

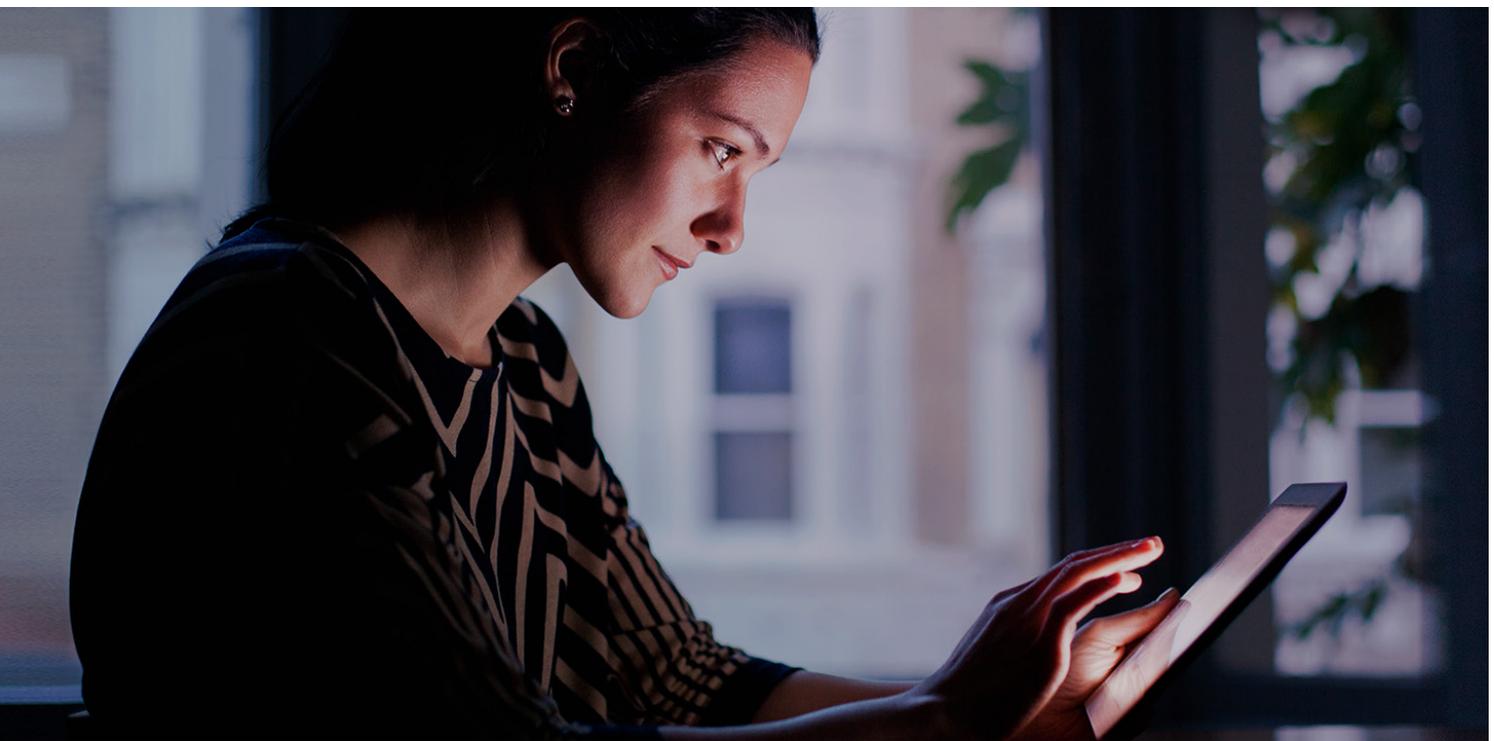
 **HUMAN**

For Mobile





HUMAN is a cybersecurity company that collectively protects global enterprises and internet platforms from digital fraud and abuse. Sophisticated bots look and act like humans when they visit websites, fill out forms, take over accounts, scrape information, and commit payment fraud creating billions of dollars in losses for brands and consumers. The Human Verification™ Engine is powered by our multilayered detection technology combining technical evidence, machine learning, threat intelligence and continuous adaptation and solves top enterprise pain points.



Varied platform environments and increased spending have made mobile fraud attractive to bad actors but difficult for advertisers to conquer. HUMAN protects and prevents fraud within both mobile web and mobile app environments in real-time. We keep mobile human.

Use Cases



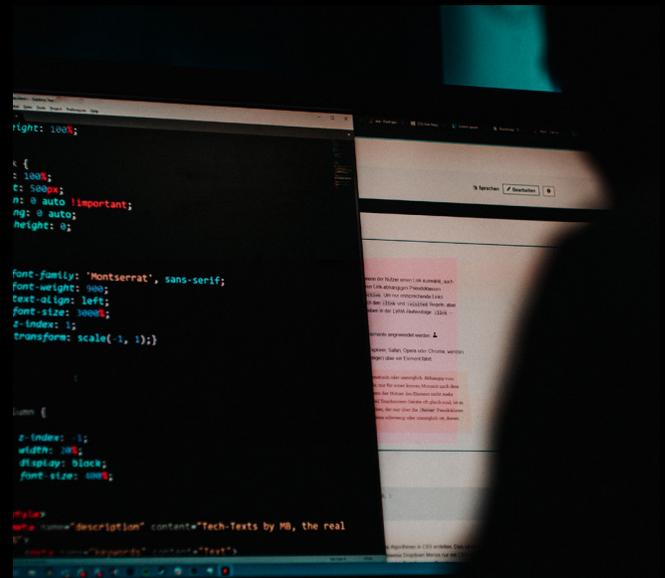
Advertising Fraud

Platforms and Publishers improve mobile inventory quality and drive increased revenue from demand partners by actively preventing bids on non-human interactions.

Advertisers and Agencies proactively monitor bot activity within digital advertising efforts to maximize mobile ad spend and ensure campaigns are only reaching humans.

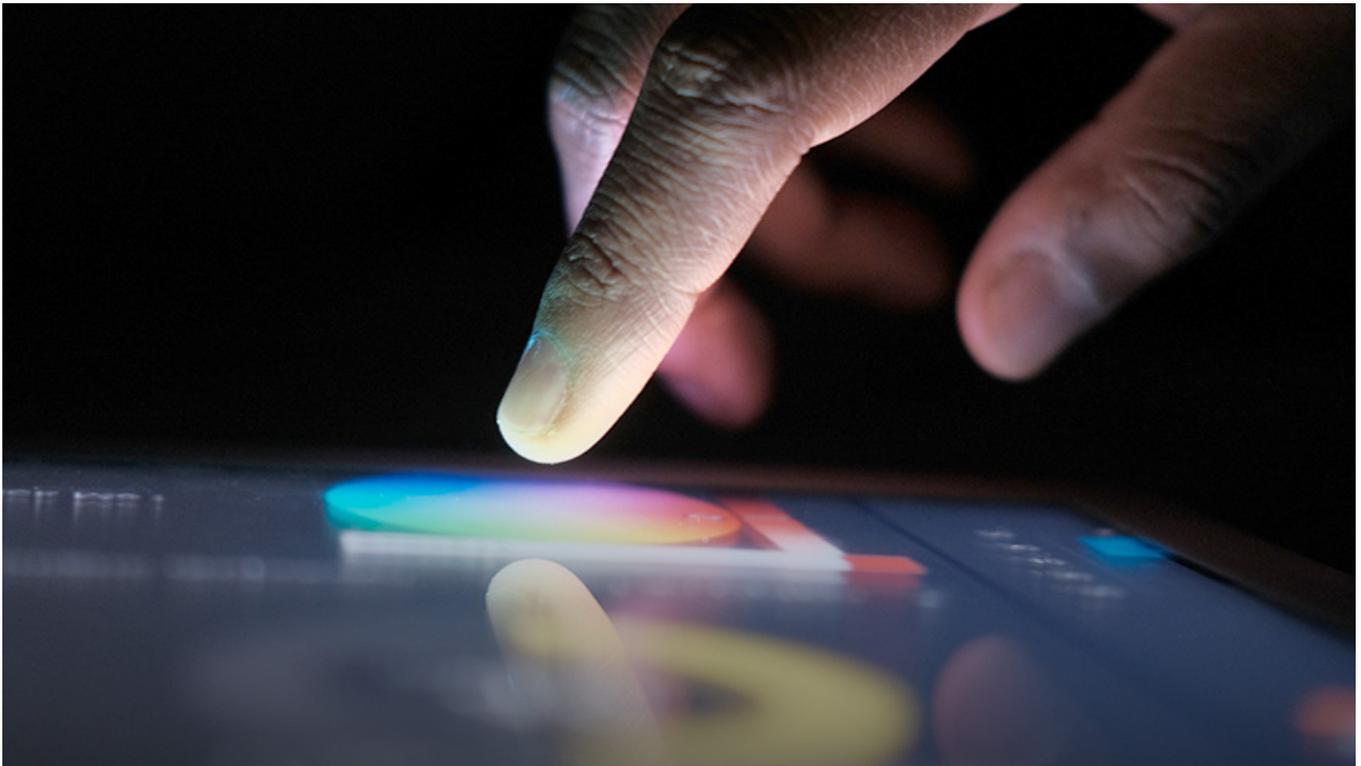
Marketing Fraud

Brands protect mobile marketing efforts from digital fraud and abuse including application install attribution fraud and in-app click fraud.



Application Fraud

Enterprises protect native mobile applications from digital fraud and abuse including account takeover attacks, new account fraud, and sensitive data scraping.



Prevalent Mobile Threats

False Representation

Bad actors drive ad requests to fake devices or apps masquerading as a bigger, more popular app to steal advertising spend.

Misleading Interfaces

Mobile apps disguised as something benign that infect a device with malware to run a host of fraudulent activity.

Fake Installs

Attribution fraud from networks or affiliates using bots to derive false credit for installs they did not drive in order to earn the payouts.

Device Farms

Collection of actual physical devices run by bots to create fake user identities and actions that emulate human traffic.

Device ID Reset

Fraudsters reset mobile device IDs to allow for repeat installs of apps on the same device, each triggering a new device install credit to drive fraudulent install incentives payouts.

In-App Click Generation

Bots leverage advertisers' in-app advertisements to deliver credit for app opens and clicks inside the app to bad actors.

In-App Account Takeover and Abuse

Bots that take-over user accounts using credential stuffing or credential cracking and perform fraudulent purchases and other fraudulent transactions or abusive interactions.

Mobile Attribution and Engagement

Bot or device farm-driven installs and engagement sessions designed to fraudulently drive cost-per-engagement (CPE) payouts to malicious networks and app install affiliates.

Fighting fraud is not just a feature



Unmatched Scale

Seeing 10 trillion transactions each week, with more than 60% of those as mobile requests, provides HUMAN with unmatched intelligence into sophisticated mobile bot fraud.



Unprecedented Accuracy

Monitoring a payload of over 2,500 unique technical tests provides real-time, deep, and accurate visibility into activity from humans and bots, good bots and malicious bots, even from within the same device on every transaction.



Flexible Implementation

Easily deploy within any technology stack through JavaScript tag, Software Development Kit (SDK), or 1x1 pixel to protect against a host of mobile threats.



Dedicated Intelligence

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



Collective Protection

Working together with over 250 clients worldwide, including some of the largest internet platforms, HUMAN has developed a community knowledge bank to more broadly fight fraud within the ecosystem.

HUMAN Mobile Software Development Kit (SDK)

Native to the mobile environment, the HUMAN Mobile SDK delivers unique fraud detection capabilities across both iOS and Android mobile applications. An easy and flexible design allows for integration into any application without affecting user experience or the application's performance in any way. With the SDK, bad actors' techniques can be identified with greater precision.



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.

The HUMAN Satori Threat Intelligence & Research team identified and has been actively defending against the attack

“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

Human Verification™ Engine

Collect Signals

Signal Evasion
Custom Data
Network
Device

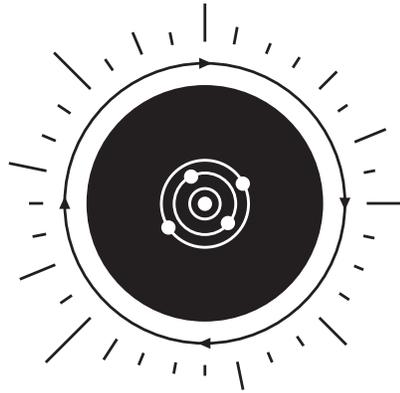


Technical Evidence



Continuous Adaptation

Decision Engine



Classify Events

Bot
Nonstandard
Valid

Global Threat Intelligence



Machine Learning



JavaScript or SDK

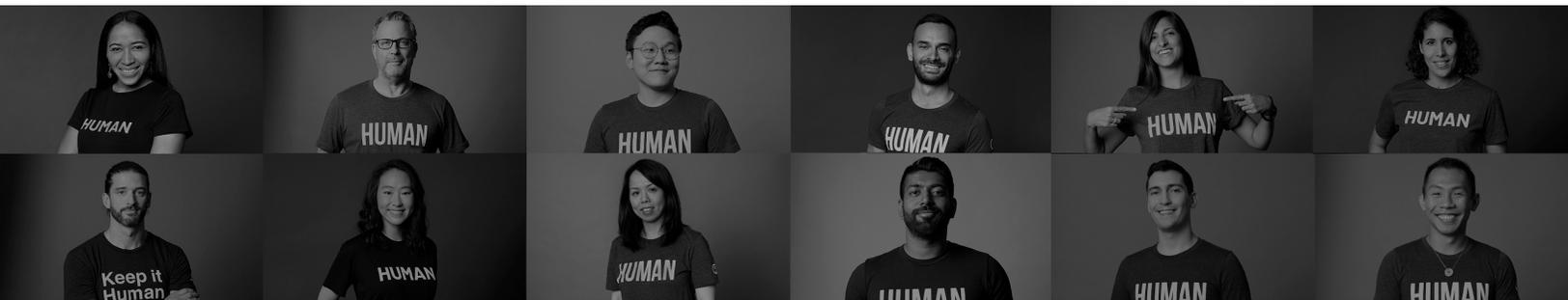
Client



Server Integration

Mitigation

Allow - Delay - Block - Deceive



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

