HUMAN

Prevent Payment Fraud

HUMAN helps security and fraud teams prevent dishonest financial transactions

Payment Fraud

Without advanced protections, your site becomes a gift to fraudsters.

In payment fraud attacks, cybercriminals use sophisticated bots and lists of stolen credit card details on e-commerce sites to buy goods to then sell for a profit. Carding attacks focus on abusing the checkout page with stolen credit card information.

Criminals buy the lists of stolen credit card numbers, including security data such as CVV values, on criminal marketplaces. They then initiate bot attacks to test their cards by attempting small purchases to build a list of valid cards. When they've proven the card details are valid, the fraudsters will deploy sophisticated bots to use the verified card details to make e-commerce purchases, steal from accounts, and buy gift cards. Gift cards are then sold at discounted prices or used to buy premium items like phones, televisions, and computers that can easily be sold on auction sites.

Risks Addressed

UNNECESSARY CHARGEBACKS

DAMAGED REPUTATION

REDUCED EFFICIENCY

How HUMAN Prevents Payment Fraud

Today's sophisticated bots behave just like real users and are much better at evading detection. Businesses find it increasingly difficult to defend applications from automated attacks. Even when apps function as intended, they are vulnerable to criminals using sophisticated bots that mimic human behavior using mouse movements, keystrokes, and fake browser behaviors. These sophisticated bots can easily evade bot detection features in traditional application security solutions that rely on behavioral monitoring or static lists, leaving your apps open to abuse. HUMAN's BotGuard for Applications protects web and mobile applications from bots and automated attacks including payment fraud. BotGuard uses a multilayered detection methodology that establishes hard technical evidence of fraud. This enables BotGuard to detect and block today's sophisticated bots with unparalleled precision to ensure that only real humans interact with your applications.

The Challenge

The refund cost is on you

Online retailers can suffer from automated payment fraud attacks that result in chargebacks - where disputed transactions result in you refunding your customer.

Chargeback hurt your credibility

Bot-enabled payment fraud is the most common cause of chargebacks. In addition, chargebacks could harm your business's reputation with credit card processors.

Bots waste resources and money

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

Benefits to Your Business

Minimize Chargebacks

BotGuard stops fraud before its committed so that you can reduce disputed transactions and chargebacks.

Protect Your Reputation

Gain peace-of-mind that your site is protected against the risk of fraud, scraping and PII harvesting by BotGuard's industry-leading detection precision.

Improve Efficiency

Preventing automation with BotGuard reduces the cost that sophisticated bots add to your infrastructure and frees-up your product team's time wasted on bot defenses for more productive tasks.

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.