For Ad Tech
For Mobile Ad Fraud
**MediaGuard** delivers robust fraud detection and prevention capabilities to verify the humanity of advertising efforts across all channels. Our unique methodology, proprietary technology, unmatched scale and proven experience allow us to more accurately detect and prevent today’s dynamic and polymorphic bots. We keep Mobile Advertising human.

Customers are increasingly engaging with mobile platforms, attracting advertisers and fraudsters alike. High CPMs and varied platform environments have made mobile ad fraud difficult for advertisers to conquer. **HUMAN** protects and prevents fraud within both mobile web and mobile app environments in real-time.
Use Cases

Passive Mitigation
Monitor activity from humans, good bots, and malicious bots across their advertising impressions. This enables you to gain insights into the quality of their inventory and take necessary actions with suppliers.

Self Monitoring & Reputation Protection
Proactively monitor for sophisticated bot activity within digital advertising efforts to maximize ad spend and ensure campaigns are only reaching humans.

Active Mitigation
Improve inventory quality and reputation strength with demand partners by actively preventing invalid traffic across desktop, mobile web, mobile app, and CTV environments in real-time before a bid is ever made on an impression to strengthen reputations with demand partners.

Monitor Supply Sources
Monitor activity from humans and malicious bots across digital impressions to gain insights into inventory quality and take necessary actions with suppliers.

Improve Inventory Quality
Actively prevent invalid traffic across desktop, mobile web, mobile app, and CTV environments in real-time before a bid is ever made on an impression to strengthen reputations with demand partners.

Self Monitoring & Reputation Protection
Proactively monitor for sophisticated bot activity within digital advertising efforts to maximize ad spend and ensure campaigns are only reaching humans.
Prevalent Mobile Threats

Automated browsing
Device activity simulated repeatedly, also known as click farms.

False Representation
Ad requests driven to fake devices or apps masquerading as a bigger, more popular app.

Misleading Interfaces
Apps disguised as something benign while infecting a device with malware.

Undisclosed use of incentives
Activities on ads driven by hidden motivators.
Fighting fraud is not just a feature

**Unmatched Scale**
Seeing 10 trillion transactions each week and more than 400B mobile requests per month provides HUMAN with unmatched intelligence into sophisticated mobile bot fraud.

**Dedicated Intelligence**
Mobile threat intelligence analysts, with specialties in threat hunting, malware reverse engineering, and threat modeling, help HUMAN stay ahead of mobile fraudsters.

**Unrivaled Detection**
Continuously adapting, mobile-specific algorithms - based on signals not lists - allow HUMAN to quickly identify and build new detection mechanisms.

**Flexible Implementation**
Easily deploy within any technology stack through JavaScript tag, SDK, or 1x1 pixel to protect against a host of mobile threats.

---

Media Rating Council accreditation for detecting sophisticated invalid traffic (SIVT) within Display and Video Impressions for Mobile Web and Mobile App
Mobile ad fraud in action: Terracotta

Sometimes hope can get the better of reason, especially when it comes to offers like a free pair of shoes for simply downloading an app. However, as with many traditional malware lures, this hope is being exploited by a family of Android apps to distribute a novel new ad fraud botnet. The HUMAN Satori Threat Intelligence & Research team identified and has been actively defending against the attack—which we’ve codenamed TERRACOTTA - that systematically misrepresented its inventory as being from apps that hadn’t implemented app-ads.txt.

“Due to our collaboration with HUMAN investigating the TERRACOTTA ad fraud operation, their critical findings helped us connect the case to a previously-found set of mobile apps and to identify additional bad apps. This allowed us to move quickly to protect users, advertisers and the broader ecosystem – when we determine policy violations, we take action.”

Google Spokesperson
About Us

HUMAN is a cybersecurity company that protects enterprises from bot attacks to keep digital experiences human. We have the most advanced Human Verification Engine that protects applications, APIs and digital media from bot attacks, preventing losses and improving the digital experience for real humans. Today we verify the humanity of more than 10 trillion interactions per week for some of the largest companies and internet platforms. Protect your digital business with HUMAN. To Know Who’s Real, visit www.humansecurity.com.
Know
Who’s Real