HUMAN

Prevent Content Manipulation

HUMAN helps security and fraud teams prevent fake comments and reviews from bots

Content Manipulation

There is such a thing as bad publicity.

Bots create fake accounts on social media platforms, forums, and email services, and they'll attempt to disguise their activity to make it appear like real user behavior. Creating a user account is simple: provide minimal details (such as name, email address, and password) and fraudsters will program their bots to fill out forms automatically and evade any CAPTCHA deterrents you have deployed. What's more, because the bot is using your app as intended, WAFs don't help.

When the sophisticated bot has accounts and access to your platform, it starts sending out unpleasant or unwanted messages, contaminating your users' experience. Furthermore, bots can also harvest email addresses, phone numbers, and personally identifiable information (PII). They scan the web, scrape contact information, and then deliver this data to the criminals to provide targets for their spam or cause you a costly data breach.

Risks Addressed

DISSATISFIED CUSTOMERS

REDUCED EFFICIENCY

COMPETITIVE ABUSE

How HUMAN Prevents Content Manipulation

Sophisticated bots behave like real users and are much better than earlier generations of bots at evading detection. As a result, businesses find it increasingly difficult to defend applications from automated attacks. A sophisticated bot can imitate human behavior using mouse movements, keystrokes, and fake browser behavior even when applications work as intended.

As a result, traditional application security solutions that rely on behavioral monitoring or static lists to detect bots are increasingly side-stepped. Unlike competing solutions, BotGuard uses a multilayered detection methodology that establishes hard technical evidence to prove fraud; This enables BotGuard to detect and mitigate today's sophisticated bots with unmatched scale, speed, and precision to ensure that only real humans are interacting with your applications.

The Challenge

Don't lose customer trust

Content tampering can ruin customer experience, drive people away, and cost you money. Customers lose faith in your app when bots spread fake news and reviews.

Bots waste resources and money

Sophisticated bots generate unnecessary traffic that slows down your app, raises your infrastructure and service expenses and wastes your product team's time.

Your WAF is not enough

Novel attacks use thousands of residential devices mimicking human behaviors to interact with your content that conventional security measures cannot counteract.

Benefits to Your Business

Stop Competitive Assaults

BotGuard's page load protection stops bots from accessing pages at scale and scraping content, protecting your pricing information and valuable data from theft and abuse.

Prevent PII harvesting

On protected pages, bots are blocked and can't harvest confidential information safeguarding your platform from a costly and brand damaging data breach.

Mitigate Risk

Gain peace-of-mind that your site is protected against the risk of scraping and PII harvesting by BotGuard's industry-leading detection precision and with minimal adde 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 combining technical evidence, machine learning, and continuous adaptation to deliver 'human or not' decisions with industry-leading accuracy, and minimal user friction.

We verify the humanity of 15 Trillion interactions per week, harnessing internet scale visibility and a decade of data to deliver continuously adaptive and mutually reinforcing protection to customers including the largest 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 attacks.