The Quadrillion Report: 2025 Cyberthreat Benchmarks

HUMAN

The Quadrillion Report: 2025 Cyberthreat Benchmarks

Table of Contents

1.

Introduction

The Human Defense Platform analyzes more than one quadrillion internet interactions every year, detecting how and where threat actors attempt to exploit vulnerabilities in the customer journey.

Users face risks at every point of this journey, from interacting with digital ads to creating accounts, logging in, and completing transactions. More than 500 customers and organizations rely on HUMAN for protection against these threats.

HUMAN's researchers analyzed these interactions from 2024 to identify new, emerging, and ongoing threat patterns and tactics. This report explores trends in several common threat vectors: account takeover attacks, fake account fraud, transaction abuse (carding attacks), scraping, and digital skimming (e.g., Magecart).

The report also identifies how specific industries are targeted by threat actors in particular ways, such as web scraping attacks on retail and e-commerce websites, carding attacks on financial services websites, and account takeover attacks on streaming and media websites.

Finally, the report delves into "big questions" surrounding major industry topics like artificial intelligence/language-learning models and major product releases.

The Human Defense Platform analyzes more than

1,000,000,000,000,000

internet interactions every year, detecting how and where threat actors attempt to exploit vulnerabilities in the customer journey.

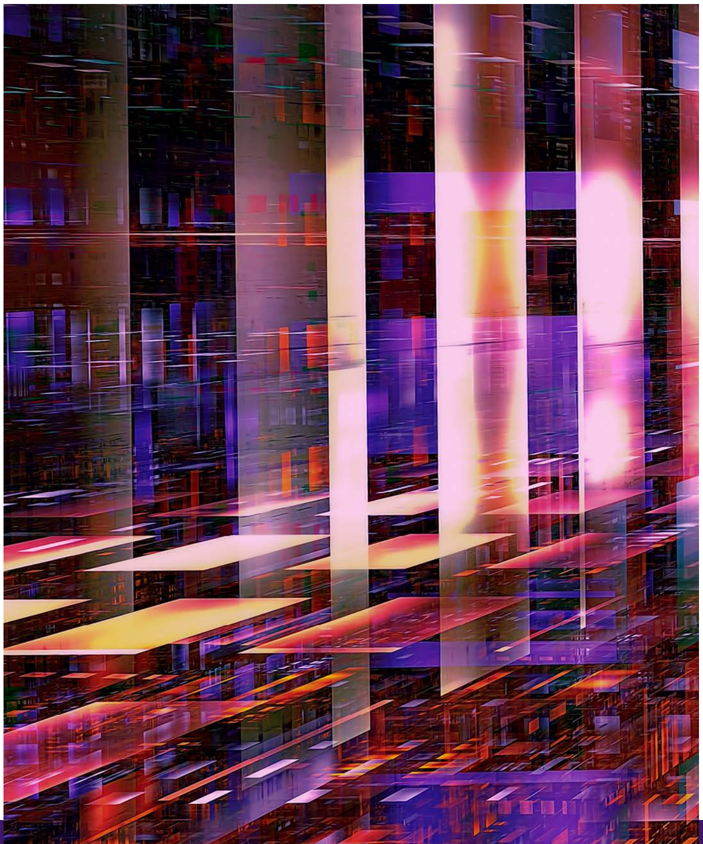
2.

Research Methodology

The data in this report was collected from interactions observed by the Human Defense Platform of HUMAN's cybersecurity customers on an aggregated, anonymized basis, which make up a subset of the full set of interactions observed by the platform.

Throughout this report, we've used the term "the typical HUMAN customer" to reference the **median** value in the data set described. Additionally, we've used the term "heavily-targeted HUMAN customer" to reference the value at the **90th percentile** for the data set described. These two values were selected to reduce the impact of outliers and extreme cases and to give an accurate representation of the trends observed.

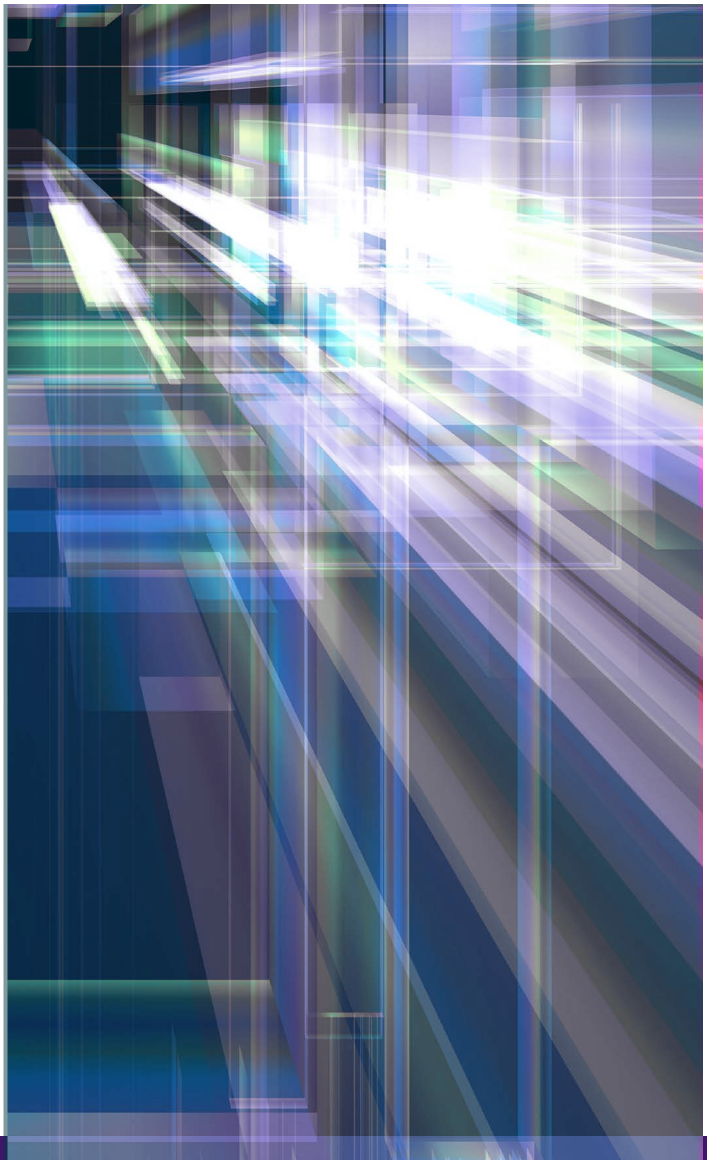
Please note: earlier iterations of this report (The Quadrillion Report: 2024 Cyberthreat Benchmarks and 2023 Enterprise Bot Fraud Benchmarking Report) presented data differently, normalizing figures to the 75th percentile. For that reason, it is inadvisable to compare figures across reports.



3. Executive Summary

The Quadrillion Report: 2025 Cyberthreat Benchmarks explores sweeping cybersecurity trends and attack patterns, highlighting the distinct threats faced by various industries and the evolving nature of cyberattacks observed by the Human Defense Platform.

Last year's report introduced **account fraud** (post-login account compromise attacks and fake account creation attacks) as a key coverage area for our research, in addition to our insights into **account takeover** (ATO), **transaction abuse** (carding), and **scraping** attacks. This year, we build on that foundation by exploring the monetary motivation behind these attacks. This year's report also looks at both the *typical* HUMAN customer as well as the *heavily-targeted* HUMAN customer, to give a perspective of what it looks like when threat actors level their sights on your business.



Let's start with some key findings:

In 2024, **HUMAN stopped**

67 billion
fraudulent login requests

2.8 billion
carding attack attempts

215 billion
scraping attack attempts

Attempted **ATO** attacks **more than doubled** year over year, with the biggest increases in the

streaming/media industry
199% increase
in **attempted attack volume**

&

travel/hospitality industry
215% increase
in **attempted attack volume**

Attempted **carding** attacks **grew most rapidly** in the

travel/hospitality industry
166% increase
in **attempted attack volume**

&

technology, SaaS, & services industry
410% increase
in **attempted attack volume**

Attempted **scraping** attack rates are **climbing rapidly** for companies in many industries, especially in the

retail/e-commerce industry
81% increase
in **attempted attack volume**

&

streaming/media industry
56% increase
in **attempted attack volume**

Last year, HUMAN identified and flagged

nearly 800,000 fake accounts per customer,

an **increase of 360% from 2023**.

SATORI

Satori Threat Intelligence researchers contributing to this report observed that attacks are getting increasingly complex and that threat actors are increasingly teaming up to distribute the workload—and the risk—among larger groups, enabling faster, more efficient, and multi-stage attacks.

In addition to our coverage of attack vectors and targeted industries, researchers explored two key questions that provided a through-line across their research:

1. **How is AI being used to aid both attacks and defenses?**
2. **What forces are at play during major product releases like ticket drops?**

AI's use by threat actors is complex. Large Language Models (LLMs) don't overtly provide cybercrime help, but tools can "jailbreak" them to develop attacks. AI acts as a "smart intern" for attackers, automating attack processes. The imminent arrival of Agentic AI, or semi-autonomous bots, complicates the issue further: while they can be used for new attacks, they can also be beneficial to a website owner in their capacity to make purchases on behalf of customers. If the guardrails are sufficient, agentic AI may be a net positive for businesses, but how quickly can those guardrails arise?

High-demand product releases are predictable, enabling scalpers to exploit the system. They use monitor bots to detect release events on target websites or APIs. Once a release is detected, all-in-one (AIO) bots automate the purchase process, securing items before genuine buyers. Scalpers often organize in "cook groups," sharing resources like tools, knowledge, proxy pools, and even resale services to maximize their efficiency and profitability. This coordinated approach gives scalpers a significant advantage in obtaining limited-release items.

Finally, next year's Quadrillion Report will incorporate insights from the newly-released HUMAN Sightline capabilities, which enable customers to track bot profiles and adaptations across time. Current HUMAN customers can get a jump-start on those findings by monitoring their properties in the console.

4.

Attack Trends

This report categorizes enterprise-focused attacks observed by the Human Defense Platform into the following broad categories:

- Account takeover (ATO) attacks
- Account fraud (including fake account creation and post-login account compromise)
- Client-side attacks (like digital skimming and script injection)
- Carding attacks
- Web scraping attacks

Each of these categories includes multiple attack targets and tactics, and most incorporate automation at some stage of the attack path. Other fraud schemes require manual intervention, but are still detectable by the Human Defense Platform.

This section will explore patterns in attack rates and offer examples of attacks that were identified to illustrate what it means to fight fraud.

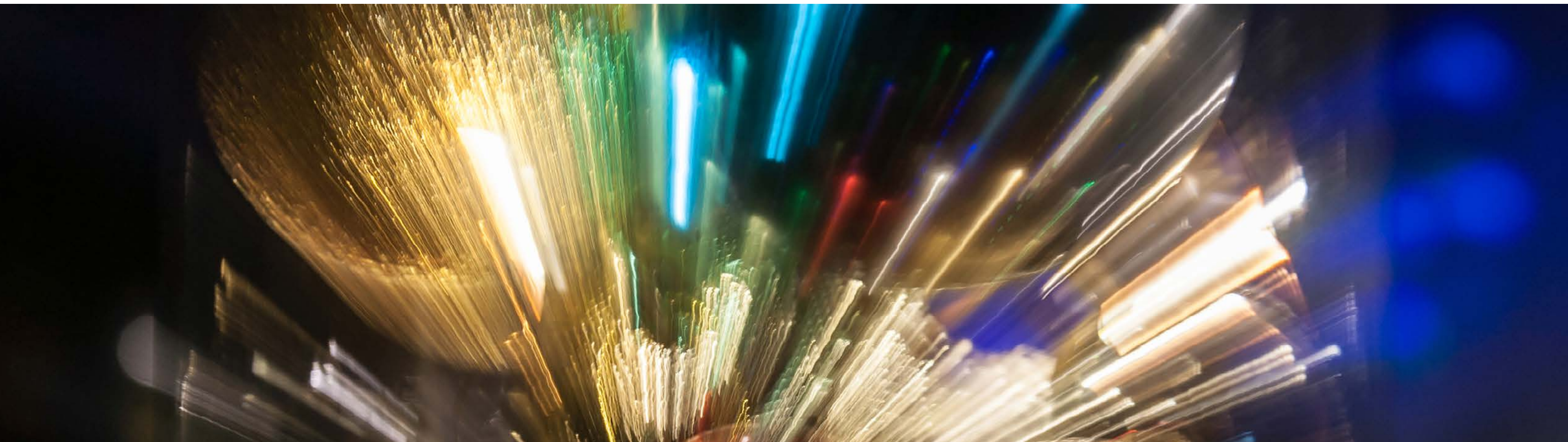
Account Takeover Attacks

Account Fraud Attacks

Client-Side Attacks

Carding Attacks

Web Scraping Attacks



Account Takeover Attacks

Account takeover attacks are among the most common—and lucrative—attacks for a threat actor to pursue. A successful attack can result in a threat actor making lots of money selling the hacked accounts downstream to other threat actors.

The sold hacked account can be drained of funds or loyalty program balances, used to make fraudulent purchases, write fake reviews, distribute spam and malware, or harvest saved payment information or personally identifiable information (PII).

These attacks occur most frequently as a result of a data breach, with harvested credentials sold from one threat actor to another and used to target accounts whose users reuse passwords from one account to the next.

Common methods used to take over accounts are **credential stuffing** (threat actors using leaked credential pairs on many login portals to find accounts that work) and **credential brute-forcing** (threat actors attempting to brute-force a successful credential pair on a particular website).

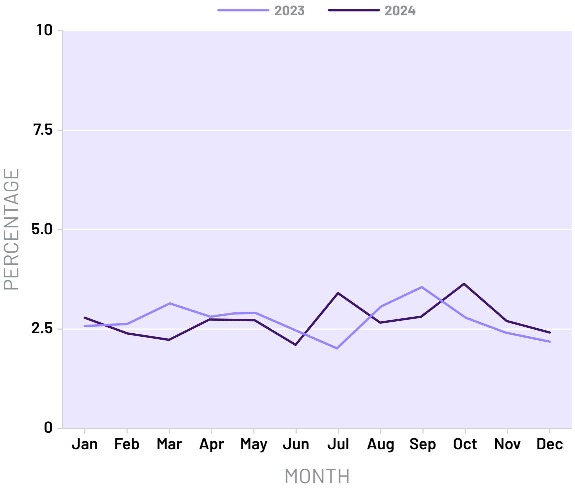
Key Findings:

- HUMAN flagged **more than 67 billion** fraudulent login requests in 2024, **more than double** the number of requests blocked in 2023.
- Attempted attack rates on highly-targeted companies peaked at **50% of login requests**.
- The value of a hacked account ranges from **a few dollars to thousands of dollars per account**, depending on stored balances, reinforcing the importance of protecting accounts from compromise.

*HUMAN flagged **more than 67 billion** fraudulent login requests in 2024.*

Below, the median of attempted ATO attacks, month-by-month, for both 2023 and 2024, showing the attack rate in both years. Overall, the rate of attempted ATO attacks in 2024 was roughly even with 2023:

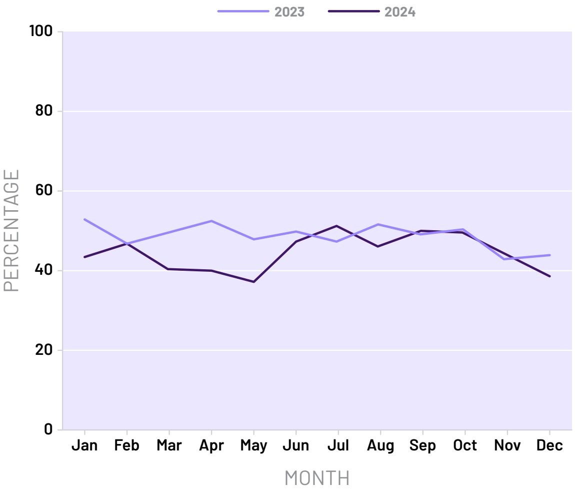
Median Rate of ATO Attack Attempts, Month by Month



Above is the ATO attack rate for the typical HUMAN customer. Attack rates were slightly lower year-over-year through the late winter and early spring of 2024, but ticked up over the second half of the year. However, not all businesses are targeted equally; consider the value to a threat actor of a hacked cryptocurrency account as opposed to a hacked newspaper website. One holds enormous resale value, while the other doesn't. (More on which attacks occur most frequently on which industries in the Industry Trends section.)

The rate of attempted ATO attacks for heavily-targeted businesses is much starker:

Heavily-Targeted Businesses, ATO Attack Attempts, Month by Month



Attack rates fluctuated more for these key targets throughout 2024. At their peak, attempted ATO attacks made up approximately **50% of all traffic to login pages**. Peak activity occurred in summer and early fall for both typical and highly-targeted HUMAN customers.

Privacy Affairs, an independent research and consulting organization, published a "Dark Web Price Index" with estimated costs for hacked accounts across a wide variety of businesses and business types. Those costs range from a couple of dollars per account for streaming services to tens or hundreds of dollars per account for rideshare, airline, social media, or email providers, to thousands of dollars per account for banks and cryptocurrency platforms.

Hacked accounts are valuable for more than just tampering with account or loyalty balances. Satori researchers identified several downstream threat actor activities that follow a successful ATO:

- **Buy4You services**, in which a threat actor uses a hacked account to make a purchase on behalf of a third party. The threat actor attaches the shipping or delivery address to the hacked account and completes the purchase, draining the account of funds without exposing the threat actor's own information to the platform or the ATO victim.
- **Enriching before resale**, in which threat actors buy low-balance accounts in bulk with the intention of reselling them for more later on.
- **Form spamming**, in which a threat actor with a hacked account spams other accounts on the platform with affiliate links or malware.

Researchers also identified a "warranty" system some threat actors offer when selling stolen accounts: if the original account is lost, the threat actor offers a replacement account of equivalent value.

Satori Perspectives

Increased Sophistication in Account Takeover Attacks

In 2024, researchers saw an increase in advanced spoofing techniques, such as TLS spoofing. TLS spoofing is the practice by which an attacker imitates the HTTPS connection patterns of a device other than the one that is actually originating the requests. Some solutions use the fingerprints of those connections as a part of their detection methodologies, prompting attackers to try to impersonate these fingerprints as well.

In the Wild

High-Volume Targeted ATO Attacks

One HUMAN customer in the retail industry experienced a months-long assault on its login portals. Beginning in November 2023, the rate of ATO attempts on this retailer exceeded **78%** of traffic to the login portal. That rate climbed above **97%** two months later, and didn't fall below 90% of traffic until December 2024.

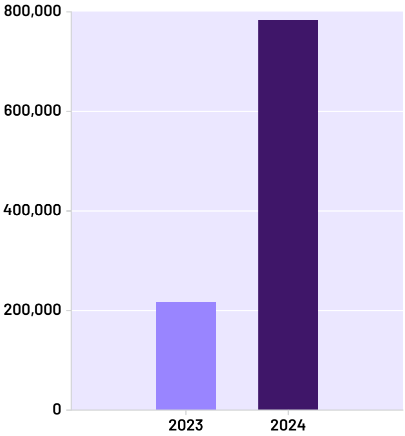
HUMAN's retail customer was protected from this months-long ATO attack.

Account Fraud Attacks

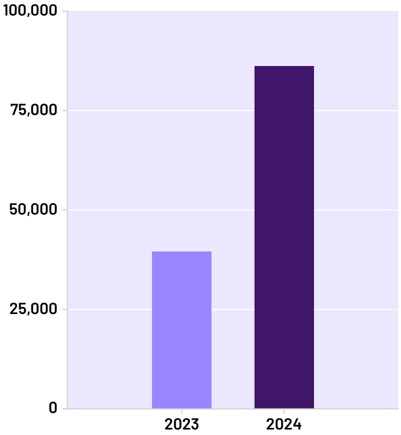
Account fraud is a wide-ranging umbrella term that includes both the creation of fraudulent accounts and the exploitation of legitimate accounts after the point of login (rather than at the point of login, as ATO attacks do).

Account fraud attacks rose dramatically from 2023 to 2024. On a per-company basis, the number of post-login compromises (flagged by the Human Defense Platform before being exploited by threat actors) **more than doubled** year-over-year, while the number of fake account creation attempts skyrocketed, with a more than **360% increase** in the number of attempts.

Fake Account Creation Attempts Per Company



Post-Login Account Compromise Attempts Per Company



Key Findings:

- HUMAN identified and flagged nearly **800,000 fake accounts** per customer in 2024, an increase of **360%** from the previous year.
- Likewise, HUMAN identified more than **78,000 post-login account compromise attempts** per customer in 2024, more than double the previous year.
- The value of fake accounts varies widely depending on the capabilities of the platform on which the account is created, but they can be monetized en masse to inflate follower/like counts or spread malware through messaging tools.

One common example of post-login fraud is **cookie theft**, which enables a form of session hijacking. If a cybercriminal steals your browser cookie for a retail website, they can effectively hijack your session. This allows them to access your account and perform actions as if they were you, mimicking the effects of an ATO attack.

*HUMAN identified and flagged nearly **800,000 fake accounts** per customer in 2024.*

The majority of account fraud attacks identified and stopped by the Human Defense Platform in 2024 were attempts at fake account creation or post-login account compromise.

The value of a fake account versus a hacked account depends heavily on the platform and the account's intended use. For example, many major internet platforms have more fake account activity than account takeover activity because fake accounts are cheaper and easier for threat actors to stage than it is to break into accounts at scale. Fake accounts on those platforms can be used for phishing attacks, as tools for abusing loyalty programs, or for misinformation. In contrast, fake accounts are less valuable than hacked accounts on a gaming/gambling site. A hacked account may have a stored account balance, while a fake account wouldn't.

On the dark web, likes or followers on social media and music sites only cost a dollar or so per thousand, according to Privacy Affairs. The source of these likes and/or follows are often fake accounts spun up en masse by threat actors.

Satori Perspectives

The Resource Demands of Post-Login Attacks

Post-login attacks like certain carding operations are especially complex. Those attacks often require payment details, billing addresses, PII, and shipping destinations. They also require a deep understanding of the security measures employed by the target website, payment processors, and credit card companies. Notably, these attacks are often manual, not bot-operated. Carding operations like these often include a "contemplation" period in which items similar to the one eventually used for the attack are added and then removed from the threat actor's cart, "warming up" the account for the attack.

In the Wild

SaaS Platform Targeted in Massive Fake Account Attack

One HUMAN customer in the SaaS industry was targeted with a large fake account creation attack attempt in December 2024. Over the course of the month, the Human Defense Platform flagged more than **4.1 million** fake accounts. The attack peaked on December 29th, with more than **140,000** fake accounts flagged, largely being used with the intent of sending messages containing links to malware through the platform's messaging tool.

HUMAN's SaaS customer was protected from this extensive fake account attack.

Client-Side Attacks

Client-side attacks are made up of code that's delivered to and executed on the end user's machine rather than on the site's server. Some common varieties of these attacks are digital skimming (a.k.a Magecart) attacks, PII and credential harvesting, and cryptojacking. Attacks like these can be virtually invisible to the user, but can have devastating downstream consequences, like carding and ATO attacks, reduced computer performance, and identity theft.

Client-side attacks are more complex to set up than many other attacks, but the payoff for a threat actor can be significant, as they can harvest payment card information, login credentials, and other PII directly from the user.

PCI DSS 4 now requires businesses that accept payments online to secure their payment page browser scripts from client-side attacks. These organizations must inventory, authorize, justify, and assure the integrity of payment page browser scripts (requirement 6.4.3) and detect modifications to security-impacting HTTP headers (requirement 11.6.1), or otherwise confirm that they are not susceptible to attacks from scripts.

Satori Perspectives

How Attackers Use Automation to Find Targets for Client-Side Attacks

Threat actors often use automated tools to scan the internet for servers or web applications with known vulnerabilities. When a new vulnerability is discovered on a popular CMS, web server, or client-side plugin, threat actors deploy scanners to identify unpatched instances of these vulnerabilities. Automated scripts can be configured to look for specific signatures in websites or servers, such as outdated software versions, misconfigurations or improperly implemented security mechanisms. Once a vulnerable target is identified, attackers can exploit these weaknesses to inject malicious code, such as in cross-site scripting (XSS) attacks or by injecting malicious ads or scripts into otherwise legitimate web pages.

In the Wild

Fake Forms Coming From Mimicked Vendors Targeting Payment Pages

HUMAN researchers uncovered a Magecart-style attack on a website that used a prominent payment provider. The attacker used a technique called **vendor mimicking** to disguise the script as a real vendor on the site, and replaced the real payment form with its own fake payment form. Vendor mimicking is an umbrella term for techniques that are designed to make a script appear to belong to a real vendor to anyone taking a look at the network or site content by either disguising the malicious domain via domain mimicking, or disguising the script's content by adding top comments from the real vendor's script. The fake form collected payment card information and relayed it back to the threat actor.

HUMAN helps customers protect against fake forms coming from mimicked vendors.

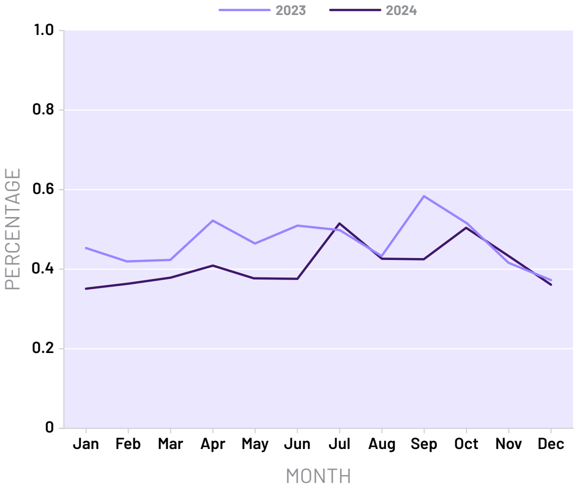
Carding Attacks

Carding is a method cybercriminals use to verify stolen payment card information. They make small test purchases on e-commerce platforms to see if cards are valid. Once a card is confirmed, they use it for larger transactions, often for digital goods like gift cards, which can be quickly resold.

Unlike attacks that target specific individuals or accounts, carding is primarily about validating the card itself. Attackers are opportunistic; they'll target any site where they can successfully validate a card. This means e-commerce sites can reduce their risk by strengthening their security, making themselves less appealing targets. The costs of being a vulnerable target include chargebacks and increased payment processing fees.

Overall, carding attacks in 2024 were slightly lower than in 2023:

Median Rate of TA Attack Attempts, Month by Month



Above, the carding rate for the typical HUMAN customer. Attack rates throughout the year were lower than in 2023 in all but two months (July and November). As with ATO, carding attack rates vary by industry. The rate of carding attack attempts on the travel and hospitality and e-commerce industries

Key Findings:

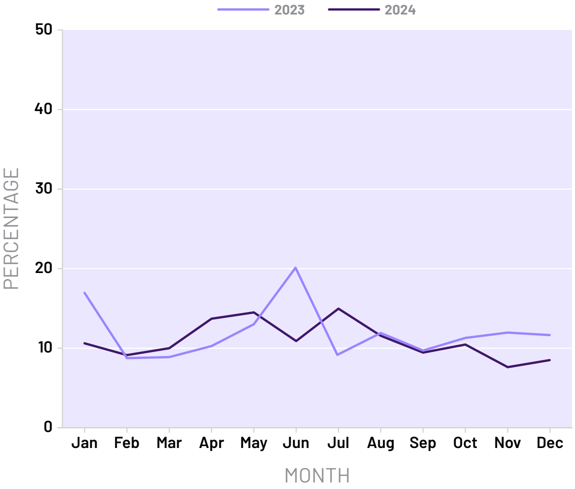
- HUMAN identified and stopped more than **2.8 billion** carding attack attempts in 2024. The share of attempted carding attacks grew most dramatically in the **technology**, **SaaS**, and **services** industry (**more than 1,487% growth year over year**) and the travel and hospitality industry (**more than 700% growth year over year**).
- The vast majority of attempted carding attacks were in the **travel and hospitality** and **retail and e-commerce** industries.
- One HUMAN customer in the retail/ e-commerce industry experienced an attack in which **86% of all checkout traffic** for the day was attempting a carding attack.

*In 2024, HUMAN flagged **more than 2.8 billion** carding attacks.*

were the highest rates among all the industries covered in this report. In 2024, carding attempts accounted for **38.49%** of traffic to checkout pages in the travel and hospitality sector, while retail and e-commerce businesses saw even higher levels —over **51%** of checkout traffic involved attempted carding attacks.

Carding attack attempts on heavily-targeted businesses were roughly even year-over-year:

Heavily-Targeted Businesses, TA Attack Attempts, Month by Month



Attack attempts on these heavily-targeted businesses hovered around **12% of traffic to checkout pages** throughout the year, with a dip just before the holiday season.

Satori researchers described the carding process at a very high level in four steps:

- Obtain card information (potentially through a Magecart/skimming attack as described above)
- Identify target for attack
- Set up a spoofed environment to match the card information
- Test card and drain or resell

The price for validated credit card details ranges from $10 to over $100 per validated card, according to Privacy Affairs. That potential profit for a threat actor underscores the importance of defending against carding attacks but also the earlier stages in the carding process which seed those attacks.

Satori Perspectives

Researchers' monitoring of dark web forums suggests that the legality of an attack doesn't impact how it's discussed among hackers. While carding is illegal everywhere, other forms of transaction abuse—threat actors using bots to beat systems set up for humans for monetary gain—aren't against the law across the board. Indeed, scalping and sniping attacks (which center on the use of bots to purchase popular items) are discussed openly among threat actors, without the need for subterfuge.

In the Wild

HUMAN Defends E-commerce Customer From 150 Million Carding Attempts

One HUMAN customer in the Retail/e-commerce industry experienced an attack in April 2024 that led to **nearly 150 million** carding attempts in that month alone.

HUMAN's retail customer was protected from nearly 150 million carding attempts.

Web Scraping Attacks

Scraping attacks, carried out by bots that visit websites, capture large amounts of data, and then leave, can cause significant damage to businesses. This seemingly innocuous act has several detrimental effects:

- **Loss of IP:** product descriptions or other intellectual property may be stolen
- **Content theft:** content on the website may be reproduced or republished by threat actors with scraper bots, damaging the website owner's reputation and potentially damaging any affiliate relationships
- **Ad fraud:** bot visits to a publisher website may be characterized as fraud in the digital advertising ecosystem
- **Server costs:** excess traffic may result in overage charges for website hosting
- **Competitive edge:** stealing pricing data may hurt a business' ability to compete
- **Breach of ToS:** any site that monetizes access (like some news sites) loses out on money and prestige as a result of scrapers.

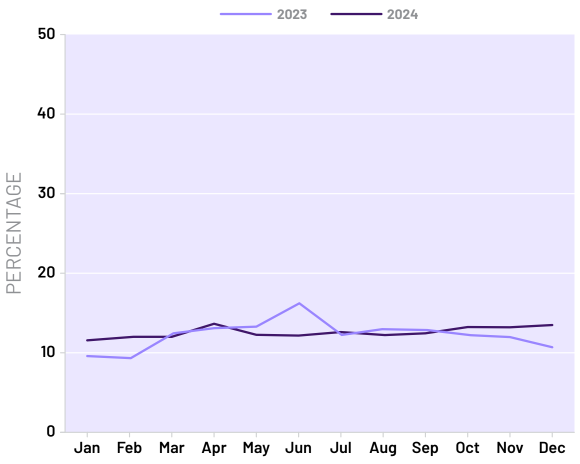
In 2024, HUMAN flagged ***more than 215 billion*** *scraping attacks.*

Key Findings:

- HUMAN identified and blocked more than **215 billion** scraping attack attempts in 2024. The share of attempted scraping attacks grew most dramatically in the **technology**, **SaaS**, and **services** industry (**more than 478% growth year over year**) and the **travel and hospitality industry** (**more than 125% growth year over year**).
- More than 73% of all attempted scraping attacks were on businesses in the **retail and e-commerce** industry.
- Some heavily-targeted businesses saw scraping attack attempt rates exceeding **90%** during month-long attacks.

Overall, the rate of scraping attacks in 2024 was roughly even with 2023:

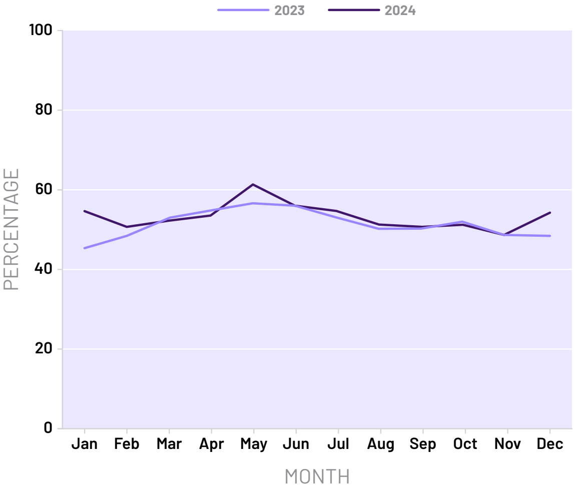
Median Rate of Scraping Attack Attempts, Month by Month



The previous chart shows the scraping attack attempt rate on the typical HUMAN customer. The rate trends upward through the holiday shopping season. Indeed, the highest scraping rate of the year occurred on December 25th, **when scrapers made up 15% of all traffic** to typical HUMAN customers. This elevated rate may reflect reduced human traffic during the holiday, making bot activity more prominent by comparison.

Heavily-targeted businesses saw significantly higher rates of scraping attempts:

Heavily-Targeted Businesses, Scraping Attack Attempts, Month by Month



For heavily-targeted businesses, the stretch between late April and mid-May was especially active. Scraping attempt rates for these businesses peaked at **63% of traffic** on April 26th and hovered around 50% of traffic for much of the year.

The value of scraped data can be surprisingly high, too. Satori researchers explained that data scraped from one high-profile retailer in one location could go for hundreds or thousands of dollars.

Satori Perspectives

Scraping as an Attack Precursor, and Other Use Cases

Satori researchers described some of the use cases for scraping attacks as being precursors to other attacks. For example, "monitor bots" may scrape the price of in-demand items and automatically purchase them if the price drops below a certain threshold. Scraping becomes the precursor to a scalping operation in that way. Many threat actors openly describe their scraping approaches.

Researchers also described a use case for scraped data in launching a new business. Unscrupulous business managers will capture the information from a competitor and deploy it into their own product. Similarly, researchers described observing an attack in the wild in which medical professionals' information was scraped from various databases, giving salespeople lists of cold-call targets.

In the Wild

E-commerce Business Hit with 725 Million Scraping Attempts Monthly

One heavily-targeted HUMAN customer in the retail/e-commerce industry experiences hundreds of millions of blocked scraping attempts every month. In April 2024, HUMAN identified more than **725 million** scraping attempts, accounting for nearly **95%** of traffic to the customer's product pages in that month.

HUMAN's retail customer was fully protected from the scraping attack.

5.

Industry Trends

The Human Defense Platform safeguards a wide range of organizations, from multinational retailers with physical stores to online sports betting platforms, airlines, educational tutoring companies, SaaS providers, and media outlets.

Every business faces unique threats and risks. A financial services organization might be vulnerable to account takeover attacks, while a retailer might be concerned about scalping or price scraping. Even businesses within the same industry may have different concerns. For example, financial services organizations might be at risk for both carding attacks and account takeover attacks, but not to the same extent as other institutions.

For the purposes of The Quadrillion Report, we've separated customers into five industries:

- Travel & Hospitality
- Retail & E-commerce
- Financial Services
- Streaming & Media
- Technology, SaaS, & Services

In reviewing the attack patterns specific to each industry, we can understand how threat actors target industries differently. This section of the report will describe attack activity using **shares**. This represents what percentage of all observed activity targeted a particular industry.

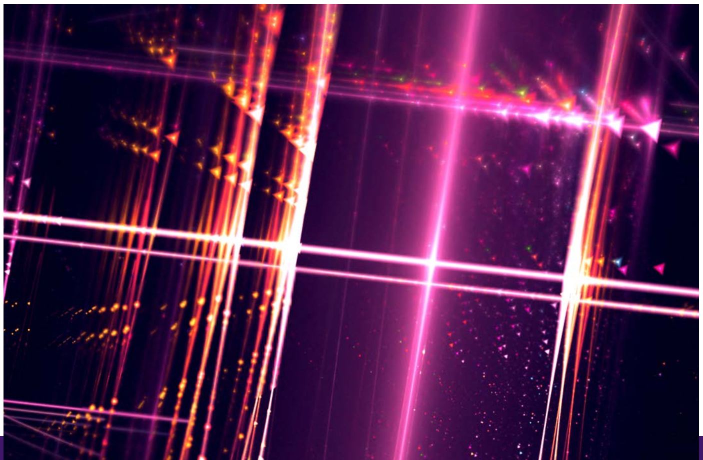
Travel & Hospitality

Retail & E-commerce

Financial Services

Streaming & Media

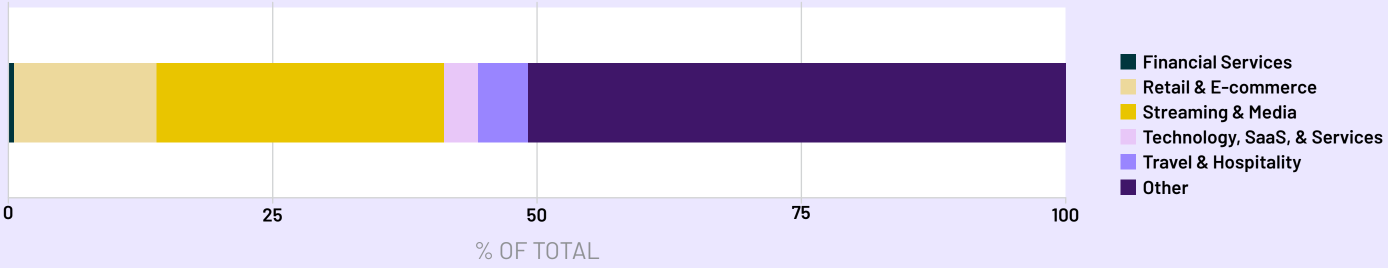
Technology, SaaS, & Services



Below, the breakdown of which industries were targeted by attempted ATO attacks in 2024:

(Note: the financial services industry's share was .4%, too small to be easily seen on the chart.)

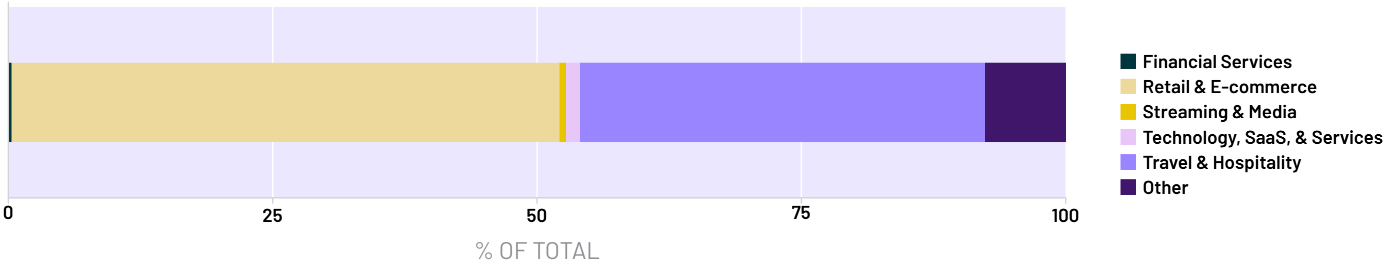
2024 Attempted ATO Attacks By Industry



Below, the breakdown by industry of which industries were targeted by attempted carding attacks in 2024:

(Note: The financial services industry's share was .2%, too small to be easily seen on the chart)

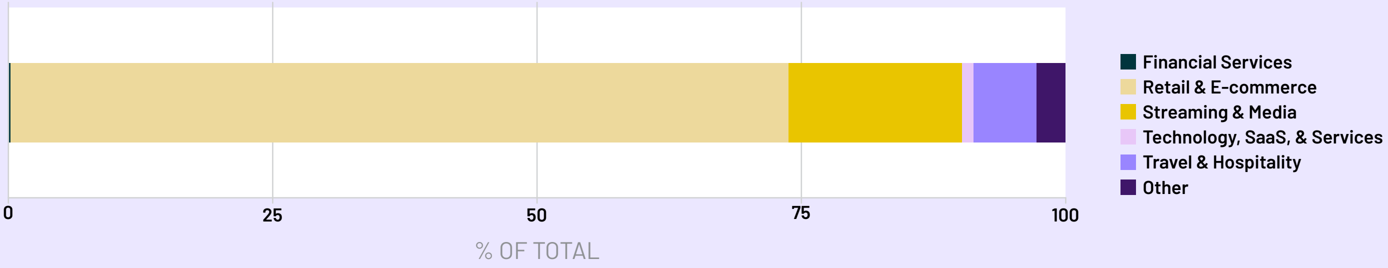
2024 Attempted Carding Attacks By Industry



Finally, the breakdown of attempted web scraping activity by industry in 2024:

(Note: The financial services industry's share is .06%, too small to be easily seen on the chart.)

2024 Attempted Web Scraping Attacks By Industry



Next, we'll go industry-by-industry and look at the last three years of data.

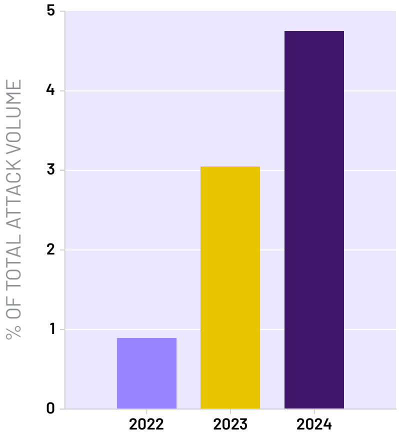
Travel & Hospitality

Businesses in the travel and hospitality industries face a wide range of threats, including:

- Web scraping attacks aimed at collecting pricing information and tracking inventory changes
- Account takeover attacks targeting stored payment information, PII, and loyalty program balances
- Account fraud attacks used to exploit new account sign-up bonuses

As a share of all attempted **ATO** attacks observed by the Human Defense Platform, the percentage of attempted attacks focused on travel and hospitality businesses has increased rapidly over the past three years:

ATO Attacks on Travel & Hospitality Businesses, 2022–2024



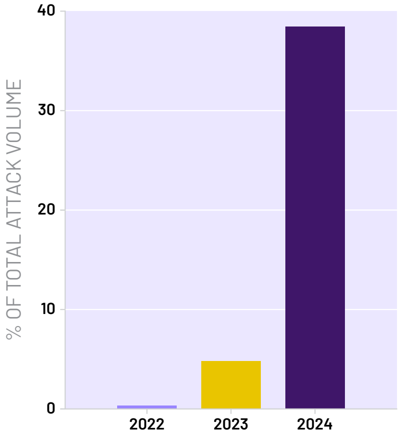
Beginning at a share of less than 1% of attacks in 2022, the share of ATO attacks targeting travel and hospitality businesses grew to more than 3% of attacks in 2023, followed by another jump to 4.76% last year.

Key Findings:

- Attempted ATO attacks on travel and hospitality businesses, as a share of all attempted ATO attacks observed, rose **more than 56% from 2023 to 2024**. This follows the trend of increasing share of attempted ATO activity for the industry.
- Attempted carding attacks jumped a staggering **707%** year over year.
- And attempted scraping attacks climbed **125%** from 2023 to 2024.

As a share of all attempted **carding** attacks observed by the Human Defense platform, the percentage of attempted attacks focused on travel and hospitality businesses has increased dramatically over the past three years:

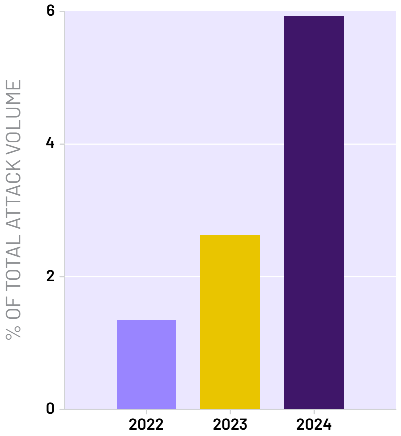
Carding Attacks on Travel & Hospitality Businesses, 2022–2024



In 2022, the travel and hospitality share of attempted carding attacks was less than one-third of one percent. By last year, that share had grown to **more than 38% of all attempted carding attacks**.

As a share of all attempted **scraping** attacks observed by the Human Defense platform, the percentage of attempted attacks focused on travel and hospitality businesses has increased consistently over the past three years:

Scraping Attacks on Travel & Hospitality Businesses, 2022–2024



Here, too, the share of attacks on this particular industry has grown over the past three years, culminating in just under **6% of all scraping attacks** in 2024.

Satori researchers estimate that the cost on the dark web of a hacked account is roughly 10% the market value of the stored balance. That pattern, researchers say, is borne out in this industry: stolen accounts for one major hotel chain were available for between $60 and $300, depending on the number of loyalty points available to the purchaser.

Satori Perspectives

Account Takeovers Fuel Fake Listing Scams

Satori researchers described a novel threat for the travel and hospitality industry: fake listings. Threat actors can break into long-standing accounts on short-term rental websites and use that access to stage fake property listings. With the reputation a long-standing account has, it's much easier to fool a traveler into booking a stay at the fake listing, which the threat actor cashes out and the platform owner has to compensate.

In the Wild

Coffee Company Targeted by Over 28 Million ATO Attempts

One HUMAN customer, a major coffee company, was targeted by a significant ATO attack in September 2024. While ATO attempts leading up to and following that month were generally less than a million attempts/month, in September 2024, the company experienced **more than 28 million ATO attempts**.

HUMAN's customer was protected from this ATO attack.

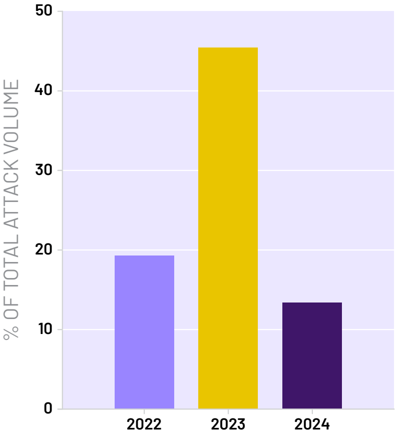
Retail & E-commerce

Retail and e-commerce businesses are prime targets for cyberattacks, including:

- Web scraping attacks to collect pricing or product information.
- ATO attacks to steal stored payment data, gift cards, and personally identifiable information (PII).
- Fake accounts to exploit new user bonuses.
- Carding attacks to test stolen payment card information.
- Client-side attacks to steal payment information during transactions.

As a share of all attempted **ATO** attacks observed by the Human Defense Platform, the percentage of attempted attacks focused on retail and e-commerce businesses has varied widely over the past three years, with a peak of 4**5% of attempted attacks** in 2023:

ATO Attacks on Retail & E-commerce Businesses, 2022–2024

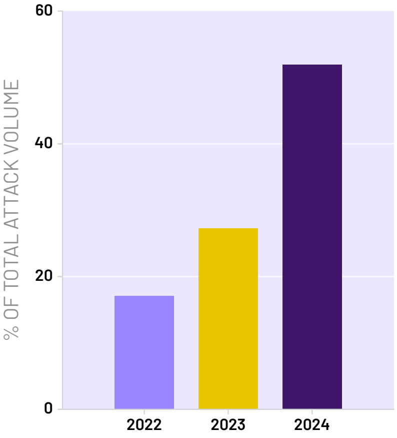


Key Findings:

- The share of attempted ATO attacks targeting retail and e-commerce businesses has been volatile over the last three years, accounting for **45% of activity** in 2023 before retreating to less than **14% in 2024**.
- In contrast, the share of attempted carding attacks targeting retail and e-commerce businesses has climbed steadily, growing more than **90% from 2023 to 2024**, and accounting for **more than half of all attempted carding attacks in 2024**.
- Retail and e-commerce's share of attempted scraping attacks was higher still in 2024, reaching a whopping **73.63% of all attempted scraping attacks**.

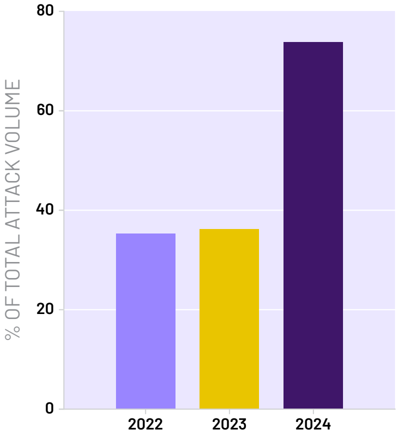
As a share of all attempted **carding** attacks observed by the Human Defense Platform, the percentage of attempted attacks focused on retail and e-commerce businesses has increased consistently over the past three years, climbing to **51.8% of activity in 2024**:

Carding Attacks on Retail & E-commerce Businesses, 2022–2024



Finally, as a share of all attempted **scraping** attacks observed by the Human Defense Platform, the percentage of attempted attacks focused on retail and e-commerce businesses has grown to include the vast majority of all activity:

Scraping Attacks on Retail & E-commerce Businesses, 2022–2024



That's a full **73.6%** of all attempted scraping attacks in 2024, and a rise of more than **105%** year over year.

The rise of scraping attack attempts is concerning but not altogether surprising; eMarketer projects global e-commerce sales to eclipse **$7.6 trillion** in 2025, and targets like limited-edition sneakers and next-generation video game consoles attract scalpers looking to get an edge on the resale market.

Satori Perspectives

High-Demand Products Drive Scalping Attacks on Retail Sites

Satori researchers identified the top items targeted for scalping attacks in underground forums:

- Sneakers
- Next-generation video game consoles
- High-performance computer parts (video and graphics cards)
- Designer clothing
- Trading cards
- Toy figurines

Each of these has significant resale value, so threat actors are highly incentivized to put in the time and effort to attack a retail site to get these items.

Scalping attacks can disrupt inventory management, skew demand forecasting, and leave legitimate customers frustrated—damaging brand reputation and customer trust. Retailers may also face increased operational costs from handling bot traffic, failed transactions, and customer support inquiries.

In the Wild

HUMAN Blocks Carding and Scraping Attacks on Streetwear Vendor

Speaking of sneakers, one HUMAN customer in the retail/e-commerce space with a particular focus on sneakers and streetwear is heavily targeted by a variety of attack attempts. In February 2025, this customer was targeted by a carding attack to the tune of **37 million** attempts. One year prior, in February 2024, the same customer was targeted with an ATO attack in which **74%** of traffic to their login page was attempting to break into a user's account. And scraping attack attempts are exceptionally high for this customer, with more than **4.3 billion attempts** over the course of the year.

HUMAN's customer was protected from all of these carding and scraping attacks.

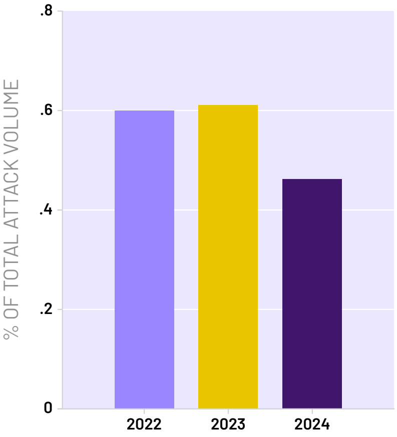
Financial Services

Financial services organizations are frequently targeted by attacks aimed at stealing money, due in large part to the fact that they manage significant amounts of it. These attacks include:

- Account takeover attacks (to drain account balances)
- Carding attacks (to test credit cards)
- Client-side attacks (to collect PII)

As a share of all attempted **ATO** attacks observed by the Human Defense Platform, the percentage of attempted attacks focused on financial services businesses has been relatively consistent over the past three years, with a drop from 2023 to 2024:

ATO Attacks on Financial Services Businesses, 2022–2024

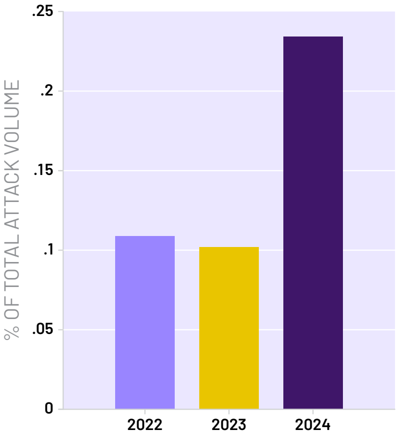


Key Findings:

- The share of attempted ATO attacks on financial services businesses **fell more than 24%** from 2023 to 2024, and remains low overall.
- In contrast, the share of attempted carding attacks on financial services businesses **jumped 130%** year over year.
- Financial services businesses' share of attempted scraping attacks **fell 14.29% year over year** and remains low.

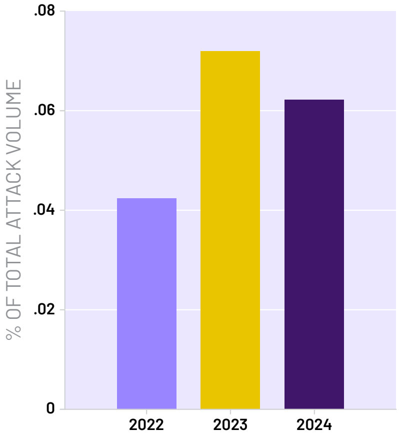
As a share of all attempted **carding** attacks observed by the Human Defense Platform, the percentage of attempted attacks focused on financial services businesses **has increased more than 130%** from 2023 to 2024 after a slight decline from 2022 to 2023:

Carding Attacks on Financial Services Businesses, 2022–2024



Finally, as a share of all attempted **scraping** attacks observed by the Human Defense Platform, the percentage of attempted attacks focused on financial services businesses fell slightly over the past year after a rise from 2022 to 2023:

Scraping Attacks on Financial Services Businesses, 2022–2024



Satori Perspectives

The Vertical Fraud Ecosystem Targeting Financial Services

Satori researchers described "vertical" ecosystems for fraud on financial services organizations, in which threat actors offer specialized services for different parts of the attack chain. For example, one threat actor may interact directly with a target to obtain the PII needed to break into an account or deliver malware, another threat actor "mules" the money away from the target's account, a third owns a foreign account into which the stolen money is deposited, etc. This structure allows attackers to assemble complex operations by purchasing services from specialized providers—reducing individual risk and lowering the barrier to entry for financial fraud.

In the Wild

Sustained Scraping Attack Targets Financial Services Platform

An international HUMAN customer in the financial services industry experienced a months-long scraping attack in the first half of 2024, with scraping attempts accounting for **50% or more of all website traffic** during each of the first six months of the year.

HUMAN's financial services customer was protected from this scraping attack.

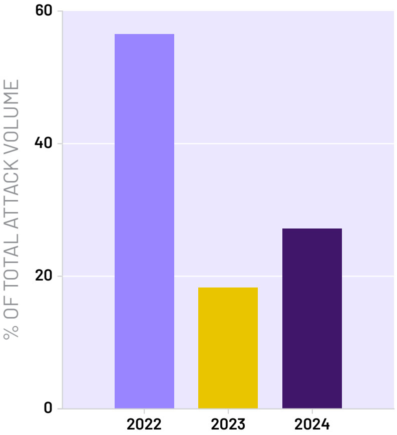
Streaming & Media

The streaming and media industry faces many threats, including:

- Carding attacks (in which successful access to a streaming service may create a second revenue stream for a threat actor)
- Account takeover and fake account attacks (often to benefit from new user promotions)
- Advertising fraud (as observed in Satori's investigation into PARETO)
- Scraping attacks (read more in the Satori Perspectives section below)
- And other attacks specific to streaming and media businesses, like streaming fraud

As a share of all attempted **ATO** attacks observed by the Human Defense Platform, the percentage of attempted attacks focused on streaming and media businesses has been volatile over the past three years, but remains high overall:

ATO Attacks on Streaming & Media Businesses, 2022–2024

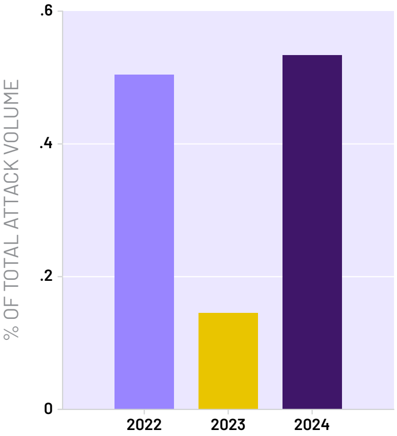


Key Findings:

- The share of attempted ATO attacks on streaming and media businesses reached a zenith in 2022 with **more than 56% of activity**, but fell significantly in 2023 before rebounding to **27% of activity** in 2024.
- The share of attempted carding attacks on streaming and media businesses is comparatively low, but grew **278%** year over year from 2023 to 2024.
- Streaming and media businesses' share of attempted scraping attacks has grown consistently over the past three years, culminating in a **16.37%** share of all activity in 2024.

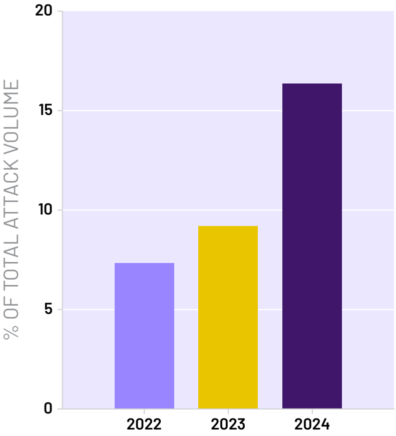
As a share of all attempted **carding** attacks observed by the Human Defense Platform, the percentage of attempted attacks focused on financial services businesses rebounded from 2023 to 2024 after a decline from 2022 to 2023:

Carding Attacks on Streaming & Media Businesses, 2022–2024



Perhaps of greatest note, as a share of all attempted **scraping** attacks observed by the Human Defense platform, the percentage of attempted attacks focused on streaming and media businesses rose consistently over the last three years, peaking at **more than 16% of all activity in 2024**:

Scraping Attacks on Streaming & Media Businesses, 2022–2024



Those scraping attack attempts may be intended in part to feed made-for-advertising (MFA) sites: threat actors capture content from legitimate publishers and republish it—with numerous ads riding shotgun—on sites built specifically to maximize ad revenue.

Satori Perspectives

Threat Actors Use AI to Build Sites for Fraud

While made-for-advertising (MFA) schemes are generally manually built by threat actors, there's a growing belief among researchers that sites showing characteristics of MFA may be generated by bots and/or AI.

In another example of AI being used for fraud, Satori researchers suspect that the sites managing the web stores that powered the Phish 'n' Ships operation were based on scraping attacks.

In the Wild

News Organization Targeted by Content Scraping Attacks

A major news organization and HUMAN customer is heavily targeted by threat actors for scraping attacks, routinely experiencing **hundreds of millions of attempts a month** across its many digital properties. HUMAN protects this customer from these scraping attack attempts, helping prevent their content from being stolen and repurposed by threat actors.

HUMAN protected their media customer from hundreds of millions of scraping attempts.

Technology, SaaS, & Services

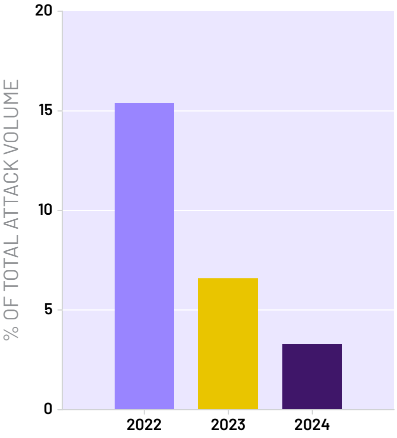
Tech companies face a wide range of cybersecurity threats, including:

- Account takeover attacks (to drain account balances, collect PII, or steal loyalty points)
- Client-side attacks (to collect PII)
- Carding attacks (to test stolen cards with immediate feedback)
- Fake account attacks (chaining fake accounts to exploit new user discounts)

Depending on the specific services offered, companies in this broad category may be particularly vulnerable to account takeover attacks and transaction abuse. The delivery mechanism used by these companies makes this a useful grouping despite the wide range of potential threats.

As a share of all attempted **ATO** attacks observed by the Human Defense Platform, the percentage of attempted attacks focused on streaming and media businesses has fallen for three consecutive years:

ATO Attacks on Technology, SaaS, & Services Businesses, 2022–2024

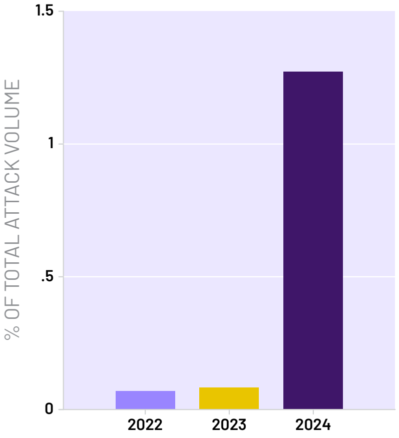


Key Findings:

- As a share of all activity, the percentage of attempted ATO attacks on technology, SaaS, and services businesses **dropped more than 50%** year over year, continuing a pattern of declining share of activity.
- The share of attempted carding attacks is relatively low for this industry, but **jumped more than 1,400%** from 2023 to 2024.
- Similarly, while the share of attempted scraping attacks is low for this industry compared to others in this report, the share **jumped more than 478% year over year**.

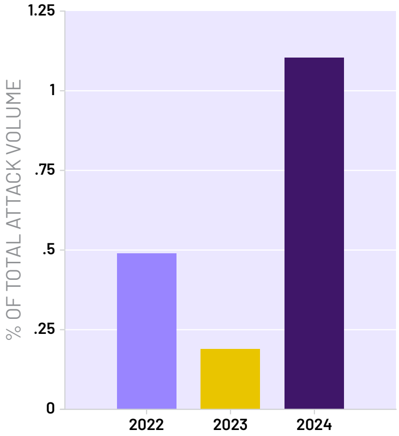
In stark contrast, while the overall share of all attempted **carding** attacks observed by the Human Defense platform is low, the percentage of attempted attacks focused on financial services businesses increased dramatically from 2023 to 2024 after being roughly level from 2022 to 2023:

Carding Attacks on Technology, SaaS, & Services Businesses, 2022–2024



Finally, as a share of all attempted **scraping** attacks observed by the Human Defense platform, the percentage of attempted attacks focused on streaming and media businesses rose significantly last year after a decline the year before:

Scraping Attacks on Technology, SaaS, & Services Businesses, 2022–2024



Satori Perspectives

Hacked Accounts Sold Cheap on the Dark Web

Satori researchers actively monitor the dark web and underground forums for threat actor activity. One such forum has numerous vendors openly selling hacked accounts for platforms in this space, often for only a few dollars each. The price for an account varies based on the account's age and any attached payment methods or rewards. It's unclear if the account's owners are aware their accounts have been compromised.

In the Wild

Delivery Platform Targeted in Scraping Attacks

An international food delivery company and HUMAN customer is heavily targeted by threat actors for scraping attacks, to the tune of **tens of millions of attempts a month**. HUMAN protects this customer from scraping attack attempts, helping prevent theft of pricing and product information for competitive purposes.

HUMAN protected their food delivery customer from tens of millions of scraping attempts.

6.

Cybersecurity Trends

In addition to analyzing data from a threat perspective and an industry perspective, we also examined questions that span multiple industries and attack types. These questions include:

1. How is AI being used to aid both attacks and defenses?
2. What forces are at play during major product releases like ticket drops?

These topics will all influence threat management in the future, acting as tools for cybersecurity professionals and threat actors or as targets for attacks.

Artificial Intelligence Introduces New Potential for Cyberthreats

While AI has revolutionized the way content creators do their work—indeed, portions of this very report were drafted with the help of AI tools—the process by which threat actors can use AI to aid in their "work" is a bit less straightforward.

All popular LLMs are built in such a way that they don't provide instructions or help for committing cybercrime. Satori researchers, however, described freely-available tools that "jailbreak" common large language models (LLMs), enabling those LLMs to offer code for nefarious activities:

One tool has no restrictions on what it can do, and as a result, provides the user with code that can be used with a scraper stack. Another example scrapes a website using a headless browser and automation, the HTML from which can be fed into an LLM, and the LLM asked to spit out a JSON with relevant scraped data ready to be pushed to a database. To that end, researchers described AI as a "smart intern" for threat actors, able to automate or expedite portions of the attack process.

The next evolution of AI-as-threat-tool is arriving imminently. Agentic AI technology centers on semi-autonomous AI-powered bots that can adapt in real time without constant human oversight. These agentic bots may be both boon and curse; in the right hands, they can purchase products on behalf of consumers, helping retail and e-commerce businesses grow. In nefarious hands, however, they can become adaptable agents of chaos.

Other new and emerging threats targeting AI and LLMs include:

- Data/model poisoning
- Prompt injection
- Misinformation
- Unbounded consumption

Additionally, as described above, Satori researchers suspect AI tools have been used in the collection of content for made-for-advertising websites, commonly used to commit ad fraud.

Threat Actors Increasingly Target Major Product Releases

Major product releases are relatively easy to predict. Ticket drops for high-profile concert tours, next-generation video game consoles, limited-inventory high-performance computer components, popular sneakers... all of these have release dates known well in advance by the general public, not to mention threat actors.

Satori researchers described the workflow for beating the system and scalping these "hype sales:"

The typical scalping workflow begins with deploying **monitor bots** on a target's website or API endpoints. Monitor bots are basically scrapers that continuously scrape a targeted page at short intervals, scouring the page's HTML to find any changes that indicate that the sale was launched.

Once the monitor bot recognizes the sale's launch, it alerts the **AIO (All in One) bot/scalping bot**. AIO bots are scalping bots that are trained to complete the purchase process: select the required item, add it to the cart, review cart, add shipping/billing details, insert payment details, and complete payment.

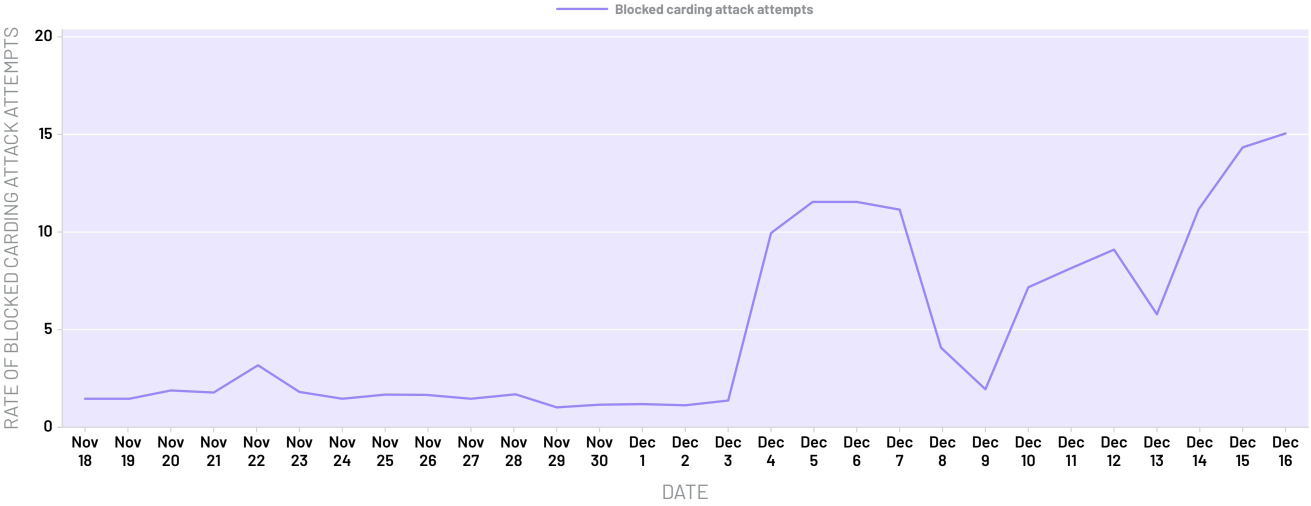
This process guarantees scalpers will have the "bot advantage" when trying to secure purchase for items that are in high-demand.

To support this process, scalpers can form or join a **"cook group"**—online underground scalping communities in which members share resources to make scalping efforts more efficient and profitable to all. Such resources can be tools, techniques and technical knowledge, insights on market trends (upcoming hype sale or discount codes for example), infrastructure (such as proxy pools), automated bots, AIO subscription, CAPTCHA solvers costs, fake accounts generators, and more. Some groups also offer "aftermath" resell services, where members can trade the scalped items and tickets, or insights and tips on where those could be resellled for a profit.

Protecting a hype sale from fraud can be tricky; the volume and speed of traffic during a sale puts any detection system to the test. The Human Defense Platform has an excellent track record of spotting and stopping fraud during hype sales.

For example, consider this chart of traffic observed by the Human Defense Platform in the two weeks prior to and two weeks following Cyber Monday (December 2, 2024):

Carding Attack Attempt Rate, November 18 – December 16, 2024



That major jump in carding attack attempt rates and its subsequent volatility immediately followed Cyber Monday.

HUMAN customers were protected from these hype sale attacks.

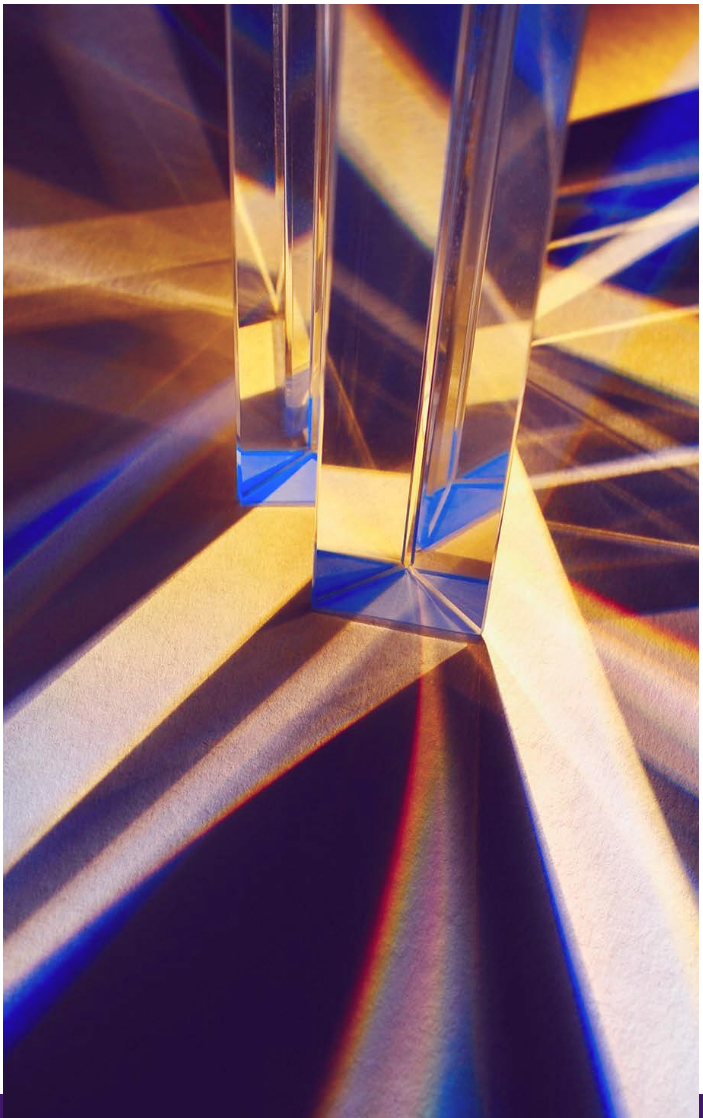
*The **Human Defense Platform** has an excellent track record of **spotting and defending against fraud** during hype sales.*

7. Conclusion

Cyberattacks such as account takeovers, fake accounts, carding, and scraping continue to pose significant threats to businesses. While HUMAN researchers have found that the rate of attacks remains consistently high, new and emerging tactics could evolve these threats in 2025 and beyond.

Next year's Quadrillion Report: 2026 Cyberthreat Benchmarks will include insights following two major milestones: enforcement of PCI DSS requirements 6.4.3 and 11.6.1, and the release of HUMAN Sightline.

As described above, the 2025 enforcement of PCI DSS requirements 6.4.3 and 11.6.1 marks a critical shift in combating client-side cyberthreats, particularly those targeting e-commerce payment pages. These requirements directly address the growing risk of attacks like Magecart, which involve malicious script injections to steal cardholder data. These requirements will herald a sea change in security in e-commerce.

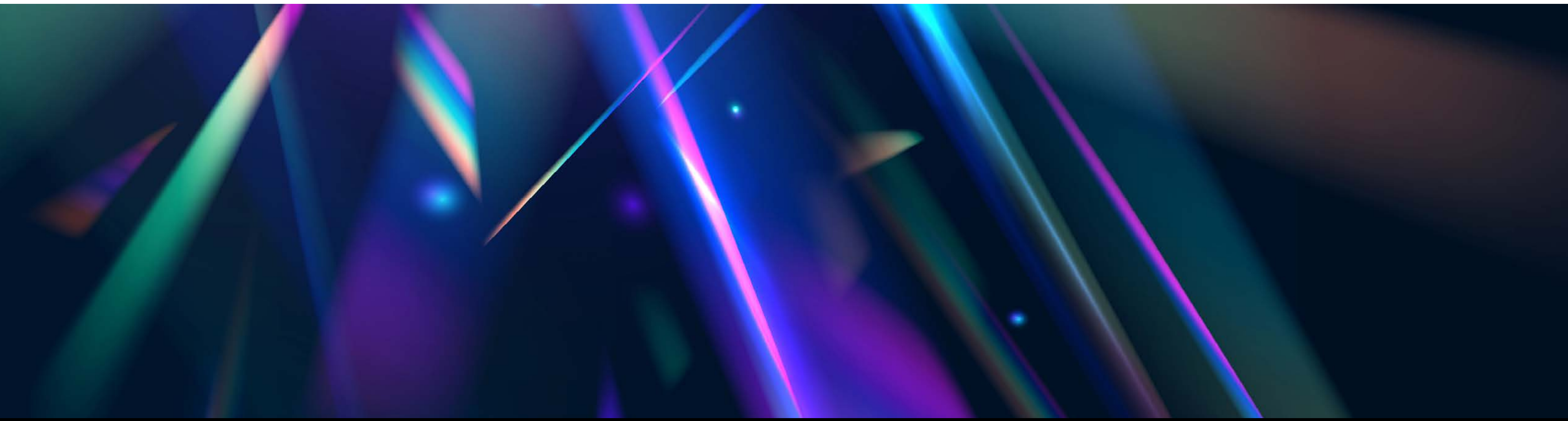


HUMAN's newly-released HUMAN Sightline capabilities allow customers to identify distinct bot profiles and detail bot-based actions on specific applications. HUMAN Sightline isolates automated traffic, tracks individual bot profiles over time, and reveals the sophistication and capabilities of attackers. The tool visualizes bot traffic, surfaces key activity details like target routes and IPs, and compares bot traffic characteristics to human traffic.

HUMAN Sightline automatically correlates disparate bot activity to pinpoint strategies and identify threat patterns. It tracks bot profiles, including potential AI agents, and uses layered AI models to analyze traffic, going beyond anomaly detection. Purpose-built AI algorithms analyze automated traffic data in aggregate, isolating and segmenting it into distinct profiles displayed in the HUMAN Sightline dashboard.

Cybercriminals will continue to operate as long as there is money to be made on the internet. The Human Defense Platform safeguards the internet for business, protecting both organizations and users.

*The **Human Defense Platform** safeguards the internet for business, **protecting organizations and users.***



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.