HUMAN

HUMAN Transaction Abuse Defense

Protect your platform from scalping, hoarding, and carding.

FORRESTER®
WAVE LEADER 2022
Bot Management

Automated transaction abuse describes the use of bots to execute fraudulent activity on your checkout flow. This includes scalping, hoarding, and carding bot attacks.

- **Scalping attacks** - Automated bots buy highly-prized products to be resold at inflated prices on secondary markets.
- **Hoarding attacks** - Sophisticated bots add items repeatedly to online shopping carts until the inventory is exhausted. These denial of inventory attacks mean competitors can then sell your customers the products that you can no longer provide.
- **Carding attacks** - Bots attempt fraudulent purchases with stolen credit card numbers then fraudsters either sell the validated card information or buy items that can be resold online.

Transaction abuse is increasingly difficult to detect. Sophisticated bots imitate real user behavior to evade detection. Traditional bot defenses—such as WAF, and home-grown tools—add friction to the user journey and are no match for advanced bots. Stopping transaction abuse requires a behavior-based approach, continuous risk assessment, and real-time mitigation of suspicious activity.

Maintain customer loyalty and reduce chargebacks

CONSEQUENCES OF TRANSACTION ABUSE:

- Increased customer frustration and service calls
- Revenue loss
- Damaged brand reputation
- Chargebacks
- Reduced efficiency

HUMAN Transaction Abuse Defense

HUMAN Transaction Abuse Defense safeguards your web and mobile applications from scalping, hoarding and carding bots. Our solution uses behavioral profiles and flow tracking, machine learning, computational challenges (PoW), and real-time sensor data to identify automated transaction abuse with exceptional accuracy.

When abuse is detected, HUMAN Transaction Abuse Defense delivers optimal fraud management using a range of mitigation actions, including hard blocks, honeypots, misdirection, and serving deceptive content. The solution stops scalping, hoarding, and carding bots without adding unnecessary friction to the user experience.

> **"Fraud conducted by bots became a real problem for us. The team had to constantly deal with fraudulent transactions, sometimes in the middle of the night...In three days [after deploying HUMAN], we could see a huge reduction of fraudulent transaction attempts — from 100,000 to 150."**

Bryan Shanaver, CEO of Donately

Benefits for digital businesses

Ensure customer experience and trust

Prevent stockouts created by bots scalping in-demand products from your site. Ensure real customers connect with your brand and don't take their business elsewhere.

Prevent chargebacks

Stop automated payment fraud that results in chargebacks, where disputed transactions require you to issue a refund.

Improve efficiency and reduce costs

Block sophisticated bots to prevent unnecessary traffic and speed up your app, lower your infrastructure and service expenses, and free up your product team's time.

How it Works

COLLECT

The sensor collects and sends hundreds of non-PII client-side indicators to the cloud-based detector for precise determination of human versus bot activity.

DETECT

The machine-learning-based detector continuously learns the normal range for human interactions and correlates it with customer-defined policies.

BLOCK

The enforcer tags bot traffic according to threat response policies and continuously updates the detector with relevant data. Responses include blocking, rate limiting, honeypots, misdirection and serving deceptive content.

LEARN

The portal features advanced reporting and analysis capabilities to investigate attacks and create custom reports. Integration with leading marketing platforms enables website analytics.

The HUMAN Advantage

Stop transaction abuse

Stop scalping, hoarding, and carding attacks to prevent stockouts, promotion abuse, fraudulent transactions, and unnecessary chargebacks.

Enforce decisions effectively

Custom mitigation actions allow fast response to threats, integrating with your workflow.

Single pane of glass management

Manage all your HUMAN solutions from one console. It's easy to see key details, edit policies, and share knowledge

Reporting for specific audiences

Out-of-the-box and custom reports for all stakeholders

Easy integration with your IT stack

Open architecture with key SIEM, marketing and monitoring integrations

Enterprise level customer service

24/7/365 proactive security services available

Key Integrations

Edge Integrations (CDN, Cloud)

fastly YOTTAA CLOUDFLARE amazon cloudfront

Application SDK/Middlware

node Java Ruby GO python

Load Balancers and Web Servers

APACHE NGINX citrix NetScaler f5

Serverless and Cloud Frameworks

E-commerce Platforms

salesforce commerce cloud Magento

Logs and Metrics

Adobe Analytics Google Analytics DATADOG splunk>

Powered by the Human Defense Platform

HUMAN uses a modern defense strategy to safeguard organizations from digital attacks, fraud, and account abuse. Our solutions increase ROI and trust while decreasing customer friction, data contamination, and cybersecurity exposure. The Human Defense Platform powers an award-winning suite of application protection solutions enabling full visibility and control of your web and mobile applications and APIs.

About HUMAN

HUMAN is a cybersecurity company that safeguards 500+ customers from digital attacks, fraud, and account abuse. We leverage a modern defense strategy —comprising visibility, network effect, and disruptions—to enable our customers to increase ROI and trust while decreasing end-user friction, data contamination, and cybersecurity exposure. Today we verify the humanity of more than 20 trillion interactions per week across advertising, marketing, e-commerce, and enterprise security, putting us in the pole position to win against cybercriminals. Safeguard your digital business with HUMAN. **To Know Who's Real, visit www.humansecurity.com.**