Transaction Abuse Defense
Protect against fraudulent automated transactions

TRANSACTION ABUSE DEFENSE
Transaction Abuse Defense stops malicious automated transactions on your web and mobile applications and APIs. The solution uses advanced machine learning, behavioral analysis, and intelligent fingerprinting to identify malicious bots with exceptional accuracy. It then delivers optimal bot management, including hard blocks, honeypots, and misdirection. The solution lets known bots and crawlers proceed unimpeded and can show bots alternative content and pricing if desired.

Transaction Abuse Defense is part of Application Protection, a suite of solutions purpose-built to secure web and mobile applications from a range of cyberthreats.

WHAT WE SOLVE

- CARDING
- GIFT CARD CRACKING
- SCALPING
- INVENTORY HOARDING

“\nIn just one hour of one day, if we had not had HUMAN in place, we would have seen about 34,000 hits on our backend payment processor. That’s about $3,100 (in fees) in just an hour.\n”

SENIOR MANAGER OF INFORMATION SECURITY ARCHITECTURE AND ENGINEERING at Sally Beauty

BENEFITS

- REDUCE CHARGEBACKS AND FINANCIAL LOSSES
  Stop automated fraudulent transactions and block bad traffic before it reaches your payment fraud solution

- PRESERVE CUSTOMER EXPERIENCE
  Allow 95% of users to proceed in under 2ms with low-latency technology and user-friendly challenge

- OPTIMIZE RESOURCES
  Reduce bandwidth strain and wasted infrastructure spend, and save time manually responding to bots
**HOW IT WORKS**

**COLLECT**
Hundreds of non-PII client-side indicators

**DETECT**
Human vs. bot activity using machine learning models

**MITIGATES**
Bot traffic according to customizable threat response policies

**REPORTS**
Incident details in intuitive dashboards for easy investigation and analysis

**OPTIMIZES**
detections by continuously updating ML models with relevant data

**KEY CAPABILITIES**

**Advanced detections** based on behavioral analysis, intelligent fingerprinting, predictive models, and 400+ machine learning algorithms

**Detailed dashboards** display traffic over time, incident types, and details on IPs, known bots, and referrers

**Mitigation responses** via customer-specific policies to serve hard blocks, honeypots, misdirection, and alternative content/pricing

**Incident analyzer** enables users to investigate key details, such as blocked IPs, targeted pages, user agents and header referrers

**Edge Sensor** is your first line of defense to block malicious bots at the edge, the first time they visit your site

**Human Challenge** is HUMAN's proprietary verification challenge: a press-and-hold button that is only shown to 0.01% of users

**THE HUMAN ADVANTAGE**

**Scale**
We verify more than 20 trillion digital interactions weekly across 3 billion unique devices providing unrivaled threat telemetry.

**Speed**
Our Decision Engine examines 2,500+ signals per interaction, connecting disparate data to detect anomalies in mere milliseconds.

**Decision Precision**
Signals from across the customer journey are analyzed by 400+ algorithms and adaptive machine-learning models to enable high-fidelity decisioning.

*HUMAN is trusted by the world's leading enterprises and internet platforms to prevent, detect, and respond to cyber attacks with unmatched scale, speed, and decision precision across their advertising, application, and account surfaces. Safeguard your customer journey end to end with complete confidence by consolidating with the Human Defense Platform.*