Why Fraud Prevention Must Follow the Entire Customer Journey—Not Just Login or Checkout

In an era of blended threats—from bots and humans to agentic AI.

1. The Reality of Cybercrime

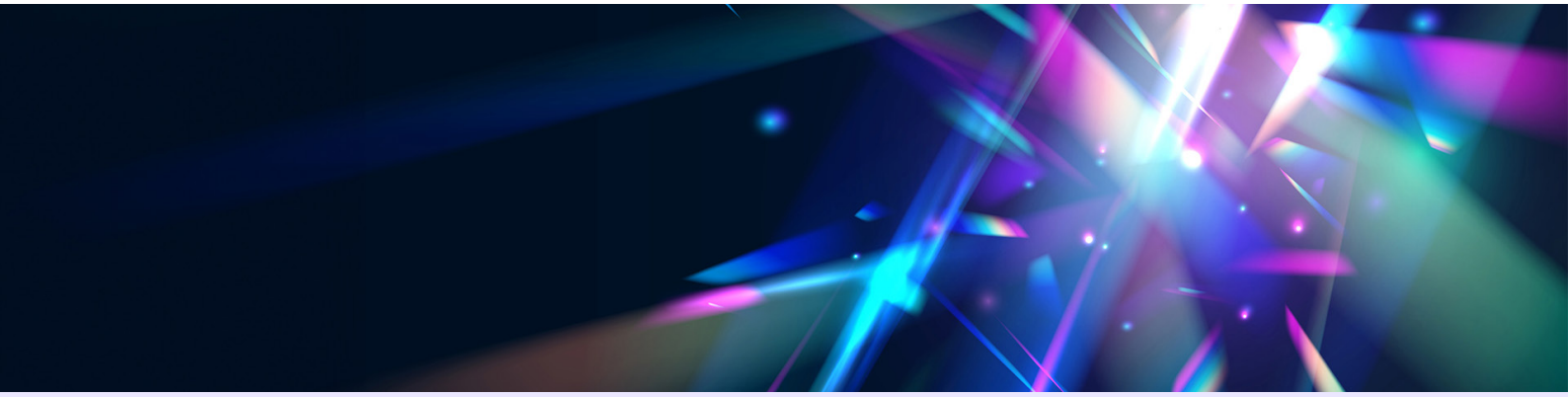
Picture this: At 2:00 a.m., cybercriminals begin trying to break into the accounts of your domain's users, using bots to automatically log into the accounts with stolen credentials.

By noon, the hackers have infiltrated your users' compromised accounts, drained their balances, transferred their gift cards, or stolen their PII. By the time you detect the breach, the damage is already done.

Unfortunately, this scenario is the reality of today's cybercrime. Complex, multi-stage campaigns routinely go undetected by traditional security controls, which are often an assemblage of siloed single-method checkpoints with dangerous gaps between them.

To adapt to this reality, the fraud-detection paradigm is undergoing fundamental changes. Instead of bolting isolated tools onto individual touchpoints, modern threat detection requires end-to-end visibility each time your domain, application, or API is accessed, from the moment the first pixel renders in a user's browser to the moment the transaction is completed.

Only a holistic approach centered on an entire session can reveal the full narrative of an attack and allow your organisation to disrupt fraudsters at any stage.



2. Why Traditional Security Falls Short

Siloed Tools Create Dangerous Blind Spots
Many companies still use separate tools for login security and payment risk checks. These systems typically don't share information with each other, and this type of isolation creates blind spots.

For example, an attacker can test stolen credentials one night, then use those same credentials hours or days later to make fraudulent purchases. Because the login and payment security tools don't share information, no single team is alerted to the coordinated attack until it's too late. Meanwhile, thanks to this same disconnect between login and checkout security, nobody was monitoring the attacker's activity while they were actually accessing the compromised account. That's why a fully integrated security system should continue to evaluate user activity within accounts in order to flag signs of compromise.

> Traditional security tools focus on individual suspicious requests, rather than connecting the dots among various types of suspect activity and synthesising that data into a full picture of a cyberattack, which can often unfold gradually, over days or weeks.

Modern fraud groups often use slow testing methods to avoid triggering security alerts. In order to understand the purpose behind these distributed activities, which can appear harmless in isolation, you have to be able to stitch together a complete narrative using information from various sources and across the timeline of the attack: login attempts, form entries, transaction attempts, and so on.

3. The Blended Threat Reality

Digital businesses now face a mix of human fraudsters, malicious bots, and AI-driven threats. Traffic from automated bots continues to rise, and it can be difficult to distinguish the good bots from the undesirable ones. Meanwhile, sophisticated bots, AI, and real people can produce similar activity patterns, making it even harder to tell good activity from bad.

Fraudsters use automated bots, AI-enabled tactics, and manual human actions to commit account takeover, scraping, carding, fake account abuse, and more.

The upshot is that companies can no longer rely on single-method defense systems to keep up with the ever-changing tactics of this blended threat environment. To effectively protect their business as well as their customers' experience, companies now need smarter solutions that can quickly and accurately figure out which traffic is fraudulent and which is legitimate, regardless of who (or what) is making each request.

4. Emerging Security Challenges & Opportunities

But the blended threat reality doesn't stop with humans and bots — the next wave is already here, powered by agentic AI.

The rapid evolution of artificial intelligence is creating new classes of sophisticated, automated traffic. While much attention has been paid to AI-driven crawling and content scraping, the most significant long-term shift is the rise of autonomous AI agents, systems that can reason, plan, and execute complex goals on behalf of a user.

This increased autonomy and capability introduces a new wave of cybersecurity challenges, which must be taken seriously.

Agentic AI also creates a new question for security, fraud, and detection teams: as these agents interact with websites and APIs, how can we distinguish between legitimate, productive automation and wasteful or malicious activity?

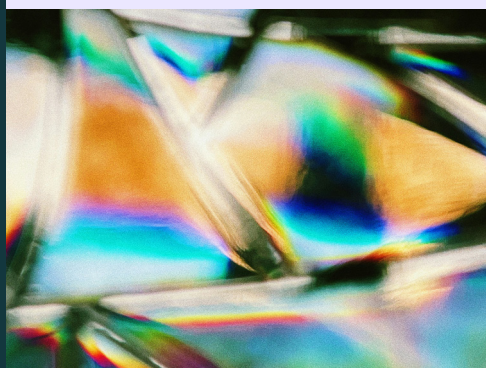
Organisations need complete visibility into traffic behavior in order to enable legitimate visitors, authorised bots, and trusted AI agents to interact with applications on their terms.

The Agentic AI Opportunity
Businesses are embracing agentic AI for its transformative potential to enhance efficiency and revolutionise the customer journey, particularly in B2C sectors. By enabling personalised assistance and automating complex interactions, businesses can unlock new opportunities through agentic commerce. The potential impact of agentic AI is immense; According to Gartner®, "by 2035, 80% of internet traffic could be driven by AI Agents."[1]

This shift demands a new posture: not all bots are threats. Success in the agentic era will depend on the ability to verify and trust automated agents, not simply block them.

That's why we built **AgenticTrust**, a new module in **HUMAN Sightline**, built to give you visibility, control, and adaptive governance over agent-based activity in your websites, applications, and mobile apps.

According to Gartner®, "by 2035, 80% of internet traffic could be driven by AI Agents."[1]



What Agentic Adoption Looks like Today
Our own telemetry confirms this acceleration. HUMAN verifies over 20 trillion digital interactions weekly, giving us a unique vantage point into traffic trends. In just eight months of 2025, agentic traffic increased more than 1,300%, driven largely by the releases of commercial agents like ChatGPT Agent and Perplexity Comet.

By examining the page paths and interactions of AI agents, we can observe that the vast majority of agentic interactions signal commercial intent. Approximately 87% of all pages browsed by agents were related to products. This means that blocking agent traffic turns away potential customers. Most agents are acting on behalf of real users; if they can't access your product pages, they simply move on to another merchant that allows them to complete the task. In other words, every blocked request risks a lost sale.

[1] Gartner, Gartner Futures Lab: The Future of Identity, 7 April 2025 GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission.

5. What "Full Customer Journey" Really Means

Effective fraud defense means coordinated detection and mitigation across all the stages of the customer journey, adapting to the specific risks that can arise before, during, and after authentication:

Journey Stage	Representative Threats	Key Detection Goals
Pre-auth (unknown visitor)	Credential stuffing, fake-account farms, scraping reconnaissance	Device & behavioral fingerprinting, compromised credential checks
At-auth (login/sign-up)	Account takeover, brute force, promo abuse	Adaptive challenges, stolen-credential interception
Post-auth (in-session)	Transaction fraud, data exfiltration, refund scams	Behavioral anomaly detection, policy-aware friction

Taking a holistic view of the entire user session illustrates that different parts of the journey require distinct tools; and also how those tools can work together to create a detection system that can rise to the challenge of today's complex fraud schemes.

5. What "Full Customer Journey" Really Means

Effective fraud defense means coordinated detection and mitigation across all the stages of the customer journey, adapting to the specific risks that can arise before, during, and after authentication:

1. Continuous Session Analytics
The key to spotting complex attacks is having the ability to string together, in real time, every request placed by a user during a session.

The most sophisticated security telemetry platforms analyse trillions—or in HUMAN's case, quadrillions—of interactions to detect new behavioral anomalies that single-purpose tools are often blind to.

When these data are combined with real-time session visibility, it's possible to pinpoint suspicious request sequences before financial or reputational harm occurs.

2. Intent-Aware Bot / Human Differentiation
Because of the increasingly blurry line between malicious bot and human behavior, as well as the rapid increase in overall bot traffic (including AI-generated traffic), it's more important than ever to determine the intent behind each visit to your domain.

Today, it's not enough to simply distinguish bots from humans. Your security system needs to be sensitive enough to tell the difference between fraudulent human actions and desirable ones, and distinguish malicious bots from good ones; for example, it should be able to discern a cybercriminal's browsing behavior from that of a regular customer, and the behavior of a malicious web scanner bot from that of a search engine's indexer.

A truly unified system should also allow a comprehensive and transparent view of traffic generated by AI systems, so that you can tailor your AI governance strategy to your business context (or even monetise traffic from data-hungry agents, using TollBit or similar integrations).

To achieve this level of granularity, advanced detection engines use advanced machine learning models to monitor inputs like mouse movements and device data throughout each user session. This allows these systems to block threats at the edge, with the added benefit of allowing smoother access for genuine users and trusted services (see point #4 below).

3. Secondary Detection and Investigation

With the comprehensive visibility that comes with full-journey protection, security teams don't just gain the real-time ability to make informed decisions about traffic from bots and AI agents and address threats as they unfold. This level of visibility also enables extensible insights that allow the continual and rapid adaptation of your cybersecurity system after the initial detection event has passed.

Secondary detection is the process of analysing threat data after the initial detection and mitigation event. This reveals connected fraud networks, hidden attack patterns, and isolated bot characteristics, actions, and attack paths. AI models track specific attacker adaptations, allowing for faster investigations and threat response in the future.

4. Adaptive, Business-Aligned Mitigation

Successful fraud prevention means finding the right balance between strong security and smooth business operations.

Risk-based authentication allows full control over when and how extra security checks are triggered, which gives an organisation the ability to adapt its authentication system to its specific needs. How the system responds to triggers like unusual transactions or logins from unfamiliar devices can be tailored to each organisation's specific business needs and risk profile.

This flexible approach keeps the user experience smooth and convenient while also delivering strong fraud prevention.

5. Unified Data & Reporting

Unifying all of an organisation's security, fraud, and bot-detection insights in a single platform can produce significantly improved business outcomes, in addition to simple fraud reduction.

For example, **one study** found that a footwear brand, by controlling traffic from reseller bots that had previously hoarded 80 percent of its limited-edition sales, was able to not only reduce its infrastructure costs but also improve its long-term revenues by increasing overall customer satisfaction and retention.

To extend this scenario: In a unified system, data gathered while mitigating the inventory hoarding bots wouldn't be discarded; it would be stored as an attack profile and re-ingested into the system's detection models, which would allow the system to better detect further inventory-hoarding behavior in the future.

7. The Business Case for Full-Journey Defense

The Benefits of Full-Journey Coverage
Today's sophisticated cyber threats require comprehensive visibility and adaptive defenses across the entire customer journey—from the first pixel loaded to the final transaction. Traditional, fragmented security approaches create dangerous gaps, allowing threats to evolve undetected.

That's why full-journey protection isn't just a security upgrade—it's a business imperative. By unifying monitoring and decision-making across every stage of user interaction, organisations gain the visibility, control, and context they need to stop threats before they escalate, while reducing customer friction and supporting strategic goals.

Full-journey coverage reduces fraud loss by linking signals across the attack lifecycle—from credential stuffing to gift card fraud to refund abuse—catching patterns that point solutions miss. Scenario-optimised mitigations lower friction for legitimate users by applying only the right intervention at the right time. And unified telemetry enables faster investigations, stronger governance, and more confident decisions across fraud, identity, and security teams.

Interested in finding out more?

Here's how HUMAN delivers full-journey protection with **HUMAN Sightline Cyberfraud Defense:**

Adaptive Learning:
Continuously evolving layered AI models proactively detect and counter emerging threats.

Agentic AI Visibility & Control:
Enable legitimate AI interactions while proactively preventing unwanted or risky AI-driven activities.

Customisable Mitigation & Governance:
Dynamically apply appropriate controls—from hard blocks and soft challenges to silent interventions and investigative triggers—that seamlessly integrate into your existing security stack (WAF, CDN, IAM, fraud operations).

Known Bots, LLMs, and AI Management:
Gain complete visibility into bots and AI-driven traffic, with granular controls to block, allow, redirect, or monetise interactions.

Secondary Detection & Investigative Intelligence:
Uncover complex fraud networks, unique threat profiles, and evolving attack patterns to accelerate investigations with precise AI-generated insights.

Contextualised Business Signals:
Balance friction and mitigation actions tailored to your organisation's revenue and security objectives, turning security events into positive business outcomes.

Explore **HUMAN Sightline** in more detail.

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**