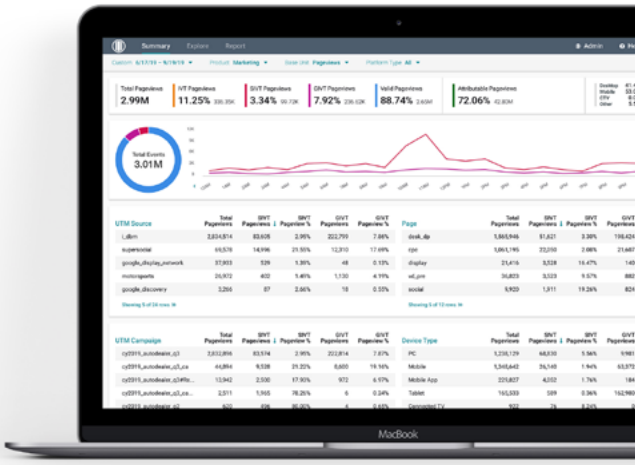
HUMAN

BotGuard for FinTech

Protect financial web and mobile applications from automated fraud and sophisticated bots



Blockchain and Web3 are transforming every part of the digital ecosystem. However, this innovation rate and the scale of the projects, introduce vulnerabilities that cybercriminals will exploit. In the finance sector, automation as a tool for digital transformation, grew 30% every year from 2017 to 2022, with the COVID-19 pandemic serving only to accelerate this transition.[1] Banking and financial services remain one of the highest risk sectors for fraud from cyber security threats, with some businesses seeing almost half of their online user engagement being conducted by bots.[2]

BotGuard for Applications lowers fraud loss and preserves customer trust and experience

STOP ACCOUNT TAKEOVER (ATO)

Breaking into existing accounts

- Credential Stuffing
- Credential Cracking

PREVENT ACCOUNT CREATION FRAUD

New sign-ups using fake and/or stolen data

- Account Creation

STOP PROMOTION AND EXPERIENCE ABUSE

Diverse in-app fraud, theft and abuse

- Promotion Abuse
- Downstream Transaction Fraud (Payment)
- Scraping
- Sniping
- Spamming
- Skewing

BotGuard for Applications

BotGuard protects finance web and mobile applications from bots and automated attacks, including account takeover (ATO), account creation fraud, and in-app content and experience abuse such as promotion code and other downstream transaction fraud, spamming and scraping. Unlike competing solutions, BotGuard uses a multilayered detection methodology that isn't reliant on any single technique. The signals collected establish hard technical evidence of fraud and mean BotGuard is able to detect and block today's automated fraud with unparallelled accuracy to ensure that only real humans interact with your applications.

HUMAN Earns **HIGHEST SCORE in Strategy and Highest Score Possible in Eight Criteria** among the 15 most significant emerging Bot Management solution providers.

The Forrester Wave™:
Bot Management, Q2 2022

Benefits

Protect your growing business

Protect customer login, new user registration and stop web scraping from even the most sophisticated bots.

Minimize fraud loss

Prevent promotion code abuse, payment fraud, sensitive data theft, and other costly losses.

Maintain customer trust

Keep in-app bot abuse and unnecessary friction from ruining the experience of real human customers.

Boost operational efficiency

Automatically block unwanted bot traffic to free your application team to focus on innovation and ensure your application infrastructure and services run efficiently.

Gain complete transparency & control

Simple to set up mitigation policies and response.

How it Works

Collect
BotGuard's human verification engine collects and sends over 2500 clientside signals indicative of 'human or not' activity to HUMAN for processing

Decide
BotGuard's Real Time Decision Engine combines technical evidence and machine learning to deliver 'human or not' decisions with industry-leading accuracy

Protect
BotGuard deploys 'human or not' decisions along with a recommended 'block', 'allow' or customizable mitigation action to automatically mitigate non-human activity

Report
Insights identifying invalid traffic and threat category are available within minutes in the BotGuard Dashboard and via Reporting API

The BotGuard for Applications Advantage

HUMAN's modern defense strategy against automated bots provides detection and "bot or not" decisions with unmatched scale, speed, and precision to safeguard your financial applications and services.

Detects Deception at Scale

Global observability: The Human Verification Engine analyzes more than two trillion interactions per day to identify traffic patterns and anomalies.

Sartori Threat Intelligence Team: Stay ahead using intelligence provided by our research team.

Multi-source collective protection: Analyzes more than 2500 signals from applications, advertising platforms, and IoT devices.

Robust anomaly detection: Outperforms rule-based detection in stability and accuracy.

Continuous learning: More than 350 machine learning models are constantly updated based on the traffic patterns of real human users.

Prevents adaptation by attackers: Adaptation-proof Machine Learning makes it arduous for bad actors to reverse-engineer workarounds.

Enables Friction Free UX/CX

Maintain customer experiences: preserve and protect your customers' trust and digital experiences with your applications and services.

Ground truth without CAPTCHA: our superior signal gathering allows us to obtain ground truth accurately without introducing friction for users.

Highest accuracy and lowest false positive rate in the Industry: Machine learning-enabled statistical models reduce inaccuracies that plague rule-based detection systems.

Provides Actionable Insights

Maintain control of your traffic: Our dashboard provides you with alerts, oversight, control, and metrics for all stakeholders.

Visualized threat profile: View a breakdown of your bot and human traffic trends and differentiate between good and bad bot traffic.

Customizable automated reporting: Set up custom reports to run on a regular schedule.

Data integrations: Directly integrate with your reporting and visualization tools.

Receive regular data exports via API: integrate with your SIEM.

Access to HUMAN Insights Services: Enhanced bot assessments, priority response, and threat intelligence services to help you prepare, respond, and recover quickly from bot attacks.

Key Integrations

Protects any web or mobile application

Web

[+ S2S API]

Mobile *(beta)*

Content Delivery Network (CDN)

Cloud

Identity and Access Management

Web Server

About HUMAN

HUMAN is a cybersecurity company that safeguards enterprises and internet platforms from sophisticated bot attacks and fraud to keep digital experiences human. **To Know Who's Real, visit www.humansecurity.com.**