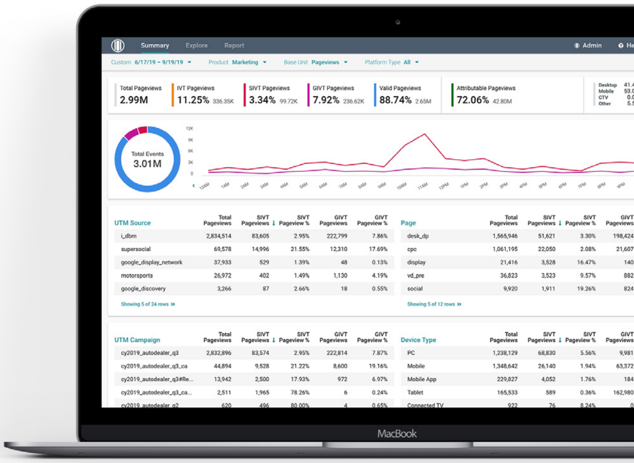
HUMAN

BotGuard for Applications

Protect web and mobile applications from sophisticated bots and automated attacks



Total Pageviews	IVT Pageviews	SIVT Pageviews	GIVT Pageviews	Valid Pageviews	Attributable Pageviews
2.99M	11.25% 336.35K	3.34% 99.72K	7.92% 236.62K	88.74% 2.65M	72.06% 42.80M

Desktop	41.4
Mobile	53.0
CTV	0.0
Other	5.5

UTM Source	Total Pageviews	SIVT Pageviews ↓	SIVT Pageview %	GIVT Pageviews	GIVT Pageview %
i_dbm	2,834,514	83,605	2.95%	222,799	7.86%
supersocial	69,578	14,996	21.55%	12,310	17.69%
google_display_network	37,933	529	1.39%	48	0.13%
motorsports	26,972	402	1.49%	1,130	4.19%
google_discovery	3,266	87	2.66%	18	0.55%

Showing 5 of 24 rows »

Page	Total Pageviews	SIVT Pageviews ↓	SIVT Pageview %	GIVT Pageviews
desk_dp	1,565,946	51,621	3.30%	198,424
cpc	1,061,195	22,050	2.08%	21,607
display	21,416	3,528	16.47%	140
vd_pre	36,823	3,523	9.57%	882
social	9,920	1,911	19.26%	824

Showing 5 of 12 rows »

UTM Campaign	Total Pageviews	SIVT Pageviews ↓	SIVT Pageview %	GIVT Pageviews	GIVT Pageview %
cy2019_autodealer_q3	2,832,896	83,574	2.95%	222,814	7.87%
cy2019_autodealer_q3_ca	44,894	9,528	21.22%	8,600	19.16%
cy2019_autodealer_q3#Re...	13,942	2,500	17.93%	972	6.97%
cy2019_autodealer_q3_ca...	2,511	1,965	78.26%	6	0.24%
cy2019_autodealer_q2	620	496	80.00%	4	0.65%

Device Type	Total Pageviews	SIVT Pageviews ↓	SIVT Pageview %	GIVT Pageviews
PC	1,238,129	68,830	5.56%	9,981
Mobile	1,348,642	26,140	1.94%	63,372
Mobile App	229,827	4,052	1.76%	184
Tablet	165,533	589	0.36%	162,980
Connected TV	922	76	8.24%	0

86% **of IT and Cybersecurity professionals believe sophisticated bots can circumvent simple protections**[1]

Enterprises 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 conventional application security solutions that rely on behavioral monitoring or static lists, leaving your apps open to abuse.

[1] 2021 Bot Management Trends - ESG April 2021

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

ACCOUNT TAKEOVER (ATO)

Breaking into existing accounts

- Credential Stuffing
- Credential Cracking

ACCOUNT CREATION FRAUD

New sign-ups using fake and/or stolen data

- Account Creation

CONTENT AND EXPERIENCE ABUSE

Diverse in-app fraud, theft and abuse

- Downstream Transaction Fraud (Payment)
- Spamming
- Scalping
- Sniping
- Skewing
- Scraping

BotGuard for Applications

BotGuard protects 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 payment and other downstream transaction fraud, spamming, inventory abuse 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 sophisticated bots with unparallelled accuracy to ensure that only real humans interact with your applications.

HUMAN **"leads the pack with robust threat intelligence, attack detection, and vision"** among the 13 most significant emerging Bot Management solution providers.

The Forrester New Wave™: Bot Management, Q1 2020

Benefits for Application Security

Protect your online business
Protect customer login, new user registration, checkout and payment flow from even the most sophisticated bots

Minimize fraud loss
Prevent payment and wire transfer fraud, sensitive data theft, and other costly losses.

Maintain customer trust
Keep in-app bot abuse 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 responses based on clear visibility of bot traffic.

How it Works

Collect
BotGuard's human verification engine collects and sends over 2500 client-side 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

Prevent
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

Most Effective Multilayered Bot Detection Methodology

- BotGuard is powered by the Human Verification Platform™ combining technical evidence, machine learning, and continuous adaptation to deliver 'human or not' decisions with industry-leading accuracy, and minimal user friction.
- HUMAN verifies the humanity of 10 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 BotGuard detection techniques with new indicators against emerging attacks.

Simple Deployment and Integration, Immediate Actionable Insight

- BotGuard's detection tags are deployed within minutes via JavaScript tag or SDK for mobile apps.
- Deploy to edge solutions with no modifications to front-end or back-end code required
- The BotGuard Dashboard and API enable analysis of aggregate trends, custom reporting, and visualization.
- Dedicated HUMAN solution engineer for deployment and integration and technical account manager for analysis and support.

Active Prevention enables real-time bot mitigation

- Real-time mitigation of malicious bots or nonstandard traffic. Enable your systems to take direct action (block, mark for review, deceive, Human challenge checkbox, etc.) as the request occurs.
- On malicious traffic detection (such as known Account Takeover bots) invalidate the request to prevent automated interactions.
- Implemented via direct server to server or edge provider integration.

Key Integrations

Protects any web or mobile application

Web

JS

[+ S2S API]

Mobile

android SDK

iOS

Content Delivery Network (CDN)

fastly

amazon cloudfront

CLOUDFLARE

Cloud

snowflake

aws

Google Cloud

Identity and Access Management

PingIdentity

okta

Web Server

NGINX

About HUMAN

HUMAN is a cybersecurity company that collectively protects enterprises from fraud and abuse including sophisticated bot attacks, lowering costs and risk while accelerating digital business performance. **To learn more, visit www.humansecurity.com.**