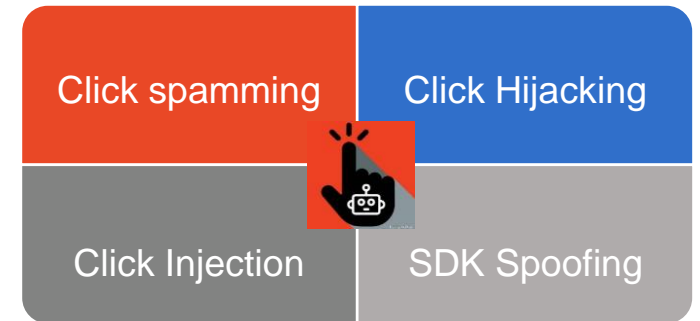
Fraudsters gaming the attribution systems have been costing **Airbnb millions of dollars** in affiliate commissions

From the top 10 sources of fraud listed by Airbnb's supply partners, **50%** were comprised of attribution fraud




The company pays about **\$1.5 million** in fraudulent commissions annually due to attribution fraud

About **8%** of Airbnb's demand campaigns and **5%** of its supply campaign conversions show "high attribution risk"

Types of attribution frauds











Ways to spot attribution frauds

-  High click volumes
-  Low click-to-install rate
-  High conversion rates

Attribution frauds are particularly difficult to detect since scammers here behave like typical organic users who in fact steal legitimate installs leading to credit loss from paid sources

Understanding mobile ad fraud operations will help get a better view of how to approach the solution

Mobile Attribution Flow	Mobile Ad Fraud Types	Common Fraudster Tools	Mobile Ad Fraud Indicators
<div>Ad Click</div> <div>↓</div> <div>Ad Network</div> <div>↓</div> <div>Recorded by Attribution Provider</div> <div>↓</div> <div>App Store</div> <div>↓</div> <div>App downloaded and launched</div> <div>↓</div> <div>Matched by Attribution Provider</div> <div>↓</div> <div>Ad Network Dashboard</div>	<div>CPI Fraud uses mobile malware to hijack attribution for an install</div> <div>Misbehaving SDKs executed by malware hidden on another app</div> <div>CPM Fraud apps loading ten of thousands of ads in the background</div> <div>Mobile Device Farm used for fraudulent clicks, mobile engagement, fake social media followings, etc.</div>	<div>Malware a software intentionally designed to cause damage to a device, server, or network</div> <div>Device Emulators created by game developers for a virtual device environment to test different app features</div> <div>VPN Proxy Tools routing the device internet connection through a chosen VPN's private server</div> <div>Android more malicious apps running in the Android operating system</div>	<div>Click to Install Time (10s < CTIT < 24h)</div> <div>New device rate</div> <div>Conversion rate</div> <div>Biometric behavior analysis with device sensors</div> <div>Limit ad tracking (only for Google and iOS identifiers)</div> <div>Artificial intelligence (applying fraud identification logic at scale)</div>

Getting familiar with common fraud tactics, technological tools, and industry vulnerabilities can help us turn the spotlight on internal and external initiatives for fighting against mobile ad fraud

Buyers and sellers need to be more meticulous of what they are buying and selling

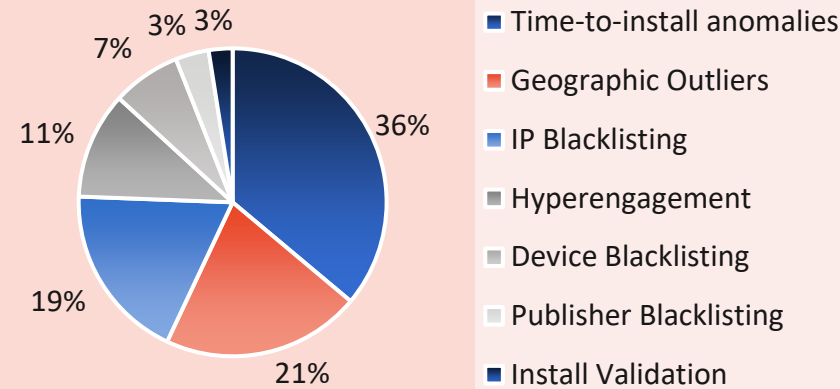


Industry leaders on Digital Ad fraud

- TAG works to fight advertising fraud by working with both the buy-side (advertisers and ad agencies) as well as the sell-side - **Mike Zaneis, CEO, TAG**
- We also work with leading fraud specialists, such as Forensiq, Protected Media, and Moat by Oracle Data Cloud, to ensure that we are actively deterring bad actor - **Sebastian Höft, Market Quality, Smaato**
- Joined industry initiative to get a clear view of the size of the problem and then take measures to erase it - **Arne Kirchem, OMW Representative**
- Rise in third-party auditors and Downward pressure from marketers - **Julius Ramirez, SVP Chartboost**

Study Shows 90% Less Fraud in TAG Certified Channels in U.S

Statistical models for detecting anomalies



Ways to Combat Ad fraud

Employ Ad Verification Tools

Leverage Big Data Analytics

Use Ads.txt

Measure Conversions Not Clicks

Don't Rely on a Machine

Use Trusted Platforms

Embrace The Defensive Buying Mindset

Setting Dashboard up and not monitoring

Keeping legal team in loop

Discrepancies Between Clicks And Visits

Monitoring Suspicious actions

Implement IP Blacklists On Google Ads

Monitor Traffic Spikes Or 'Clusters'

Set Up Real-Time Reporting

Switch Your Bidding Proposition To Conversions

Be Conscious Of Budget Allocations

Ad fraud detection methods

It is essential for the ad fraud industry to focus on emerging detection models, recurrent errors, statistical models and the views of experts with domain knowledge to combat and reduce fraud

Advertisers are relying on blockchain to improve the detection of unscrupulous digital ad activity

Limitations of the current digital ad model

Ad buyers

- **Lack of trust** in publisher reported impressions
- Rising **customer expectations**
- Justifying **ROI** and **spends** associated with frauds
- **Complexity** in choosing the **best media mix**

Publishers

- **Lack of transparent metrics** for ad buyers
- **Credibility loss** with B2B and B2C customers
- Risk of compromising the **ad buyer's brand** health
- **Tremendous efforts** to sell digital ad products

Consumers

- **Irrelevant ads** leading to a **poor experience**
- **Lack of control** over personal data
- **Reduced trust** in online content due to fake media
- **Frustration** in the online experience
- **Lack of education** on the benefits of advertising

Using blockchain for innovating digital ads



Distributed Ledger Technology with multiple security layers to host smart contracts and automate transactions



Automated algorithms to guarantee integrity and authenticity



Cryptography to secure verified records and allow access to authorized users only



Immutable data structures ensure tamper-proof records through individual, customized dashboards



Enabling customers to react to ads and provide demographics for **personalized targeting**



Smart contracts to **determine automatic payments** and offers digital tokens

Barriers to blockchain adoption



Regulatory uncertainty



Lack of trust among users



Ability to collate networks



Separate blockchains unable to work together



Inability to scale



Intellectual property concerns



Audit and compliance issues

By incorporating vigilant data governance standards, companies can increase users controls over their online identities to boost their confidence and ensure advancement in the digital advertising industry

Reviewing current trend and listening to experts' advice prepare us better for future ad fraud threats

Trend: 2019 WhiteOps Bot Baseline Report



IVT sourcing is declining in general

- **Less sophisticated** cybercriminals have **abandoned** their fraud schemes due to narrowing profit margin
- Ad fraud evolves persists in **new, creative forms**

Frauds are shifting to new frontiers

- Fraud volume in desktop was at **historic low**
- **Mobile, OTT and CTV** are fields witnessing higher ad fraud

Industry coalitions shine new light

- The adoption of **ads.txt** in 2017 effectively curbed domain spoofing
- Most video ads today still **don't support VAST 4**, which is the new gold standard in transparency

Recommendations from WhiteOps



Adopting latest industry standards

- Work with vendors who have implemented **ads.txt**
- Continue to advocate for **JavaScript and VAST 4** support, compatibility, and implementation

Require transparency from partners

- Ask how your vendor **measures** invalid traffic
- Set **fraud goals** early and frequently discuss with your partners if goals are not met

Include non-IVT traffic in your contract

- Insist that your company will **only pay for non-SIVT** or non-IVT impressions
- "Final numbers to be actualized based on **third-party reported non-SIVT impressions**"

Point of views from Dr. Augustine Fou

CTV ad fraud schemes in 2020



Enemies are trickier and evolving

- Fake ads.txt, renting legit ads.txt from co-conspirators are ways to **bypass the inspection**
- New schemes are being discovered **one after one**

MRC, TAG are not silver bullets to ad fraud

- "**Self-attested** certifications where firm's complete paperwork, pay the fee and earn the plaque"
- A few TAG certified companies committed ad fraud

Insist on your own visibility an into traffic

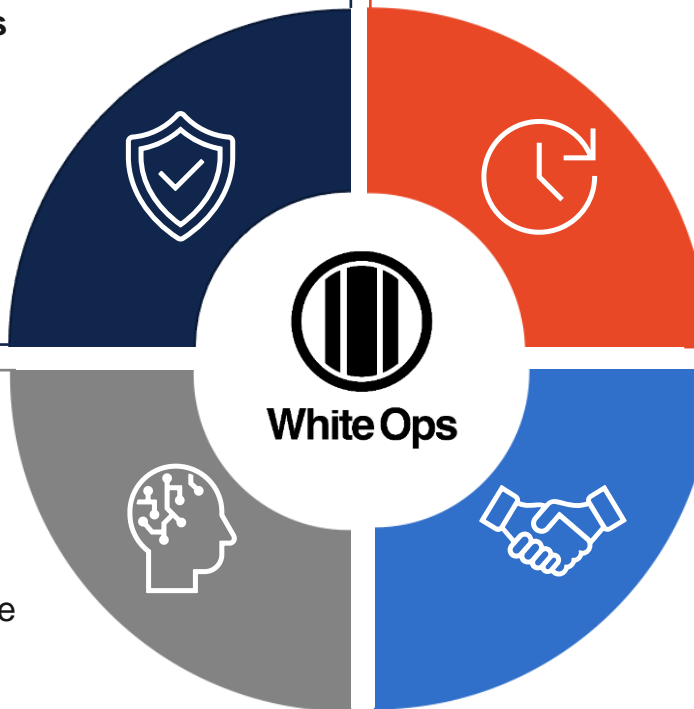
- Have the right analytics, **see the data** and block the defrauding sites and apps yourself
- **Black-boxed** verification vendors (e.g., IAS, DV) may be **harder to provide proof or valuable insights**

The ongoing game between fraudsters and verification companies might reduce in overall scale but intensify in complexity

White Ops is pioneering the market of ad fraud with its ambition of staying ahead

Multilayer and Full Protection

- Provides full visibility and services for both **SSPs** and **DSPs**
- Enables to gather data on the **network, device, software, application, and user configuration** to detect technical evidence of compromise
- Covers multiple media environments: **Video, Mobile, Display, OTT, and CTV**



Continuous Adaptation for Future

- Continuously adapted over the last 7+ years, speeding to **identify and build new detection mechanisms** more than other solutions that are built on fixed detection mechanisms
- Releases advanced research reports and analytics for **fraud evolutions and future trends** in Mobile app and CTV ad fraud

Global Treat Intelligence

- Specializes in threat hunting, malware reverse engineering, and threat modeling by the **Satori Threat Intelligence and Research Team**
- Analysts proactively **hunt for new threats** on the internet, **attributing threats** to specific botnet operators, campaigns, and other threat actors
- Identifies sophisticated bot traffic and major global ad fraud events (**e.g. 3ve, ICEBUCKET**)

Ideal Partnership for Collaboration

- Has **established partnerships** with MediaMath, P&G, LAND O'LAKES, etc. and received affirmation for its outstanding service performance
- Wins **eight 2020 Cybersecurity Excellence Award** and be recognized by the industry and experts
- Comparatively small market share (**<0.1%**) with high growth prospects

Amongst all other competitive vendors, White Ops is standing out providing full and developing solutions for bot detection and mitigation, thus could be an ideal asset for the client

Interview with the expert: solving the situations below to get back to the real digital marketing

Overview of the current situations



- Middlemen: Get **more revenue and volume**
- Marketer: Buy **massive quantities impressions** with **lower cost**



- Bots can **get by the detection**
- Bots can **trick the measurement**, and **block the detection tag**



- **Outsource** algorithms to **low-wage humans** to solve captures



- Fraudsters focus on where **the ad budgets** spent on and **shift from channels to channels**



- **Distract advertisers on the fraud** by focusing on **the brand safety**

“

White Ops is probably **one of the few actual credible ones** and that is because they are actual hackers themselves and they **focused on the ad fraud that is caused by malware on devices.**

”



Dr. Augustine Fou

Dr. Fou's recommendations for the future

- Marketers can **investigate the analytics themselves** rather than rely on others to reduce the fraud
- Marketers can **turn off the ad spends gradually** to see if there is **any change on business outcomes**
- Marketers can be **corporate with the real credible cybersecurity firm** to against the ad fraud

Fraudsters are getting more adaptive and sophisticated that expert suggests marketers to take actions to avoid the loss

Thank You