HUMAN

Prevent Content Scraping

HUMAN helps security and fraud teams stop web scraping and personal information harvesting

Content Scraping and PII Harvesting

Is your site crawling with bad bots and vulnerabilities?

Web scraping isn't always bad, and good bots continually crawl websites to capture pricing data and product descriptions. Platforms like search engines and insurance comparison sites aggregate scraped data to make it easy for humans to find the information they're looking for. However, malicious bots are also crawling your site and scraping your content with more sinister motives, using it to compete unfairly with your business or selling it on the dark web to criminals.

Fraudsters harvest PII by exploiting vulnerabilities in JavaScript or other code used to build websites and web applications. Software developers often use off-the-shelf code to add new capabilities and features to apps and websites. This approach can introduce unintended vulnerabilities that allow your adversaries to inject malicious code into your website, particularly where a vulnerability is well-known.

Risks Addressed

COMPETITIVE ASSAULTS

PII HARVESTING

SERVICE ABUSE

How HUMAN Prevents Content Scraping

Sophisticated bots behave like real users and are designed to evade detection. As a result, businesses find it increasingly challenging to defend applications from these automated attacks. A sophisticated bot can imitate human behavior using mouse movements, keystrokes, and fake browser behavior using your applications as you intended. As a result, traditional application security solutions that rely on behavioral monitoring or static lists to detect bots are increasingly vulnerable to abuse.

Unlike other solutions, BotGuard for Applications combines superior detection techniques, internet-scale observability, and hacker intelligence to make bot or not decisions with no impact on page load times or friction on end-users. With this scale and speed, we can mitigate today and tomorrow's sophisticated bots.

The Challenge

Rivals covet your customers

Unscrupulous profiteers use price scraping bots to undercut your prices, and content scraping bots are used to steal your content and your customers' sensitive data

Data scraping damages trust

Successful attacks can result in stolen sensitive data, causing customers' trust in your platform to erode, driving their business elsewhere, and costing you revenue.

Your success invites attacks

Scraped duplicated content hurts SEO rankings. Worse, the more successful your company grows, the more likely it is you will be attacked by a competitor.

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.