HUMAN

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**

> **"In 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."**
>
> ***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

Human Challenge: HUMAN's user-friendly CAPTCHA-alternative, a press-and-hold button that is only shown to 0.01% of users.

Precheck: Block bots at the edge, on the first request by showing a quick animation on certain protected paths.

HUMAN Sightline: Automatically isolate distinct bot profiles and reveal in granular detail what each attacker is doing on your application.

Adaptive Learning: AI models spot nuanced bot behavior shifts and automatically optimize mitigation workflows.

Incident analyzer: Investigate key details, such as blocked IPs, targeted pages, user agents and header referrers.

Secondary detection: Uncover hidden threat patterns by automatically analyzing all current and historical traffic data in aggregate after an initial bot-or-not decision is made.

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.