HUMAN

Prevent New Account Fraud

HUMAN helps security and fraud teams detect and stop fake account creation to safeguard your customer database

New Account Fraud

You want account creation to be easy for humans. But is it also easy for bots?

Sophisticated bots can quickly and easily create large numbers of fake new user accounts. The accounts are either completely fake or are created using details where the real human is unaware of the fraud. These new phony accounts are then used to carry out malicious activity, such as payment fraud, special offers and discount abuse, and spam and misinformation spreading.

Creating a new account needs to be quick and easy, so your prospective customer isn't frustrated and lost. You want users to create accounts to provide offers and discounts and ensure they become long-term clients. Customer accounts also help you monitor customer behavior enabling you to make sound business decisions. However, sophisticated bots can use that same easy system to register new account after new account to use for their cybercrimes.

Risks Addressed

- PLATFORM REUSE FOR FRAUD
- SKEWED METRICS
- ACCOUNT RESELLING

How HUMAN Prevents New Account Fraud

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 side-stepped.

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

WAF is not enough

Novel attacks use thousands of residential devices to mimic human behavior that conventional security measures cannot counteract.

Not all growth is good

New accounts are a positive sign of growth. But if left unchecked, they can lead to account creation anomalies contaminating your customer database and causing long-term problems.

Do criminals now own your platform?

When fraudsters create many fake accounts, your application can become a platform to validate stolen credit cards, hide credential stuffing attacks, and abuse customer discounts.

Benefits to Your Business

Prevent New 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 customers.

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 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 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.