CONQUER BOTS BEFORE THEY CONQUER YOU

A Whitepaper

Abstract

This paper discusses the current state of the art in Bot Management to minimize damages hackers and fraudsters create in today's IT infrastructure. It also delves into detailed descriptions of HUMAN Security's BotGuard for Applications, BotGuard for Growth Marketing, and MediaGuard for Ad Integrity and why they are best-of-breed products in their respective categories.

info@humansecurity.com

Table of Contents

List of Figures

Know Who’s Real:
Pre-Filter Bots Before They Transact to Stop Payment Fraud and Cyber Risk

1. Malicious Bots are a Growing Threat to Business

Fraudsters and hackers are increasingly using sophisticated malicious bots to illegally profit from the boom in online transactions (Figure 1). Bots and spiders make up anywhere from 40%[1] to more than 50%[2] of internet traffic and are used in 77% of cybercriminal attacks.[3] Eighty four percent of companies have seen an increase in the number of bot-based attacks[4] and ninety percent rate protecting websites and applications from these attacks as a top five security initiative.[5] Yet, 78% of organizations are woefully unprepared since they are using subpar solutions[4] that only handle Distributed Denial of Service (DDoS) attacks or only rely on the features of Content Delivery Networks (CDNs) or Web Application Firewalls (WAFs).

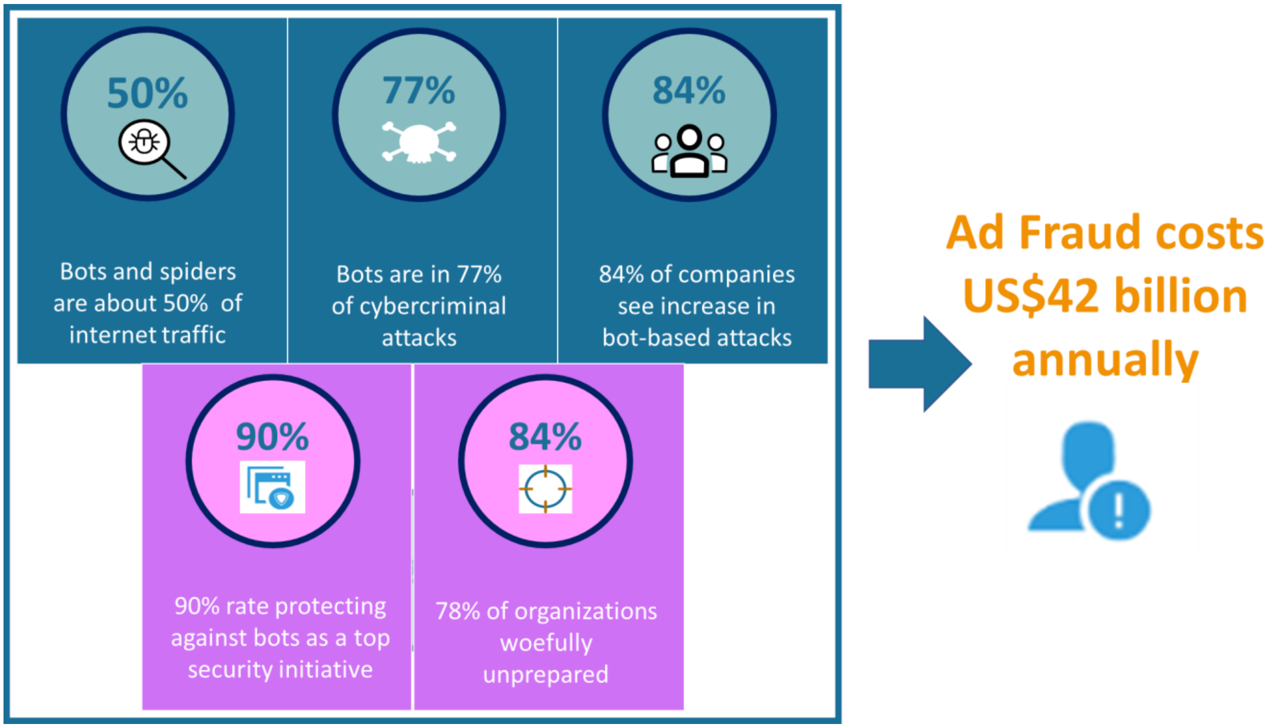

50%
Bots and spiders are about 50% of internet traffic
77%
Bots are in 77% of cybercriminal attacks
84%
84% of companies see increase in bot-based attacks
90%
90% rate protecting against bots as a top security initiative
84%
78% of organizations woefully unprepared
Ad Fraud costs US$42 billion annually

Figure 1. Transmission and Transaction Bot Attacks

A recent survey of 440 businesses across many sectors in the U.S. and the U.K. concluded ad fraud costs businesses US$42 billion annually, or four percent of their revenue, the same percentage lost annually to skewed analytics.[6]

Bots threaten businesses with increased payment fraud and cyber risks, more downtime, slower performance, wasted ad and marketing spending, and squandered resources to fight bot farms. For example, incorrect data caused by bots can result in businesses wasting money on running special promotions, ordering new stock even when their inventory is not depleted, or burning money through marketing promotions.

The good news is that it is significantly harder to scale attacks by stopping malicious bots. However, this requires a combination of highly accurate innovative detection solutions and deep expertise in threat intelligence. This is how HUMAN conquers the shrewdest hackers and fraudsters behind the most sophisticated bot attacks. Customers across

[1] "‘Bad bots’ make up a huge amount of all internet traffic," TechRadar, September 02, 2021.
[2] “How Much Web Traffic is Bots?,” Web Traffic Geeks.
[3] Report: 77% of companies lost revenue due to bot attacks (venturebeat.com)
[4] State of Online Fraud and Bot Management, Forrester and Google, January 2021
[5] Enterprise Strategy Group, Protecting Applications with Bot Mitigation, February 2021
[6] "Bots Skew Marketing Analytics, Cost Businesses Millions," John. P. Mello, Jr., *Commerce Times*, December 7, 2021.

streaming media, financial services, retail, entertainment, and other industries trust HUMAN to detect and takedown bots before they transact to mitigate cyber risk and prevent fraud.

2. Accurate and Actionable Bot Detection and Takedown are Challenging

It is very hard to know which bots are good (search engine bots, site metrics bots, and more) and which are malicious (content scraping, credential stuffing, etc.). This is particularly true as the rate and pace of malicious actors with major economic incentives on the Internet are escalating and bot attacks are getting more sophisticated. Bot attacks have gone beyond traditional account takeover, card cracking, credential stuffing and cracking, denial of service (Layer 7 DDoS), fake account creation, scraping, server overload, vulnerability scanning, and others. Today's sophisticated bots impersonate human behavior to evade detection technologies that are typically found in WAFs and CDNs.

Further many traditional preventive methods are unsatisfactory. They often add friction that turns away legitimate traffic. Techniques such as CAPTCHA, reCAPTCHA v2, and reCAPTCHA v3 with user interactions, are no longer fully adequate because sophisticated software with Artificial Intelligence (AI), Machine Learning (ML), and image recognition are getting smarter and easily recognize mundane objects as bicycles, boats, buses, pedestrian crossings, and so on. Some vendors have deployed techniques that require solving puzzles or image manipulation (e. g., ensure a four-legged animal is standing upright on its feet), but it won't be long before AI-enabled bot attack software wins this game too.

Bot engineers are smart, but hackers and fraudsters are very close behind—often maybe even a step or two ahead. The goal must be to not only to keep up with these bad actors, but also "destroy" them, take them down permanently, and bring them to justice. This requires a threat intelligence team with deep expertise and proactive innovative detection approaches that collect a large range and scale of signals and implement sophisticated artificial intelligence/machine learning (AI/ML)-based algorithms. HUMAN provides the industry's best Bot Detection capabilities coupled with HUMAN's world-class Satori Threat Intelligence and Research Team. Both are needed to accurately pre-filter bots before they cause economic harm and essential for cybersecurity.

3. Accurate Bot Management Quintessential for Cybersecurity

Bot Management is a daunting task and must address both: Transmission and Transaction (Figure 2) attacks. Transmission, typically the domain for the Chief Information Security Officer (CSO/CISO), are techniques hackers use to attack IT infrastructure and, once successful, Transaction, usually the domain of the business owner/fraud fighter, propagates the attack causing financial damages.

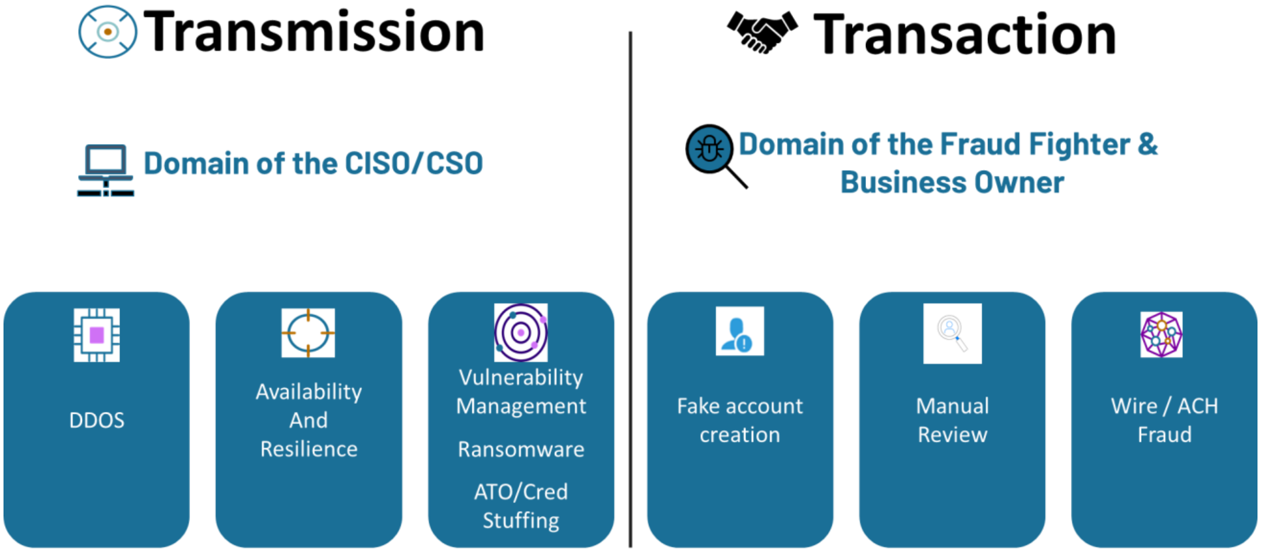


Figure 2. Transmission and Transaction Bot Attacks

For example, in 2018, the U. S. Government labelled "3ve" as one of the most devastating online ad fraud operations. Brazen in its scale, it reached peaks of 3 billion bid requests per day and gained control of almost two million victim computers during Transmission by infecting them with Boaxxe/Miuref and Kovter malware, as well as Border Gateway Protocol-hijacked IP addresses. 3ve counterfeited over 10K domains, many of the most popular publishers on the web. During Transaction, it monetized in two ways: counterfeit inventory and traffic selling through very large number of seller accounts, widely available across the ecosystem since one pub/company could have numerous seller accounts.

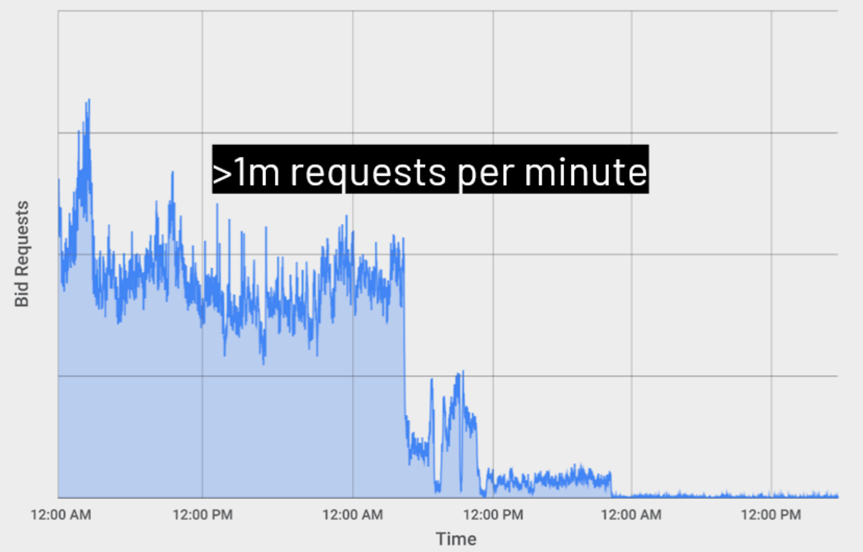


Figure 3. 3ve Successful Takedown

HUMAN was able to acquire samples of the 3ve malware and infect its own machines early on to study the behavior of 3ve anti-forensic behavior: geo checks, security software checks, crypto-mining, and tag evasion. On Oct 21, 2018 the U. S. Law Enforcement (LE) executed an international takedown and arrest of the key players behind 3ve and began a seizure of the command-and-control infrastructure. In parallel, a handful of private-sector technology companies, spearheaded by HUMAN and Google, also began efforts to dismantle the infrastructure behind the operation. Figure 3 shows the result of the technical takedown illustrating the drop in requests per second originating from part of the 3ve operation. The phases during this operation included quiet suppression, LE action, and remediation of infections.

Protecting the many targets – including customers – of an operation like 3ve in the context of a multi-stakeholder working group requires patience, dedication, diligence, endurance, and deep expertise. At the core, HUMAN's objectives are to detect and prevent this type of fraud on behalf of customers and Internet users, and to cut off these types of operations from its sources of profit. This is only possible because of the unique investments in the Satori threat intelligence team and the continuous innovation in fighting malicious bots.

The Satori team consists of over 70, and growing, experts in threat intelligence, threat detection, engineering, and go to market. Meaningful research is not limited to any one aspect of the bot universe, and the diverse backgrounds of Satori's team members reflect the diversity of the challenge. Members of the Satori team have a passion for shining a light on the dark corners of the bot universe that are not frequently exposed.

HUMAN understands that Bot Management is critical to a customer's digital journey and not just a feature in their cyber security solutions portfolio as many competitors suggest. The ROI of establishing the veracity of traffic on a site can be in the 100s of percent.

4. Why is HUMAN Better at Knowing Who's Real?

To defeat today's bots, HUMAN uses a unique multilayered approach that enables the verification of the humanity of digital interactions with unmatched speed and accuracy. HUMAN's chief competitors offer a variety of cloud/web security tools, including Bot Management software, CDNs, WAFs, and Web Application and API Protection (WAAP) software. However, they suffer the following shortcomings when *compared to HUMAN:*

1. Bot Management most often is not offered as a standalone product, but as part of larger, integrated (often with non-best-of-breed products) expensive product suites, forcing customers to license products (e. g., CDN and WAF) they may already have licensed and paying for in their IT infrastructure. *HUMAN does one thing—Bot Management—and does it very well, and works with partners to provide clients with best-of-breed and complete end-to-end business solutions with easy deployment and no vendor lock-in. Most enterprise security leaders realize that specialist solutions (not WAF/CDN and bot management feature add-ons) are the most effective way to solve the bot problem.*

2. Have limited scale. *HUMAN processes ~1B detection events, observes ~500M+ unique devices daily and can meet the scale and performance demands of top internet platforms, hence any business. With a 10-year history, over 10 Trillion interactions are verified each week across customers, over 80% of US consumers. HUMAN leads in collective protection by observing and detecting more for better client protection.*

3. Rely on rule/anomaly-based methods or device fingerprinting alone often with no or limited AI/ML and threat intel capabilities. This delivers more false positives for complex bots. They also claim their Bot Management software is multilayer, whereas it is multistep, onerous with higher latency, and often adds friction. *HUMAN's multi-layered human verification engine (constantly updated by the Satori team) is unmatched in maturity, sophistication, and user experience. It collects 2500+ signals to analyze with over 350 independent Statistical and AI/ML algorithms to make deterministic decisions based on both technical and behavioral evidence. This contributes to high accuracy and ultra-low false positive rates and adds no friction.*

4. View bots as a software, and not as a human, problem. *HUMAN offers a human and software approach to take down humans behind malicious bots and offers its clients "white glove" service and tailored business solutions that are value-priced based on outcomes.*

5. Exclusively rely on customer data (often private) and a combination of algorithms and CAPTCHA that add friction, and typically learn *after* an attack has occurred. They also solve yesterday's bot problems, e. g., signature-based predefined pool of bots, and do not address today's more-sophisticated threats that can bypass and scrape data. *HUMAN offers unique threat intel capabilities with Satori and several approaches to identify malicious actors and take down botnets at the source to provide zero-day threat protection. This ability to do a causal analysis using threat intel gives HUMAN the ability to have a deeper understanding of the source of all types of threats and fraud trends based on industry-agnostic R&D capabilities. Clients benefit from this constant innovation.*

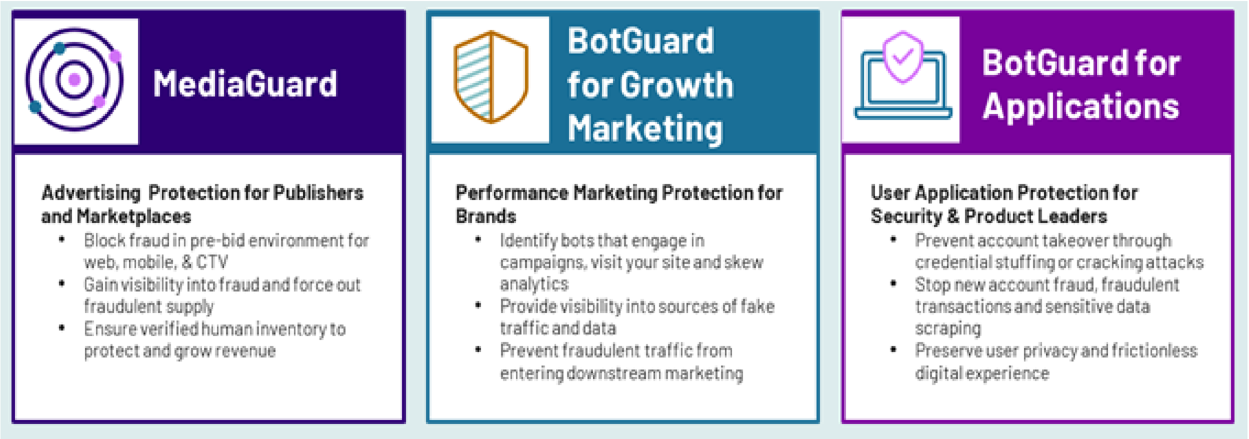
The HUMAN Bot Management Portfolio packages these high-value differentiators across applications, growth marketing and advertising use cases.

5. HUMAN Bot Management Portfolio

The HUMAN product portfolio includes:

- Human Verification^{TM} Engine
- BotGuard for Applications
- BotGuard for Growth Marketing
- MediaGuard for Ad Integrity

Human Verification Engine is the basic technology upon which BotGuard and MediaGuard are built. BotGuard has some application-specific features for Applications and Growth Marketing. Together this portfolio supports use cases (Figure 4) across the digital customer journey, from programmatic advertising to user application protection.



MediaGuard

Advertising Protection for Publishers and Marketplaces

- Block fraud in pre-bid environment for web, mobile, & CTV
- Gain visibility into fraud and force out fraudulent supply
- Ensure verified human inventory to protect and grow revenue

BotGuard for Growth Marketing

Performance Marketing Protection for Brands

- Identify bots that engage in campaigns, visit your site and skew analytics
- Provide visibility into sources of fake traffic and data
- Prevent fraudulent traffic from entering downstream marketing

BotGuard for Applications

User Application Protection for Security & Product Leaders

- Prevent account takeover through credential stuffing or cracking attacks
- Stop new account fraud, fraudulent transactions and sensitive data scraping
- Preserve user privacy and frictionless digital experience

Figure 4. Human Verification Engine Use Cases

5.1 Human Verification Engine

HUMAN Verification Engine protects applications, APIs, and digital media from bot attacks, preventing losses and improving the digital experience for real humans. HUMAN's multilayer detection methodology (Figure 5) combines *continuous adaptation*, *machine learning*, and *technical evidence* to deliver 'bot or not' decisions with industry-leading speed and accuracy, and without user friction. HUMAN collects more than 2,500 signals, including data from the application, device, network, software, and user configuration layers, and deploys over 350 algorithms per interaction. Of all the tests served, it only takes one failure to identify a sophisticated bot.

To attain global visibility, HUMAN verifies the humanity of ten trillion interactions per week across APIs, applications, and digital media, harnessing internet-scale visibility and a decade of data to deliver continuously adaptive and mutually reinforcing protection to all.

> ***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**

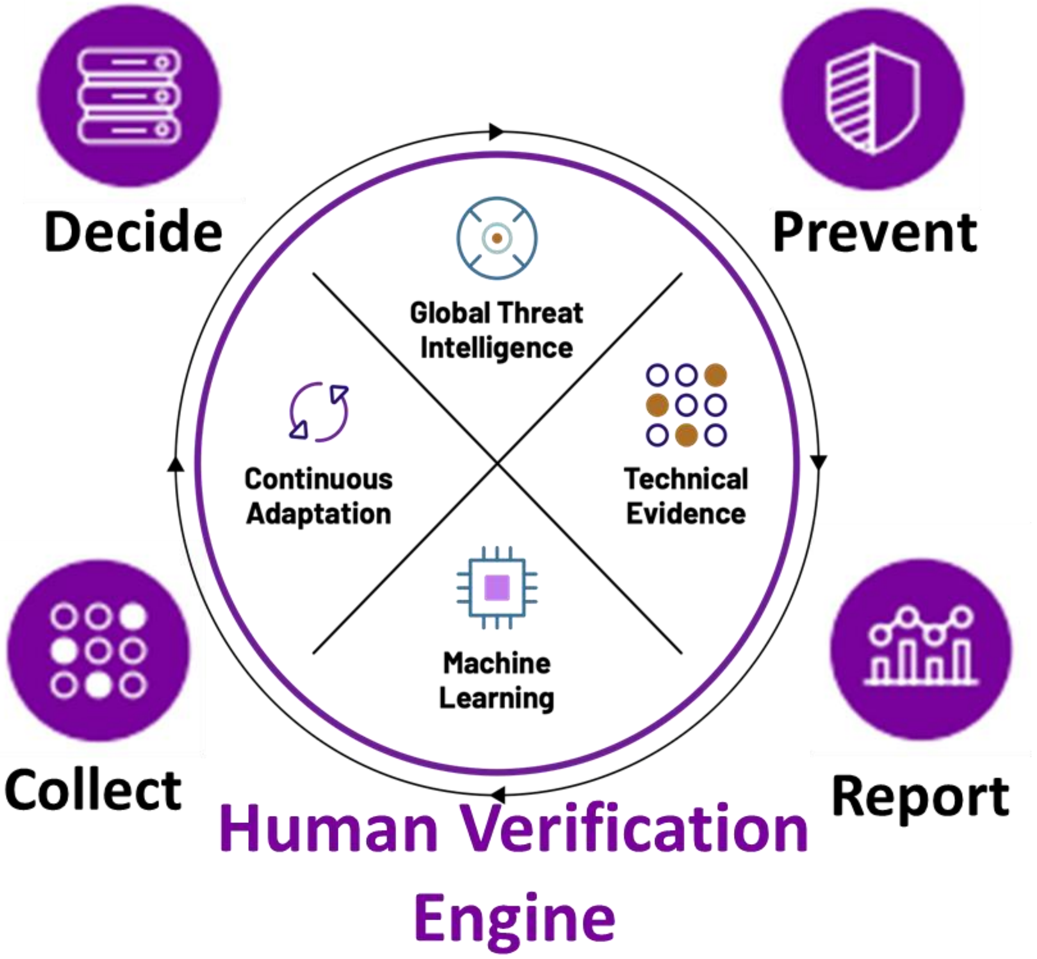


Figure 5. HUMAN's Multilayered Bot Detection Methodology

At a high level, here is how Human Verification Engine works:

- **Collect**: HUMAN is deployed via JavaScript tag (or Mobile SDK for mobile apps) to collect and send over 2500 client-side non-PII signals indicative of 'human or not' activity to HUMAN for processing.
- **Decide**: Combines technical evidence and ML to deliver 'human or not' decisions with industry-leading speed and accuracy.
- **Prevent**: HUMAN 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 HUMAN Dashboard and via Reporting API.

Finally, HUMAN's Satori Threat Intelligence and Research Team takes down multiple large-scale attack networks every year. The TEAM identifies and reverse engineers new threats to fine-tune HUMAN's detection techniques with new indicators against emerging attacks. HUMAN works with the largest internet platforms and law enforcement to research and take down cybercriminal threats.

5.2 BotGuard for Applications

Eighty-six percent of IT and Cybersecurity professionals believe sophisticated bots can circumvent simple protections.[7] BotGuard for Applications detects and mitigates sophisticated bot activities on sites and applications including:

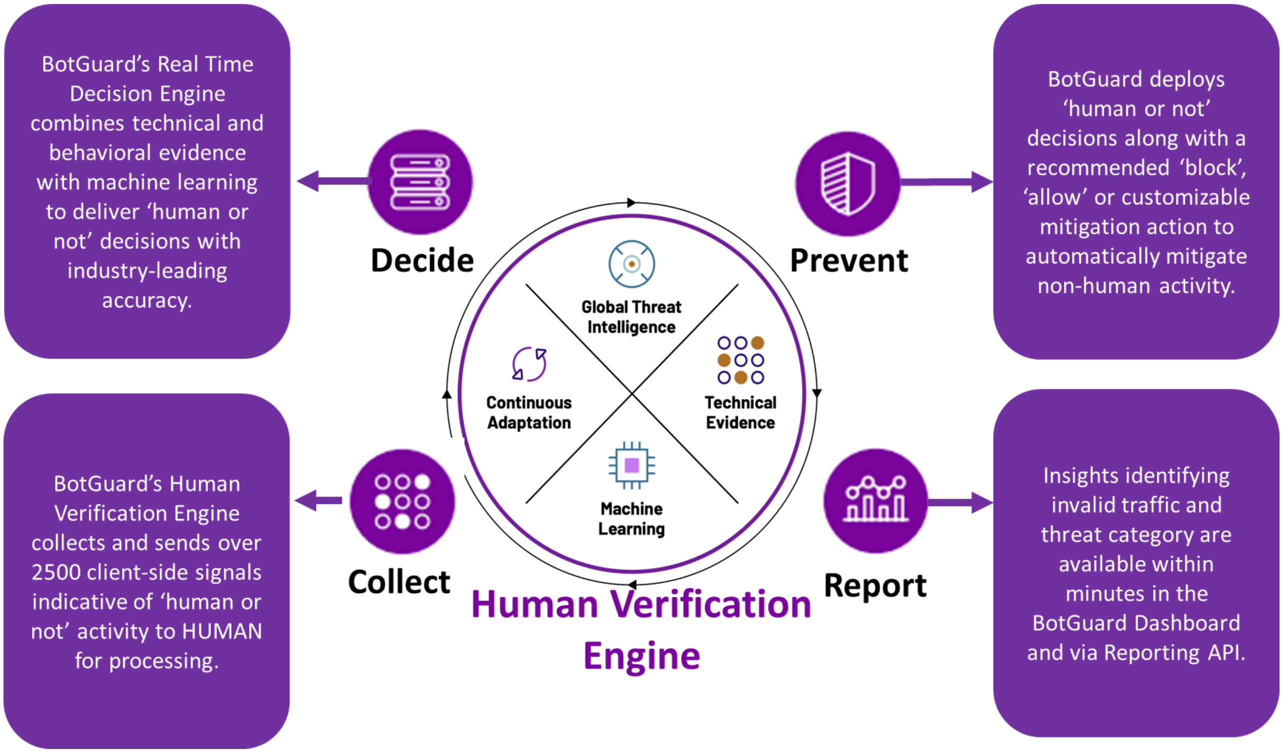
- *Account creation fraud* where fraudsters create new sign-ups using fake and/or stolen data
- *Account takeover* where swindlers break into existing accounts to execute credential cracking and credential stuffing
- *Content and experience abuse* where impostors commit diverse in-app fraud, theft, and abuse to commit downstream transaction fraud (payment), spamming, scalping, sniping, skewing, and scraping.

5.2.1 Benefits for Application Security

- *Protect 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 the application team to focus on innovation and ensure application infrastructure and services run efficiently.
- *Gain complete transparency and control*: Simple to set up mitigation policies and responses based on clear visibility of bot traffic.

5.2.2 How it Works

Unlike competing solutions, BotGuard uses a multilayered detection methodology that does not rely on any single technique (Figure 6). The signals collected establish hard technical and behavioral evidence of fraud. This means BotGuard can detect and block today's sophisticated bots with unparalleled accuracy to ensure that only real humans interact with the customer's applications.



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

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

BotGuard's Human Verification Engine collects and sends over 2500 client-side signals indicative of 'human or not' activity to HUMAN for processing.

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

Figure 6. BotGuard for Applications

[7] "2021 Bot Management Trends," ESG April 2021.

5.2.3 Advantages of BotGuard for Applications

BotGuard for Applications:

- Offers the most effective multilayered bot detection methodology powered by the Human Verification Platform™ and supported by Satori Threat Intelligence and Research Team
- Provides simple deployment and integration via JavaScript tag or SDK for mobile apps and immediate actionable insight through the BotGuard Dashboard and API
- Enables real-time mitigation of malicious bots or nonstandard traffic with active prevention (block, mark for review, deceive, Human challenge checkbox, etc.) as the request occurs, implemented via direct server-to-server or edge provider integration.

5.2.4 Key Integrations

These integrations (Figure 7) help protect any web or mobile application.

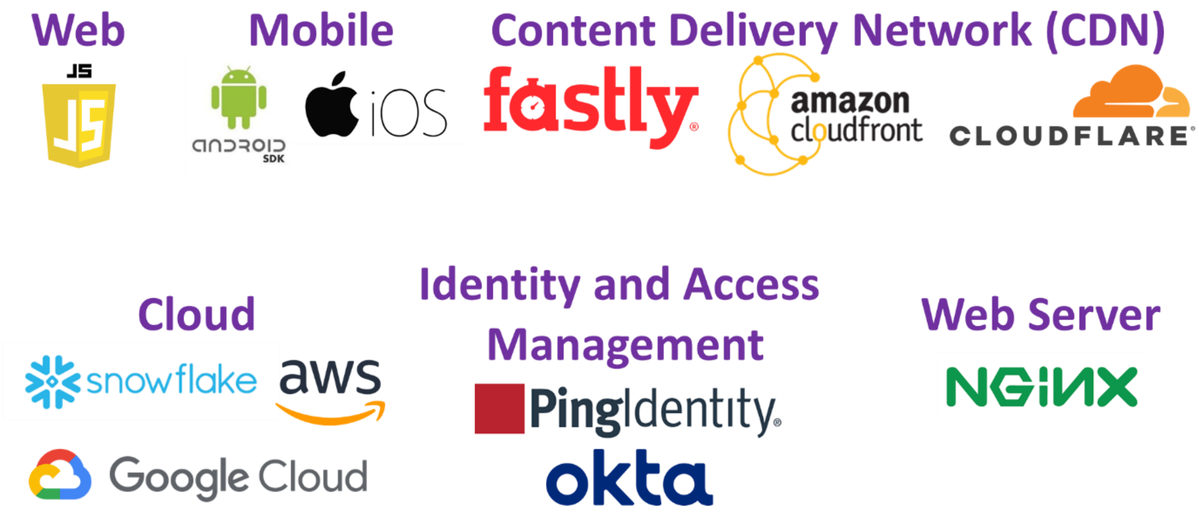


Figure 7. Key Integrations of BotGuard for Applications with Industry-Leading Vendors

5.3 BotGuard for Growth Marketing

The annual cost of global marketing fraud is also estimated to be in the billions of dollars. Cybercriminals and fraudsters are targeting digital marketing investments by using sophisticated bots in order to profit through deceptive and abusive engagement in marketing campaigns. These bots click on paid ads and search results and visit sites and mobile apps where they can fill out forms with stolen personal information or abuse inventory and incentive programs. Investments on acquiring, remarketing, and storing to fraudulent traffic cost brands millions of dollars each year. Bot traffic also skews marketing and analytics data, obscuring customer insight and executive decision making.

BotGuard for Growth Marketing protects against media buy fraud, lead generation fraud, lookalike and retargeting fraud, competitive assaults, app install fraud, and in-app engagement fraud.

5.3.1 Benefits of BotGuard for Growth Marketing

- Decrease acquisition costs
- Improve lead quality and conversion rates
- Increase overall customer conversion rates, revenue, and lifetime value
- Maintain clean, efficient data, and downstream marketing.

5.3.2 How it Works

BotGuard for Growth Marketing is a human verification service that detects automated engagement in digital marketing and automatically prevents invalid traffic from entering ad targeting systems, CRM, and downstream marketing systems to lower costs and boost marketing performance (Figure 8). BotGuard detects invalid site traffic in real-time without impacting page load times or user privacy. Detection insights are delivered immediately for visualization and actioning directly within marketers' preferred tools and technology stacks.

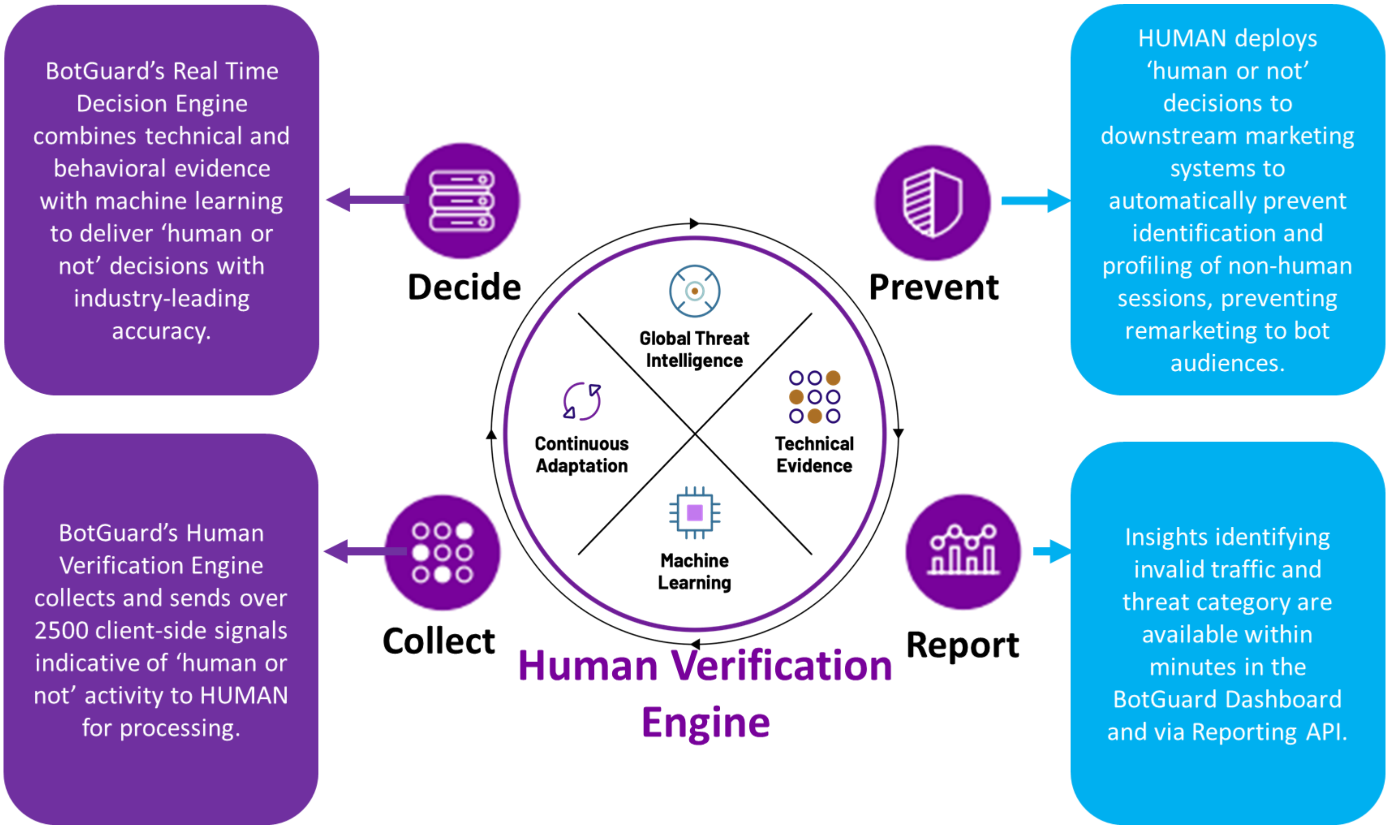

BotGuard's Real Time Decision Engine combines technical and behavioral evidence with machine learning to deliver 'human or not' decisions with industry-leading accuracy.
Decide
Prevent
HUMAN deploys 'human or not' decisions to downstream marketing systems to automatically prevent identification and profiling of non-human sessions, preventing remarketing to bot audiences.
Global Threat Intelligence
Continuous Adaptation
Technical Evidence
Machine Learning
BotGuard's Human Verification Engine collects and sends over 2500 client-side signals indicative of 'human or not' activity to HUMAN for processing.
Collect
Report
Insights identifying invalid traffic and threat category are available within minutes in the BotGuard Dashboard and via Reporting API.
Human Verification Engine

Figure 8. BotGuard for Growth Marketing

BotGuard for Growth Marketing provides key integrations with:

- *Marketing Analytics*: Adobe, Google Analytics
- *Marketing Technology*: Bing, Facebook, Google Marketing Platform, KOCHAVA, Mailchimp, Outbrain, Taboola, TikTok, Twilio Segment
- *Online Marketplaces*: AWS Marketplace, Snowflake
- *Tag Managers*: Adobe Launch, Google Tag Manager

5.3.3 Advantages of BotGuard for Growth Marketing

BotGuard for Growth Marketing is:

- Easy to Deploy
    - Tag Manager can used to configure and deploy the lightweight JavaScript detection tag to a website within minutes
    - Tag Manager can also be used to send detection decisions and data to other marketing systems in real-time
- Made for Marketers
    - Visualize fraudulent traffic by UTM Source, UTM Campaign, and Page destination
    - Create and analyze bot audiences within popular marketing analytics platforms
    - De-target bot audiences from active marketing campaigns, boosting conversion rates and lowering cost-per-acquisition
    - Automatically prevent the identification and profiling of non-human sessions in downstream marketing including remarketing, audience enrichment, and cross channel attribution systems
- Powered by the HUMAN Verification Engine

- HUMAN’s multilayered detection methodology combines technical evidence, machine learning, and continuous adaptation for ‘human or not’ decisions with industry-leading speed and accuracy, and without user friction
- Verifies the humanity of 10 Trillion interactions per week across digital advertising, marketing, and applications, harnessing internet-scale visibility, and a decade of data to deliver continuously adaptive and mutually reinforcing protection to all.

5.3.4 Key Integrations

The integrations (Figure 9) with best-of-breed technology products help marketers decrease acquisition costs and improve lead quality and conversion rates.

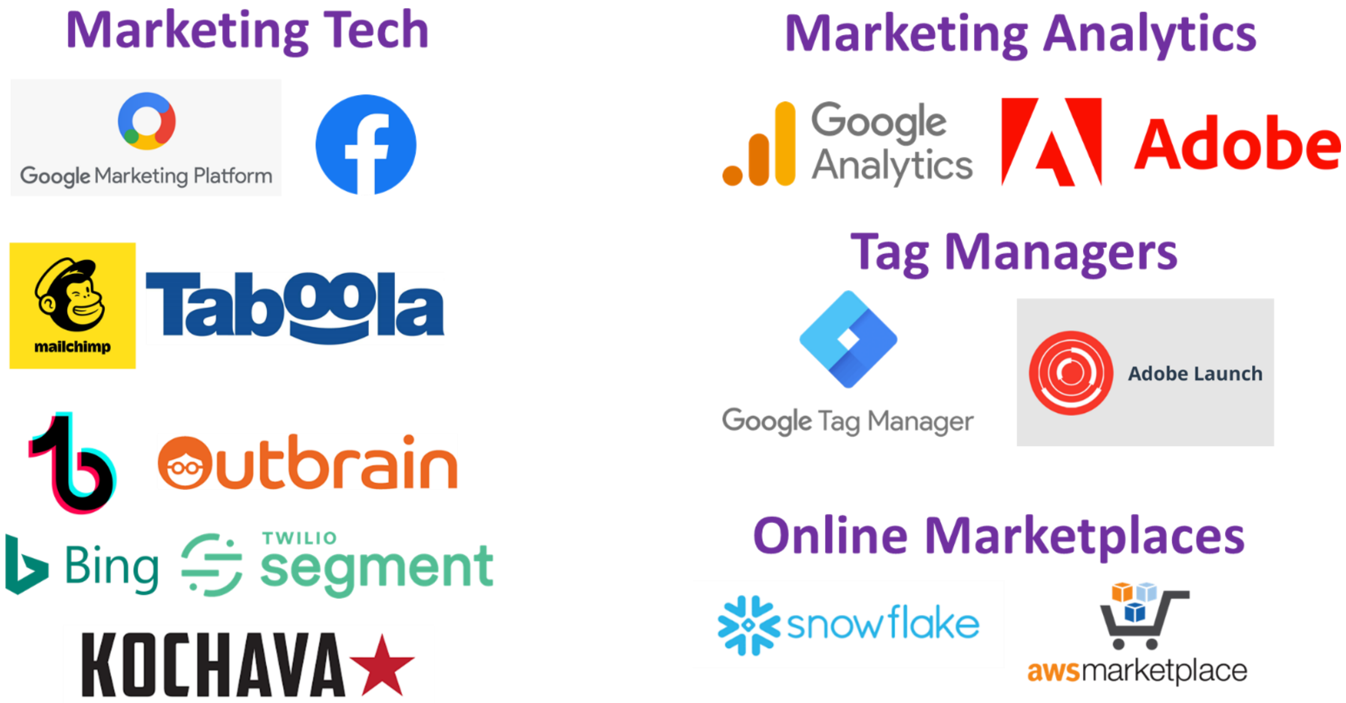


Figure 9. Key Integrations of BotGuard for Marketing with Industry-Leading Products

5.4 MediaGuard for Ad Integrity

Digital ad spending is soaring as enterprises adopt new ways to reach audiences—connected TV, mobile web and mobile apps, native, and web. But the highways to new destinations for advertising are strewn with a wave of hijackers (fraudsters) looking to grab their piece of the loot. These fraudsters click on ads, invade digital advertising, and steal advertising spend. When fraudsters invade ad tech platforms, they not only steal digital spend from advertisers, but also damage inventory reputation and future revenue streams for platforms.

> *“...the first company to receive MRC accreditation for SIVT solutions that encompass both the pre- and post-bid processes, across desktop, mobile web, in-app, and OTT platforms, clearly speaks to its continued position at the forefront of this vital industry space.”*
> – George W. Ivie, Executive Director & CEO, MRC

5.4.1 5.4.1 Benefits for Ad Integrity

- *Maximize Inventory Visibility*: Actionable insights into the presence of sophisticated bots to ensure each impression only reaches humans.
- *Protect and Grow Revenue*: Prevent fraud to deliver validated supply, improving trust and transparency with demand partners to increase revenue opportunities.

5.4.2 How it Works

MediaGuard provides advertisers with robust detection and prevention capabilities to verify the humanity of advertising efforts across all channels (Figure 10). Using a multilayered detection methodology that relies on session-level analysis of every impression and a collective protection approach that builds upon the community of knowledge, HUMAN more accurately detects and prevents today's dynamic and polymorphic bots. MediaGuard helps advertisers ensure that only real humans interact with their advertising.

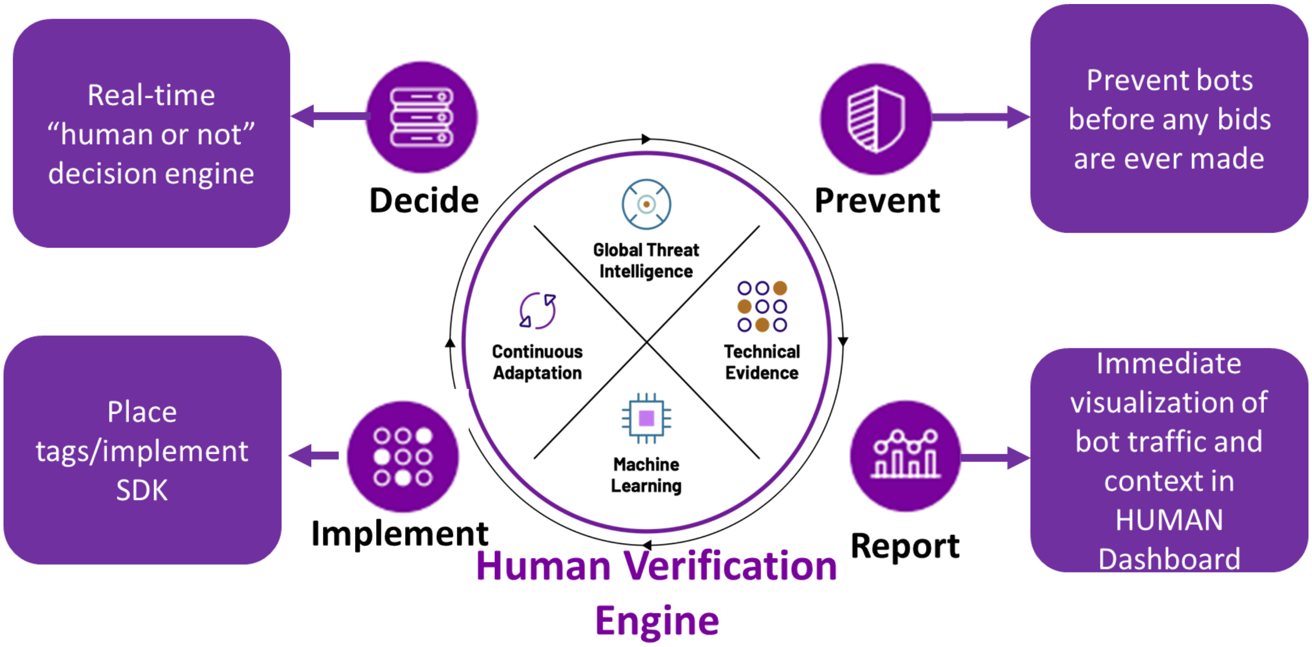

Real-time “human or not” decision engine
Decide
Prevent
Prevent bots before any bids are ever made
Global Threat Intelligence
Continuous Adaptation
Technical Evidence
Machine Learning
Place tags/implement SDK
Implement
Human Verification Engine
Report
Immediate visualization of bot traffic and context in HUMAN Dashboard

Figure 10. MediaGuard for Ad Integrity

5.4.3 Advantages of MediaGuard for Ad Integrity

- *Unmatched Scale*: Seeing 10 trillion transactions each week and more than 300 million devices daily provides unmatched intelligence into sophisticated bot fraud across all channels.
- *Unprecedented Accuracy*: Sophisticated, multilayered detection methodology, leveraging technical evidence, machine learning, threat intelligence, and continuous adaptation.
- *Complete Precision*: Impressions are only identified as Sophisticated Invalid Traffic (SIVT) and prevented when there is absolute certainty traffic is invalid. HUMAN is able to decipher between real humans and sophisticated bots on the same machine.

5.4.4 Key Integrations (Figure 11)

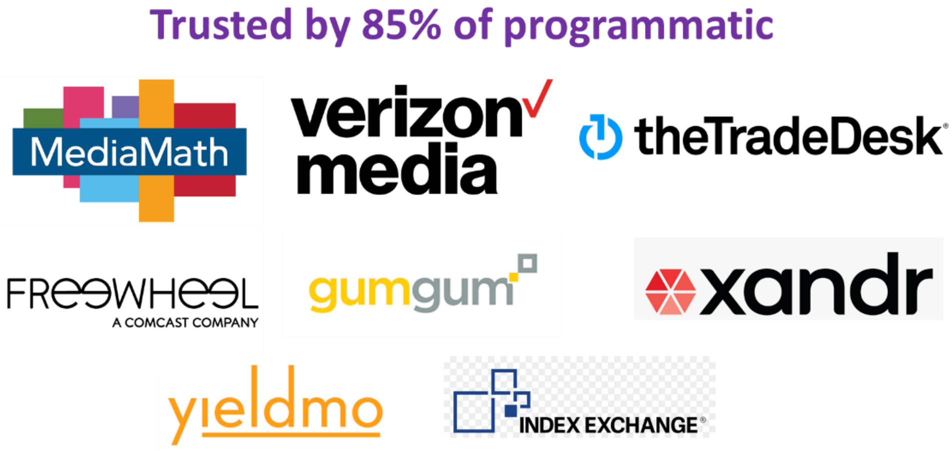


Figure 11. Key Integrations for MediaGuard with Industry-Leading Vendors

6. Customer Successes

HUMAN solutions have been deployed (often replacing competitors) at leading businesses worldwide across many industries and are delivering significant ROI.

6.1 Streaming Music Provider

Hackers registered by creating fake accounts and logged in an attempt to takeover accounts (Figure 12). They then resorted to stream fake listening and paid by credit validation and fraud payments. The customer deployed HUMAN's prefiltering and protected downstream transactions.

> *"We effectively stopped credit card fraud! By blocking the bots at registration+login, we prevented them from reaching the subscription flow." – Senior Executive, Streaming Music Provider*

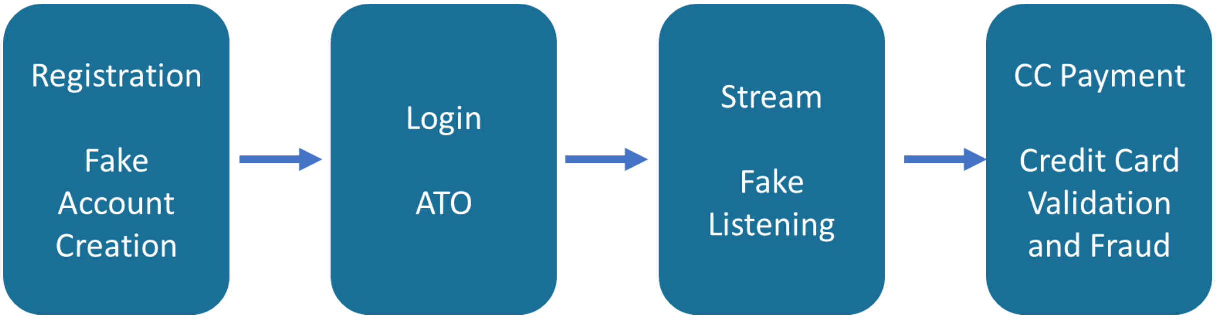


Figure 12. Streaming Music Fraud

Human recommended:

- Maximizing marketing spend efficiencies
- Protecting against the entire scope of marketing fraud
- Using HUMAN BotGuard's Google Analytics
- Employing Application Security to guard against login abuse

These resulted in discovering that over 10% of the CRM data were fraudulent. The vulnerability was immediately identified and quickly adjusted to mitigate the fraudulent data points. The missed revenue opportunity would have extrapolated to over $2,000,000 annually. Identifying the vulnerability immediately accelerated a massive optimization strategy toward data segments consisting of real humans.

6.2 Online Retail Bank

This is an online banking customer who thought the bot management feature provided by their CDN would be adequate for stopping bots. They deployed HUMAN on top of it to see whether that was true and discovered that 14% of their invalid traffic was sophisticated bots—and it was all passing through the CDN's bot management feature, completely undetected. The bank was pondering many options and choices and what could be done once a transaction had been submitted since hackers were using 12,000 stolen sets of usernames and passwords to gain access to real human users' accounts (Figure 13).

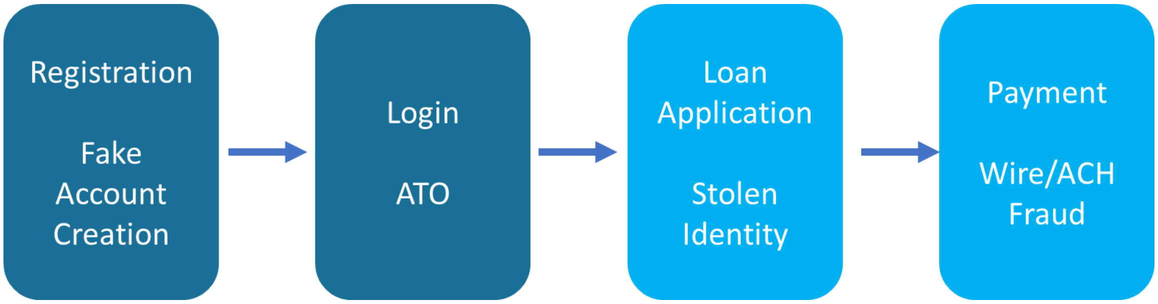


Figure 13. Online Banking Fraud

HUMAN immediately detected this bot activity, and its detection team named the operation TipJar. With HUMAN's guidance, the customer implemented application-level friction in the form of multi-factor authentication (MFA) when its solution detected bot activity.

Because of HUMAN's 'bot or not' accurate decisions, mitigation was effective in stopping the bots, but the real human users whose accounts were compromised actually did not need to be stopped. They could keep using their accounts without disruption and there was no need to engage with the Call Center. The online banking provider pleased its customers and avoided fraud losses.

6.3 Global Entertainment Company

A global entertainment company was using two leading bot management solutions to protect its digital purchase experience, but bots were still getting through. This was accomplished by having a botnet impersonate human traffic to the customer's mobile app and abusing its API directly to cash out on previous customer purchases, making it past two different bot management solutions. In other words, a core functionality specifically designed to protect customers from fraud was under direct attack by sophisticated threat actors. The botnet was also being used to scan relevant news and media sites, automatically determining when to operate to maximize profit. Implementing HUMAN's solution helped the company stop event reservation fraud, saving millions in fraudulent event registration, and improving customer experience.

6.4 Marketplace Retail Company

A gig economy-based retail company uncovered a major competitive price scraping operation costing millions of dollars in unwanted infrastructure load and significant impact to user experience. Often, unwanted automation does not necessarily come from malicious attackers in another country—it could be from your own industry/country (or 'the bot next door').

In this case, the retailer realized that a major competitor was using bots for price scraping to gain a competitive advantage and it cost the retailer multiple millions in infrastructure load, not to mention the incalculable loss of revenue due to competitive disadvantage. In fact, the retailer realized 70% of its traffic was due to bots and a 1% reduction in bot traffic reduction resulted in $250,000 in compute savings. After deploying HUMAN's solution, the retailer now has the evidence to confront its competitor, address the issue, and set things right.

6.5 Insurance Provider

An insurance company that was investing heavily in affiliate, search, and social strategies had growing concerns about bots infiltrating their purchase funnel. Each completed step of the provider's registration process assigns a different value for customer targeting and modeling. Any user who drops off during the process is entered into retargeting pools and is modeled for look-alikes.

The customer deployed HUMAN BotGuard and measured consistent threats throughout the testing period. An analysis by HUMAN of Invalid Traffic (IVT) categories discovered that Automated Browsing was the most common type of Sophisticated Invalid Traffic (SIVT). Stopping bots from engaging within the purchase funnel saved over $4 million annually.

6.6 Direct-to-Consumer (DTC) Provider

A DTC beauty brand was tasked with sales growth needed to test new audience engagement tactics and decided to place an increased emphasis on paid search and social campaigns. The provider deployed HUMAN BotGuard and found an average SIVT of 6.73% with the peak SIVT of 22%. Several of the new social campaigns were driving over 50% bot traffic, but because the social channels were important for awareness, they could not completely eliminate them.

The brand is currently building fraud mitigated segments with HUMAN for each of the new social media partners. HUMAN analysis predicts that brand can realize an 8X performance increase.

7. The HUMAN Advantage

Bots are about half of the traffic on the Internet – good (harmless and useful) bots and bad malicious bots. Bad bot attacks are over 3/4th of cybercriminals and cause significant economic damage (billions of dollars) for customers in every industry. Over 80% of companies list bot mitigation as a top security concern. However, 90% of them are woefully underprepared.

This is because accurate and actionable bot detection and takedown are challenging especially as bot attacks get more sophisticated and impersonate human behavior to evade detection technologies that are typically found in WAFs and CDNs. Other traditional CAPTCHA-like preventive methods are unsatisfactory as they often add friction that turns away legitimate traffic. More recently, as AI adoption continues to grow, AI/ML algorithms are used by bad actors to outsmart traditional bot detection solutions. As long as there are major economic incentives, bad actors will try to be one-step ahead of bot-mitigation solutions.

To win this battle, businesses must:

- Invest in and investigate technology behind advanced AI-enhanced bots and how to mitigate them. Hackers are no longer just individuals, but in many cases are state sponsored with enormous financial resources supporting their misdeeds.
- Deploy AI/ML and other analytics solutions that must be steps ahead of malicious actors.
- Bot Management should not be just an IT concern. It must be tightly integrated with cybersecurity infrastructure and be vital to business units, e. g., Advertising, Business Development Marketing, and Sales.

HUMAN does one thing—bot management—and does it very well with efficient, cost-effective ,easy-to-deploy, and unmatched solutions with better:

- **Scale:** Process ~1B detection events, observe ~500M+ unique devices daily and can meet the scale and performance demands of top internet platforms, hence any business. 10 Trillion interactions verified each week across customers, over 80% of US consumer. With a 10 Year history, leads in collective protection: more observations and more detection for better client protection.

- **Detection efficacy:** The multi-layered Detection Engine is unmatched in maturity and sophistication. BotGuard collects 2500+ signals to analyze with over 350 independent Statistical and AI/Machine Learning algorithms to make deterministic decisions based on both technical and behavioral evidence, while many vendors rely on anomaly-based methods or device fingerprinting alone. This contributes to higher accuracy and ultra-low false positive rates. No vendor can compete with the level of expertise and intelligence community credibility of the Satori Threat Intelligence Team who continuously contribute emerging threat intel and innovation into the Detection Engine that is frequently updated automatically at the client site.

- **Threat provenance and attribution:** Unlike competitors who primarily just provide pure technology solutions designed to block specific threats, HUMAN with Satori also leverages many datasets and intelligence community capabilities to continuously identify the malicious actors and take down their botnets at the source. This permanently eliminates these specific threats for clients and in fact for the entire community and provides protection against zero-day attacks.

- **Transparency and control:** The Dashboard lets users easily understand the specific threat category and threat factors observed for each detection. Customers can integrate their own signals, customize mitigation actions, and generate custom reporting.

- **High value integration:** Can integrate several leading CDNs, cloud service providers and other complementary Cybersecurity offerings to provide a higher value solution with a better ROI and value-based consumption pricing and a very high Net Promoter Score (NPS). This also provides clients a better user experience within their current familiar environment.

- **Privacy by design:** Privacy-sensitive code detects bots without tracking individual users across the internet (no collection of 3rd-party cookies). HUMAN is GDPR, SOC 2 Type 1, and Privacy Shield

Compliant, and a Member of the IAB’s Global Vendor List under the Transparency and Consent Framework (TCF).

HUMAN solutions have been deployed (often replacing competitors) at leading organizations worldwide across many industries and are delivering significantly better ROI.