



Bot and Fraud Mitigation: Then and Now

The threat landscape has changed. Are you protected?



Introduction

The Digital World is No Longer Human by Default

The use of automation by both basement hackers and sophisticated cybercriminals is scaling faster than ever, eroding digital trust and putting businesses at risk. Fake accounts, synthetic traffic, and fraud are becoming more deceptive and challenging to detect—and more costly to ignore.

But it's not all bad news. Bots and AI have many positive benefits, including increasing efficiency, improving data analysis, and automating tedious tasks. Agentic AIs specifically can streamline online shopping and other transactions on behalf of legitimate consumers. Getting complete visibility into this activity and understanding its intent is critical to safely adopt AI technology. Only with full insight can security teams customize mitigation actions to block, monetize, or allow AI traffic as appropriate.

In this evolving market, the end goal isn't stopping bots; it's enabling positive business outcomes. That means enabling authentic and well-intentioned interactions to **preserve user trust, provide an uninterrupted user experience, and protect revenue.**



*In this evolving market, the end goal isn't stopping bots; it's **enabling positive business outcomes.***

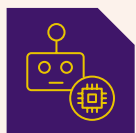
Key Market Shifts

**1.**

Cyberattacks and fraud are fueled by interconnected automated and manual attacks

The lifecycle of digital attacks and fraud often involves both automated and human activity. Fraudsters are increasingly blending bot attacks with fraudulent human behavior to commit account takeover, scraping, transaction abuse, and other types of fraud. As a result, security teams must be responsible for the end-to-end protection of their user accounts and business interests.

End-to-end protection means going beyond just blocking bots at the front of the funnel, but also proactively neutralizing compromised credentials and remediating human-led fraud. This requires multi-method detection that differentiates between good and bad bots and authentic and fraudulent human activity across their customers' entire digital journey—as well as deep investigative capabilities that enable visibility into exactly what is happening on your application.

**2.**

Advances in artificial intelligence are driving a widespread increase in bot usage

Large language models (LLMs) and AI agents blur the line between human, good bot, and bad bot. Legitimate consumers use chatbots, price comparison tools, and agentic AIs to navigate the digital world and interact with your organization online. At the same time, attackers are exploring AI tools as an accelerant to evade detection.

This means the challenge isn't just blocking sophisticated threats; it's gaining complete visibility into the behavior and intent of AI agents to help you make strategic and security decisions that protect your customers and your business.

**3.**

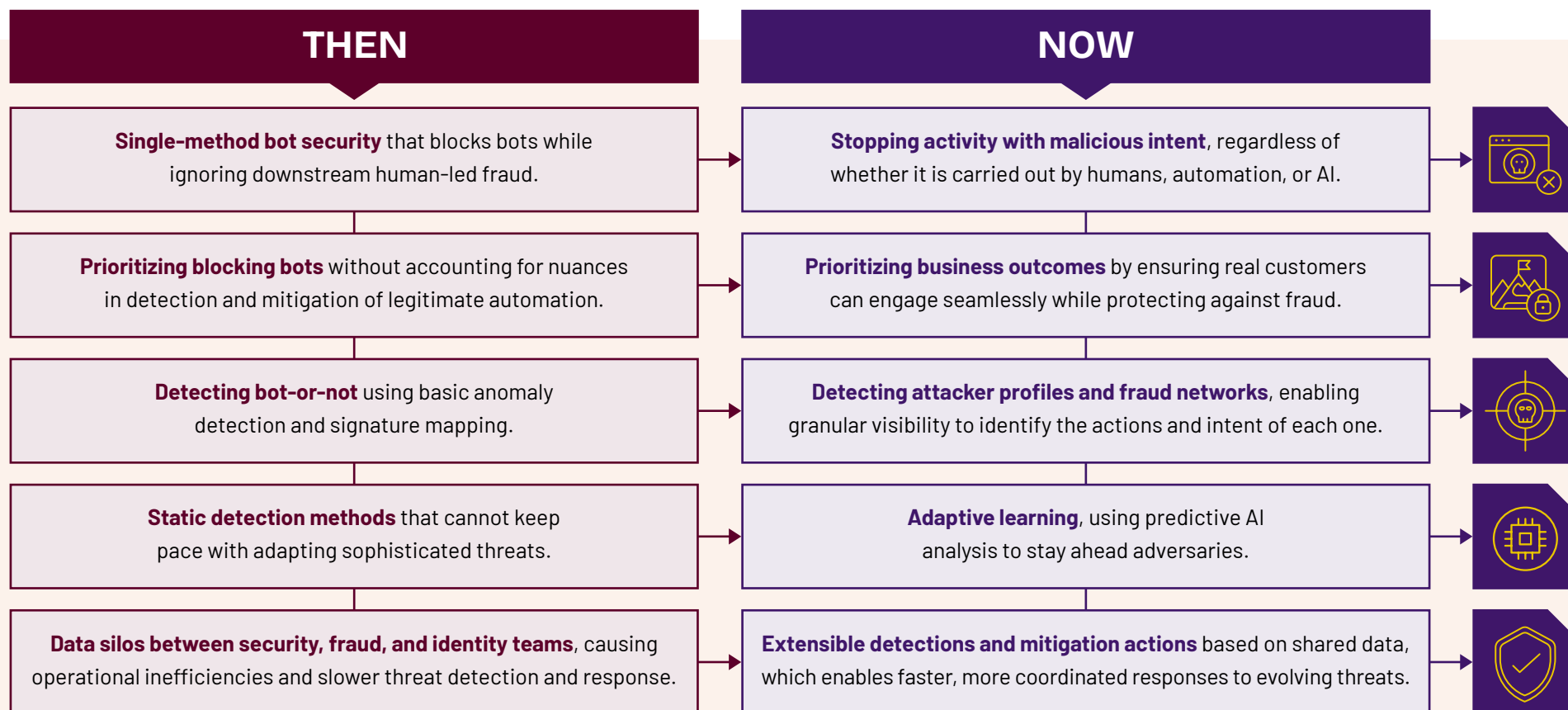
Security is shifting its focus to business outcomes, not simply blocking threats

Security teams protect users and business interests. Modern security solutions must be purposeful, collaborative, and laser-focused on business outcomes. Organizations are reframing the definition of threat mitigation from stopping attackers to enabling legitimate customer interactions.

In the past, bot management has been reactive, fragmented, and narrowly focused on blocking bots out considering the broader impact. Security teams are expanding their scope and look holistically at preventing fraud, increasing revenues, and preserving customer experience and trust.

The Evolution of Bot and Fraud Management

In the AI era, bot management is critical and necessary—but traditional approaches no longer cut it. As the cyberthreat landscape shifts, so do the expectations of and requirements for bot management solutions.



Granular Visibility is the Foundation of Modern Security Approaches

Fully understanding the threats you face is just as important as blocking them. Everyday consumers and cybercriminals alike are increasingly using a mix of bots, AI agents, and manual engagement to search, shop, stream, and socialize online. It is critical to understand the authenticity and intent of every interaction, regardless of whether it is carried out by a bot or human. Here are a few tools to help in that respect:

Secondary Detection

Secondary detection refers to advanced analysis after the initial decision is made. It uses purpose-built AI that reviews data in aggregate, comparing each new detection with everything that happened previously. With secondary detection insights, analysts can uncover hidden threat and fraud patterns and zero in on the areas that matter—which, in turn, accelerates investigations and threat response.

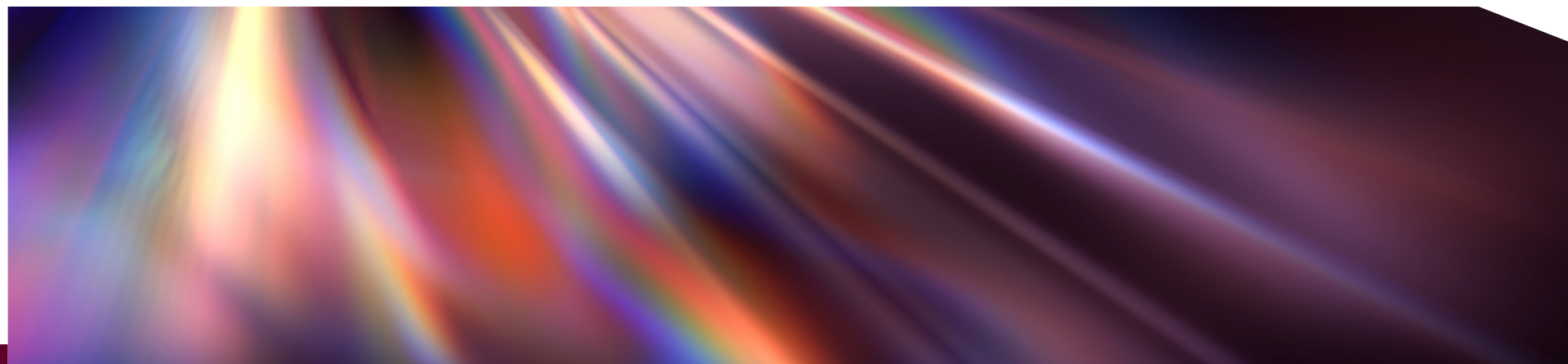
Examples of secondary detection include:

Attack profiling

An attack profile is the set of requests with shared capabilities, characteristics, and actions. Analysts can understand exactly what bad bots are doing, their sophistication, their capabilities, and the specific characteristics that distinguish them from other humans and bots on the application. This surfaces hidden insights that were not visible before, saves analysts hours on investigations, and enables teams to build an actionable threat narrative.

Network event detections

Using advanced machine learning and cluster detection, security teams can identify and correlate large patterns of fraud. This helps organizations understand the scale and complexity of an attack, so they can better identify and neutralize large-scale abuse of fake and compromised accounts carried out by both bots and humans.



Tracking Known Bots, Crawlers, and AI Agents

Reporting on bot activity in aggregate isn't sufficient for the AI era. By tracking the activity of specific bots on your application, security teams can understand which bots and AI agents are accessing their application and what paths they are targeting. This enables them to monitor impacts and make informed decisions to respond appropriately—whether that means blocking or allowing, suppressing ads or monetizing the traffic.

Request, Attacker, and Fraud Characteristics Analysis

With deep analysis capabilities, practitioners can drill down into specific IPs, ASNs, and other request characteristics to understand why certain traffic was blocked, which pages it was targeting, and header referrers. They can identify the most common risky activities associated with fraud in an account and understand the characteristics that link compromised or fake accounts together.

Compromised Credential Monitoring

Credential stuffing attacks are one of the most common attack vectors used by bad actors to commit account takeover attacks. By monitoring and flagging compromised credentials that are actively being used in attacks, security teams can encourage users to change their passwords—rendering the credentials useless before they are used to commit fraud.

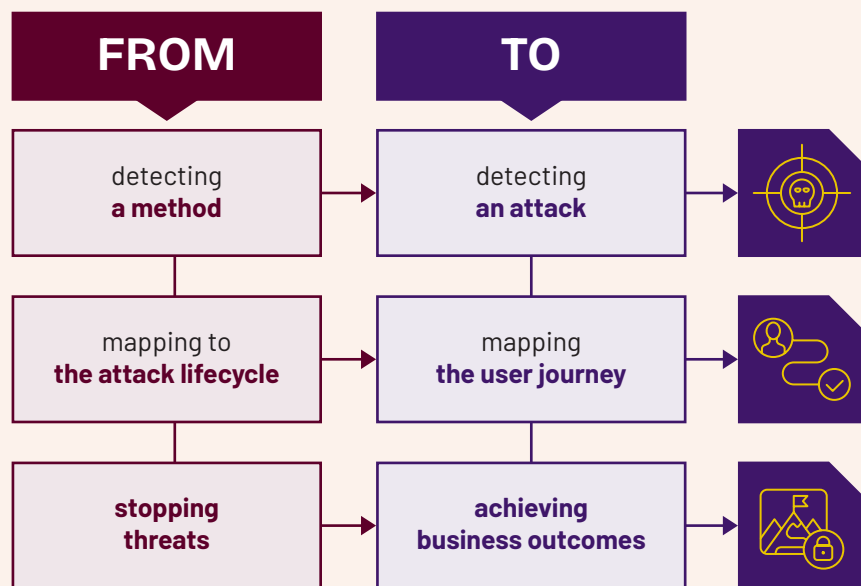


*Fully understanding
the threats you face
is just as important
as blocking them.*

Mitigation Must Be Customizable and Extensible

Single-method security solutions are incomplete. Attackers blend bots, AI-driven deception, and human fraud to bypass security defenses. Modern security requires sophisticated threat detection and mitigation that works regardless of the cybercriminal tactic. This demands adaptive decisioning and customizable response actions to neutralize both automated and human-led attacks tailored to your environment and business.

Mitigating cyberattacks requires a paradigm shift:



Point solutions will never completely eliminate fraud—and this is where **secondary detection** comes in. Secondary detection is critical to protecting applications end-to-end. By analyzing behaviors in depth, and comparing with other recognized threats, secondary detection systems can continue to detect and block malicious activity, even if it was able to bypass the initial primary detection.

A choice of default response actions and API integrations that allow **customizable mitigation** is key. Stopping bots hitting websites and apps with a straightforward block is usually default, but some organizations may prefer to display alternative content depending on their use case. With online accounts, organizations may wish to send password reset emails if compromised credentials are identified. If fraudulent activity is flagged in an account, they may wish to lock the account, flag it for review by their fraud team and create a ticket for their support team in case of a helpdesk call.

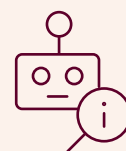
Ultimately, the purpose of security is to enable better business outcomes. An **extensible solution** will enable you to achieve stronger mitigation with bespoke detection data and custom response actions. By mixing your data with your vendor's detection models, you can work together to improve the efficacy of your solution toward your specific business goals.

It's About the Data—And What You Do With It

Organizations often operate in silos, but fraudsters don't. Modern cyberattacks are interconnected and follow consumers throughout their digital journey—as they click on a digital ad, browse an application, log into an account, and enter payment information on a payment checkout page. There are ample opportunities for bad actors to capitalize on the gaps in protection coverage by committing numerous types of attacks using automation and fraudulent human activity that span ad fraud to account takeover.

The only way to defeat interconnected cybercrime is with interconnected data. That means capturing signals from user interactions across advertising, application, and account surfaces.

The result is end-to-end protection from malicious automation and human-led fraud, in service of your desired business outcomes.



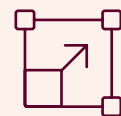
Analysis

Use purpose-built AI to analyze the specific bot and human traffic on your application, predict emerging threats, and automatically strengthen mitigation flows.



Visibility

Gain clarity into each attacker's behavior, strategy, and intent, so you can choose how to respond in the way that's best for your business.



Extensibility

Partner with your vendor to share your specific application knowledge and reach a solution that achieves your unique business goals.

The New Era of Bot and Fraud Management

Security teams need outcome-centric, customizable detection and mitigation that spans the entire lifecycle of bot attacks and fraud—as well as robust investigative capabilities that enable deep understanding of your unique threats. Solutions must free busy security and fraud teams from the management, investigation and mitigation burden, instead allowing them to focus on business outcomes. Here's what this looks like in practice:



Defense in Depth Across the Full Attack Lifecycle

Bad actors and fraudsters will use whatever techniques they need in order to exploit online organizations and their customers' journey. Modern solutions need to stop threats at every stage.

Example: Catching credential stuffing bots at authentication isn't enough to stop account takeovers. In addition to blocking fraudulent login attempts, security teams must also look pre- and post-login to proactively neutralize compromised credentials before bad actors can use them and monitor account activity post-authentication to remediate any accounts that have been broken into.



Quickly Delivering Answers So Users Can Understand Threats

Stopping an attack is expected. Helping security teams to understand the threat, attacker tactics and big picture fraud patterns over time is vital.

Example: Reporting on anomalies in aggregate doesn't provide the insights teams need. Instead, analysts should dive into individual attacker profiles in order to understand each one's specific actions and characteristics, such as which paths it was targeting, why it was flagged as fraudulent, how it was attempting to evade detection, and how it compares to legitimate human users. Similarly, visualizations of fraud networks over time illustrate how individual clusters of targeted accounts are actually interconnected and part of a long term 'low and slow' exploitation.



Protection That Works the Way Organizations Do

Solutions that force a team to change how they work are force subtractors, not multipliers. True integration goes beyond plugging into CIAMs, SIEMs and BI tools; it focuses on improving business outcomes.

Example: One-size-fits-all doesn't work for threat detection and mitigation. Organizations require detection that adapts to and learns from their bespoke environment, as well as customizable mitigation options that can be tailored to give maximum protection and minimal friction to customers.


Fraud Mitigation Centered on Business Outcomes

The purpose of stopping fraud is to generate positive business outcomes. Therefore, security solutions must evaluate fraud against the metrics that matter to your organization. This means providing business context for detection and mitigation events, preserving user experience and trust, and boosting revenue with the perfect blend of friction and mitigation actions for your needs.

By leveraging adaptive machine learning and AI models trained on a large and extensible data set, HUMAN provides unified, comprehensive detection and mitigation. The solution protects organizations from account takeover, scraping, new account fraud, transaction abuse, and other attacks throughout the customer journey—from the very first interaction with a website or app, through to the day-to-day usage of accounts.

Our unprecedented visibility and investigative tools enable security teams to take actionable steps to understand and mitigate the specific threats on their application. This ensures a line of sight into attackers over time, and protection against specific attacker adaptations.

Learn more at www.humanysecurity.com.



*HUMAN provides
**comprehensive
detection, mitigation
and visibility** into bot
attacks, human-led
fraud, and AI traffic.*



About HUMAN

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We ensure that every digital interaction, transaction, and connection is authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information, visit www.humansecurity.com.

