HUMAN

Replay Without Spin Fraud

HUMAN helps security and fraud teams banish artificial streaming from their platforms

Prevent cyber criminals from cashing in on your revenue sharing model

Spin Fraud, also known as Artificial Streaming Fraud, occurs when an artist, studio, or marketing agency acting on their behalf employs automated bots to increase the number of song or video plays on a particular streaming platform. In other instances, fraudsters upload fake or stolen content to drive manipulated streaming traffic to albums and playlists, allowing them to also profit from unearned royalty payments. In addition, when streaming platforms offer an ad-supported freemium model, unscrupulous advertisers are unintentionally incentivized to game the system using automated bots.

As the popularity of streaming content grows, malicious actors continue to see an opportunity to profit by manipulating these marketplaces. Streaming farms, for example, inflate the number of times a song or video is played or watched by creating free accounts or taking over existing paid accounts when real human subscribers are not consuming content. These bots affect revenue and degrade the customer experience by returning misinformed recommendations from algorithms designed to surface trending or personalized content.

Risks Addressed

ACCOUNT CREATION

ACCOUNT TAKEOVER

SPIN FRAUD

Safeguard Against Spin Fraud

Sophisticated bots behave like real users and are designed to evade detection. As a result, streaming platforms find it increasingly challenging to defend against spin fraud generated by automated attacks. A sophisticated bot can imitate human behavior using mouse movements, keystrokes, and fake browser behavior, using your streaming service as you intended. As a result, traditional application security solutions that rely on behavioral monitoring or static lists to detect bots are increasingly side-stepped. BotGuard for Applications combines superior detection techniques that, amongst other things, look for markers, signals, and patterns that indicate spin fraud. Utilizing HUMAN's observability advantage and hacker intelligence to make human or not decisions with no impact on page load times or end-user friction. We can mitigate today's and tomorrow's sophisticated bots with scale, speed, and precision.

Pain Points

Evolving threats

Novel attacks use thousands of devices in streaming farms to mimic human behaviors to access your platform and content that simple security measures cannot counteract.

Increased risk

New Account Fraud and ATOs put your users and your business at risk by exposing PII, preventing account access, and allowing attackers to perform artifical streaming fraud.

Not all growth is good

When fraudsters create many fake accounts, your streaming services can become a platform to validate stolen credit cards, hide spin fraud attacks, and encourage ad fraud.

Benefits to Your Business

Optimize Return

Deliver streaming services to verified human users for improved revenue performance and royalty distribution to genuine content creators.

Prevent Account Fraud

HUMAN's modern defense strategy keeps fake sign-ups from contaminating your customer account database while providing friction-free access to your real users.

Mitigate Risk

Gain peace-of-mind that your platform is protected against the risk of Spin Fraud by using BotGuard's industry-leading detection and precision with minimal added friction.

The HUMAN Botguard Advantage

Secure Accounts

For Real Humans Only:
Protect customer logins and new user registrations from account takeover attacks and PII harvesting while lowering captcha and multi-factor authentication friction for real humans.

Reduce Fraud

Prevent crime before it is committed:
Stop sophisticated bot attacks such as credential stuffing and cracking, which enable payment and wire transfer fraud,sensitive data theft, and other costly fraud-related losses.

Optimize Efficiency

Gain control and minimize losses:
Actionable insights help you reduce manual workflows and customize mitigation policies and responses to detect and prevent unwanted bot traffic from consuming time and infrastructure resources.

Powered by the Human Verification Engine™

BotGuard for Applications 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.