HUMAN

Stop Spoofing, Increase Revenue

Safeguard the digital advertising ecosystem by preventing faked requests from costing everyone money

Even the Most Premium and Secure Platforms Can Be Spoofed

Despite the fact that many mobile and CTV platforms operate in closed systems, spoofing can occur outside of the control of individual device stores, app publishers, or media owners. This fraud technique fakes the true origin of ad requests in order to attract valuable advertisements from brands.

Impersonating devices, apps, or even the servers inserting ads enables fraudsters to fake the entire system in order to steal from it. When fraud enters the digital advertising ecosystem it steals more than just ad dollars. It undermines the trust and relationships between all parties - demand partners, ad tech platforms and supply partners alike.

Protected Attack Surfaces

DESKTOP | MOBILE WEB | MOBILE APP | CONNECTED TV (CTV)

Prevent Device, App and SSAI Spoofing

Developing shared standards and more accurate device identification, as well as collective protection, allows HUMAN clients and partners to stay ahead of bad actors to protect their valuable digital advertising investments.MediaGuard is the industry leading solution protecting more than 85% of the total global programmatic impressions that delivers collective protection for the ecosystem from disruptive ad fraud.

MediaGuard uses a multilayered detection methodology that establishes hard technical evidence to prove fraud. This enables MediaGuard to detect and mitigate today's sophisticated bots and advanced spoofing techniques with unmatched scale, speed, and precision to ensure that only real humans are interacting with your digital advertising activity.

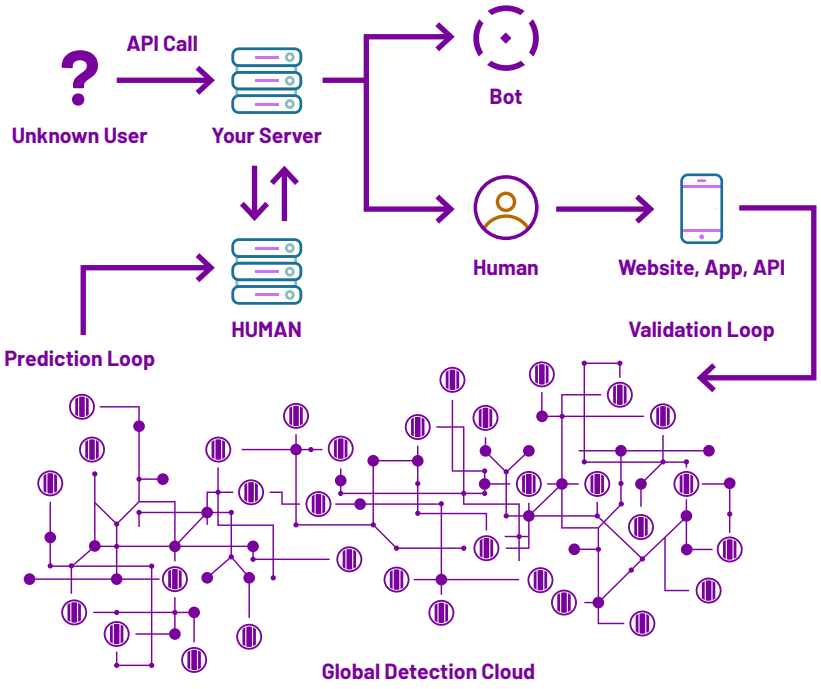
Pain Points

Spoofed Origin Identity
Fraudsters faking their true identity to look like something they are not leaves loss in their wake.

Evolving Threats
Constantly modifying their fictitious identities to mask their genuine origin identities enables bad actors to circumvent preexisting security measures.

Diminished Revenue
Spoofed ad requests steal revenue from ad platforms and media owners while also putting the entire ecosystem at risk of losing valuable earnings.

How MediaGuard Works



The HUMAN MediaGuard Advantage

Increase Trust

Serve Ads to Real Humans

Prevent fraud in pre-bid environments across desktop, mobile and connected TV (CTV) to improve demand partner trust in programmatically traded media.

Improve Quality

Strengthen your Reputation

Eliminate fraud before it enters your platform with greater transparency of supply and stop wasting resources - time, people, technology and money - on remediation and clawbacks.

Optimize Return

Gain Control and Maximize ROAS

Deliver only verified human impressions for more valuable and better performing inventory to gain increased value and revenue from demand partners.

Powered by the Human Verification Engine™

MediaGuard is powered by the Human Verification Engine, which combines technical evidence, machine learning, and continuous adaptation to deliver 'human or not' decisions with unmatched scale, speed, and precision to safeguard your applications and services.

Every week, we verify the humanity of over 15 trillion interactions by leveraging our distinct observability advantage established by analyzing over a decade's worth of data to provide continuously adaptive and collective protection to our customers, who include the world's top internet platforms.

Our Satori Threat Intelligence and Research Team takes down multiple large-scale attack networks every year, proactively identifying and reverse engineering new threats to inform our detection techniques with new indicators against emerging automated attacks.